



**Integrated
Care System**
Nottingham & Nottinghamshire

Sherwood Forest Foundation Hospitals Trust

Data Protection Impact Assessment

Name of Project/ Activity/ service:	Capacity & Flow System Wide View
Date of expected project delivery:	Phase 1 - 03 Oct 22
Parties & roles of those involved:	All ICS Partners
Date of DPIA (start):	01 Jul 22
Date of activity (start):	01 Jul 22
Date of activity (end):	01 Jul 23
Date of approval/ final sign off:	
DPIA Reference number:	DPAI/SFH/001/JUL22

Contents

1	Introduction	6
2	The Proposal	7
3	Details of Leads	8
4	Details of Information Asset Owner	9
5	Key Stakeholders	9
6	Organisation Data Protection Status	9
7	DPIA Risk Assessment	10
8	Data Sets	10
8.1	Data Sets – General	10
8.2	Data Sets – Personal	11
8.3	Data Sets – Source	11
8.4	Data Sets – Format	12
9	Data Flows	12
9.1	Outbound	12
9.2	Inbound	14
9.3	Aggregated Data	14
9.4	Data View	15
9.4.1	<i>Data View - Data Entry Screen</i>	15
9.4.2	<i>Data View - OPEL Status Page</i>	15
9.4.3	<i>Data View - Dashboard Screen</i>	16
10	Data - Activities	17
11	Data - Personal	17
11.1	Personal Data - Purposes	17
11.2	Personal Data - Processing	17
11.3	Personal Data - Pseudonymisation or Anonymisation	18
11.4	Personnel Data – Free Text	18
11.5	Personal Data - Accuracy	18
11.6	Personal Data - Retention	18
12	Legal	19

12.1	Personal Data - Processing.....	19
12.2	Personal Data - Special Category	19
12.3	Common Law Duty of Confidence (CLDC).....	20
12.4	Other Legislation	21
13	Consent, Privacy and Rights.....	21
13.1	Individual’s Rights	22
13.2	Privacy Notice	22
13.3	Data Subject consultation.....	22
14	Security.....	23
14.1	Organisational Controls.....	23
14.2	Other Organisational Controls.....	23
14.3	Processing Activity	23
14.4	Technical Controls	24
14.5	Access Controls	24
14.6	Security	24
14.6.1	<i>Security - Data Storage.....</i>	<i>24</i>
14.6.2	<i>Security – Data Transferred or Transmitted</i>	<i>25</i>
14.6.3	<i>Security – Physical Measures</i>	<i>25</i>
15	Disclosure and Sharing	25
15.1	Information Sharing.....	26
16	Risk Management.....	27
17	Risk Assessment	28
18	Associated Documentation	29
19	Review Periods.....	29
19.1	Review Outcomes	29
19.1.1	<i>Review One</i>	<i>29</i>
19.1.2	<i>Review Two</i>	<i>30</i>
20	Approvals	30

List of Tables

Table 1: Details - The Proposal.....	8
Table 2: Details - Lead Details.....	8
Table 3: Details - Information Asset Owner.....	9
Table 4: Details - Key Stakeholders.....	9
Table 5: Details - Data Protection Status.....	9
Table 6: Details - High Risk Processing.....	10
Table 7: Details - Data Sets General.....	11
Table 8: Details - Data Set Personal.....	11
Table 9: Details - Data Set Sources.....	11
Table 10: Details - Data Set Format.....	12
Table 11: Details - Outbound Data.....	12
Table 12: Details - Outbound Data Flows.....	14
Table 13: Details - Agreement to Share data with SAIU.....	14
Table 14: Details - Inbound Data.....	14
Table 15: Details - Inbound Data Flows.....	14
Table 16: Details - Data Activities.....	17
Table 17: Details - Personal Data Purposes.....	17
Table 18: Details - Personal Data Processing.....	17
Table 19: Details - Pseudonymisation or Anonymisation.....	18
Table 20: Details - Accuracy of Personal Data.....	18
Table 21: Details - Personal Data Retention.....	18
Table 22: Details - Personal Data Processing.....	19
Table 23: Details - Special Category.....	20
Table 24: Details - CLDC Consent.....	20
Table 25: Details - CLDC Process.....	20
Table 26: Details - Other Legislation.....	21
Table 27: Details - Consent Type.....	21
Table 28: Details - Consent.....	21
Table 29: Details - Individuals Rights.....	22
Table 30: Details - Privacy Notice.....	22
Table 31: Details - Data Subject Consultation.....	22
Table 32: Details - Organisational Controls.....	23
Table 33: Details - Other Organisational Controls.....	23
Table 34: Details - Processing Activity Period.....	23
Table 35: Details - Technical Controls.....	24
Table 36: Details - Access Control.....	24
Table 37: Details - Security of the Data within Systems.....	24
Table 38: Details - Security of the Data Transferred/Transmitted.....	25
Table 39: Details - Physical Security Measures.....	25
Table 40: Details - Disclosure and Sharing.....	25
Table 41: Details - Information Sharing.....	26
Table 42: Details - Risk Management.....	27
Table 43: Details - Risk Assessment.....	28
Table 44: Details - Associated Documentation.....	29
Table 45: Details - Review Periods.....	29

Table 46: Details - Review One29
Table 47: Details - Review Two30
Table 48: Details - Approvals.....30

List of Figures

Figure 1: Data View - OPEL Data Metric Entry Screen.....15
Figure 2: Data View - OPEL Status Screen.....16
Figure 3: Data View - OPEL Dashboard View16

1 Introduction

Data Protection legislation requires organisations to implement appropriate measures to ensure and be able to demonstrate data protection compliance, taking into account the risks to individuals data protection rights and freedoms. In certain circumstances, completion of a Data Protection Impact Assessment (DPIA) is a requirement by law and an important means of evidencing our compliance with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation.

The DPIA process must:

- describe the nature, scope, context, and purposes of the processing.
- assess necessity, proportionality, and compliance measures.
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Completed DPIAs will form part of the Capacity and Flow-System Wide View Project and wider ICS (or where completed on behalf of Nottingham GP practices, the Practice's) 'Record of Processing Activity' which documents practice and provides assurance and compliance with statutory data protection responsibilities.

This DPIA is to be completed where the Nottingham and Nottinghamshire ICS Partners are the Data Controllers or where they are approving/commissioning a service or change to a service involving processing of personal data and personal special category data.

Special Category data is classed as:

- personal data revealing **racial or ethnic origin**; personal data revealing **political opinions**; personal data revealing **religious or philosophical beliefs**; personal data revealing **trade union membership**; **genetic data**; **biometric data** (where used for identification purposes); data concerning **health**; data concerning a person's **sex life**; and data concerning a person's **sexual orientation**.

Third parties completing this DPIA should ensure it is written from the ICS partners perspective.

A DPIA should be completed by the Project/initiative Manager, in conjunction with the relevant Information Asset Owner(s) with the help of Information Governance (IG) and any other relevant parties such relevant information asset owners e.g. Data team, Procurement, ICT and Legal team colleagues and/ or third parties to be involved in the work.

Users are encouraged to follow the detailed DPIA guidance when completing this DPIA form.

2 The Proposal

Details about this assessment are contained in the table below

Title of the Project	Capacity and Flow-System Wide View Dashboard
<p>Brief description of the project to include parties involved and role description.</p> <p>Description of proposed use/ movement of / access to personal / special category personal data (data flows).</p>	<p>Data that is currently supplied for OPEL reporting to be captured automatically from source (Nerve Centre and TIE or Line of Business System) and pushed into a database to view on a dashboard style interface. Until automated data paths are achieved for all data metrics the interim approach is to enter data manually.</p>
<p>Describe any benefits, quality expectations & intended outcomes</p>	<p>Benefit - System Calls and Meetings. Possible reduction in the frequency/requirements, by sharing relevant real-time data to all partners there is no requirement to discuss during meetings and calls</p> <p>Benefit - Availability of Information. The dashboard could allow more people within organisations to access whilst mobile/home working. More flexibility for Operational Staff when mobile or home working</p> <p>Benefit - Duplication of Effort. The data can be captured once and re-purposed for other requirements around the system such as analysis and modelling. No duplication of effort in gathering data. Gather once and gather for all.</p> <p>Benefit - Bed Days. Potential saving on bed days across the system by providing high-level data to reduce transfers/discharges through forecasted demand. Lost bed days or costs associated with lost packages if resources are in the right place at the right time as forecasted through the data.</p> <p>Benefit – Discharges. Potential to assist with simple and supported discharges across the ICS by advance notification of pressures and issues as displayed on the dashboard</p> <p>Benefit – Packages of Care. Possible savings in packages of care across the system by providing the high-level data everybody can be proactive in seeing what is coming and therefore possibly reduce delays in transit/discharges.</p> <p>Benefit – System & Partner Administrative Time. Possible reduction in the overall system/partner time taken to gather the data required on a daily basis to populate the OPEL Report.</p>

	<p>Benefit – Re-usable Product. <i>The Dashboard product could be re-used to cater for other data metrics across partnerships/departments etc which could ensure a more proactive service rather than a reactive one.</i></p> <p>Benefit – Automation of the OPEL Scores for partners. <i>The software can allow an automated process to the scoring requirements so apply some uniformity on scoring as currently could change depending on who is reporting.</i></p> <p>Benefit – Better use of Resources. <i>Planned resources rather than short notice based on the high-level data, improved staff morale when being more proactive rather than reactive with constant changes and improved stress levels at all levels.</i></p> <p>Benefit – Data Collection. <i>The data promotes sharing across the partnership for better analysis and predictive work for the future</i></p> <p>Benefit – System Redundancy. <i>Existing system would be made redundant eventually releasing funds back to the system.</i></p>
Describe the number of individuals affected.	All operational staff and patients/residents across all partners in the system as well as Resilience Team at the NHS Nottingham and Nottinghamshire Integrated Care Board.
Provide information with regards the individuals involved – i.e., adults, children, vulnerable individuals etc	Adults, Children, Vulnerable incl Mental Health. Although only high-level data (figures) rather than patient identifiable data will be presented on the dashboard
Describe any relevant constraints to the project	<ol style="list-style-type: none"> 1. Obtaining data from partners automatically to fully realise all the benefits. 2. Operational engagement due to existing pressures in the system

Table 1: Details - The Proposal

3 Details of Leads

Details of the responsible lead to the project (this must be an internal NHS staff lead) Any external party details can be added in addition

Name	Jeremy Baxter
Job Title	Project Manager – System Wide View
Department	Digital Notts - Capacity and Flow
Contact address	N/A
Email address	Jeremy.baxter@nhs.net
Telephone number	07918 963177

Table 2: Details - Lead Details

4 Details of Information Asset Owner

Details of the Information Asset Owners (Information Asset Owners must include a SFH individual or if relevant, other NHS organisation individual)

Name	Rachel Eddie
Job Title	Chief Operating Officer
Department	Sherwood Forest Hospitals NHS Foundation Trust
Contact address	N/A
Email address	rachel.eddie@nhs.net
Telephone number	N/A

Table 3: Details - Information Asset Owner

5 Key Stakeholders

Details of key stakeholder. (These may be internal individuals and external parties)

Name & Job Title	Org	Email
Jaki Taylor/Chair Programme Board	NHIS	jacqueline.taylor@notts-his.nhs.uk
Fiona Yates/Digital Transformation Engagement Lead	NHIS	fiona.yates@notts-his.nhs.uk
Simon Frampton/Head of Urgent Care Resilience	ICB	simon.frampton@nhs.net
Maria Principe/Population Health and Outcomes Lead	ICB	maria.principe@nhs.net
Rachel Eddie/Chief Operating Officer	SFH	rachel.eddie@nhs.net
Lorraine Palmer/Head of Care Integration	SFH	lorraine.palmer2@nhs.net
Claire Waite/Care Integration Manager	Digital Notts	claire.waite1@nhs.net

Table 4: Details - Key Stakeholders

6 Organisation Data Protection Status

Details of ICO registration and Data Security & Protection Toolkit (DSPT) submission status (please state if full toolkit or entry level submitted and status e.g. (fully met) in **Table 5**.

Note:

- ICO Registration - <https://ico.org.uk/ESDWebPages/Search>
- DSPT Submission Status- <https://www.dsptoolkit.nhs.uk/OrganisationSearch>

Organisation Name	ICO Registration Number	DSPT Submission Status
SFH	Z4885823	Approaching Standards

Table 5: Details - Data Protection Status

7 DPIA Risk Assessment

Assessment of the proposal against the GDPR ‘High Risk’ criteria requiring a DPIA. High Risk Processing please state Yes or No in **Table 6**.

Does the processing meet the criteria of ‘high risk’ processing? (see guidance below) – Yes/No. Add comments as required.	No
Comments: <i>No personal identifiable data will be requested or used within the Capacity and Flow dashboard. Only high-level data will be requested and used for all partners in the ICS.</i>	

Table 6: Details - High Risk Processing

Guidance: Examples of high-risk processing are:

- Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
- Any profiling or monitoring of individuals on a large scale
- Decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data. (Special category data includes personal health data).
- Data matching: Combining, comparing or matching personal data obtained from multiple sources
- Tracking: Processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment.

8 Data Sets

8.1 Data Sets – General

Does the project /activities include any of the following data sets. Enter Yes or No in **Table 7**.

Srl	Data Set	Yes/No
A	Person-identifiable details (e.g. name, address, e-mail address, postcode, date of birth)	No
B	Identifier numbers (e.g. NHS, national insurance, passport, driving license numbers)	No
C	Genetic data (e.g. DNA, an individual’s gene sequence)	No
D	Biometric data (e.g. fingerprints, facial recognition, retinal scans)	No
E	Family, lifestyle and social circumstances (e.g. marital status, housing, travel, leisure activities, membership of charities)	No
F	Vulnerable individuals (e.g. refer to safeguarding policies)	No
G	Education and training details (e.g. qualifications or certifications, training records)	No
H	Employment details (e.g. career history, recruitment and termination details, attendance details, appraisals)	No

DATA PROTECTION IMPACT ASSESSMENT

I	Financial details (e.g. banking, income, salary, assets, investments, payments)	No
J	Goods or services (e.g. contracts, licenses, agreements)	No
K	Legal details (e.g. legal documents or agreements, court papers)	No
L	Cultural identity including racial or ethnic origin	No
M	Political opinions, religious or philosophical beliefs	No
N	Health data (e.g. treatment, diagnosis, medical information including a physical or mental health or condition)	No
O	Location data (e.g. GPS location, Wi-Fi tracking, vehicle tracking)	No
P	Technology identifiers (e.g. device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags)	No
Q	Criminal proceedings (e.g. convictions, outcomes, sentences including offences or alleged offences)	No
R	Sexual life (e.g. sexual health, sex life or sexual orientation)	No

Table 7: Details - Data Sets General

8.2 Data Sets – Personal

Indicate which data subject's personal data will be processed. State Yes or No in **Table 8**.

Srl	Subject	Yes/No
A	Employees'/ Contractors'	No
B	Patients', their relatives or representatives	No
C	Students'/ Pupils'	No
D	Business partners' or organisations'	No
E	Other (please specify): No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard	

Table 8: Details - Data Set Personal

8.3 Data Sets – Source

Indicate the source of personal information. All information and information sources must be covered in **Section 9** (Data Flows). State Yes or No in **Table 9** below.

Srl	Information	Yes/No
A	Obtained from the individual directly	No
B	Obtained indirectly from another source	No
C	Publicly Available	No
D	Other (please specify): Line of Business System/TIE	

Table 9: Details - Data Set Sources

8.4 Data Sets – Format

Indicate which of the following formats are used for the data by stating Yes or No in **Table 10**.

Srl	Information	Yes/No
A	Audio or Video tape/cassette	No
B	Digital document	No
C	Digital image	No
D	Digital video	No
E	Email	Yes
F	Microfilm	No
G	Paper documents	No
H	Web Content	No
I	Other (please specify): HL7 Messaging , Manual Input , Excel Files , HTML	

Table 10: Details - Data Set Format

9 Data Flows

The next two sections describe the data flows involved. They should be described from the originating data controller’s point of view. Try to describe the flows in a way that describes the journey of the data. Include all necessary detail even if this repeats something described at another point. The data flow section is key to understanding risks and lawfulness of the data processing.

9.1 Outbound

Outbound data flows, Outbound is where data is sent or made available to another party or individual outside of the sending team or organisation. State Yes or No if there is No Outbound Flowing Data.

State Yes or No if there is no Outbound flowing data	Yes
---	-----

Table 11: Details - Outbound Data

Outbound data flows: list all outbound flows whether sent internally within the organisation or sent externally to outside organisations. List ALL flows, where possible, in sequential order in **Table 12**.

Srl	Data Item	Format	Method	Receiver
1	Undeclared Bed Requests	Manually Entered	Manually Entered	Database
2	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
3	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
4	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
5	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
6	Number of Patients in ED (Kingsmill)	Manually Entered	Manually Entered	Database
7	Number of Adult Mental Health patients in ED	Manually Entered	Manually Entered	Database
8	Waiting Time	Manually Entered	Manually Entered	Database
9	Admission Wait via ED	Manually Entered	Manually Entered	Database
10	Adult Occupancy - Kingsmill	Manually Entered	Manually Entered	Database
11	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
12	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
13	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database

DATA PROTECTION IMPACT ASSESSMENT

14	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
15	Patients Discharged Straight Home	Manually Entered	Manually Entered	Database
16	Planned Simple Discharges	Manually Entered	Manually Entered	Database
17	Planned Supported Discharges	Manually Entered	Manually Entered	Database
18	Total in ITU	Manually Entered	Manually Entered	Database
19	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
20	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
21	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
22	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
23	COVID Status	Manually Entered	Manually Entered	Database
24	COVID +ve	Manually Entered	Manually Entered	Database
25	<i>No of Male</i>	Manually Entered	Manually Entered	Database
26	<i>No of Female</i>	Manually Entered	Manually Entered	Database
27	COVID +ve Inpatients	Manually Entered	Manually Entered	Database
28	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
29	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
30	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
31	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
32	<i>Closed Beds</i>	Manually Entered	Manually Entered	Database
33	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
34	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
35	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
36	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
37	<i>Beds Closed for Infection</i>	Manually Entered	Manually Entered	Database
38	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
39	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
40	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
41	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
42	<i>Closed Empty Beds</i>	Manually Entered	Manually Entered	Database
43	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
44	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
45	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
46	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
47	<i>Empty Beds Closed for Infection</i>	Manually Entered	Manually Entered	Database
48	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
49	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
50	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
51	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
52	<i>Total Leaving ITU</i>	Manually Entered	Manually Entered	Database
53	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
54	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
55	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
56	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database
57	<i>Total Arriving ITU</i>	Manually Entered	Manually Entered	Database
58	<i>No of Male Beds</i>	Manually Entered	Manually Entered	Database
59	<i>No of Female Beds</i>	Manually Entered	Manually Entered	Database
60	<i>No of Enhanced Beds</i>	Manually Entered	Manually Entered	Database
61	<i>Total % against Capacity</i>	Manually Entered	Manually Entered	Database

DATA PROTECTION IMPACT ASSESSMENT

62	Elective Cancellations	Manually Entered	Manually Entered	Database
63	Total Staff Sickness Loss	Manually Entered	Manually Entered	Database
64	Total Staff Sickness Loss (COVID)	Manually Entered	Manually Entered	Database
65	Daily OPEL Score/Rating	Numeric 1-4	Manually Entered	Database
66	No Right to Reside Totals	HTTP Post API	Pushed 15 mins	Database
67	Medically Safe for Transport	HTTP Post API	Pushed 15 mins	Database

Table 12: Details - Outbound Data Flows

Note: It should be noted that the data will be stored in the Database. The data can then be used for analytical and modelling purposes by other departments within the ICS, including the System Analytical and Insight Unit.

State Yes or No if you agree to share data stored with SAIU	Yes
--	-----

Table 13: Details - Agreement to Share data with SAIU

9.2 Inbound

Inbound data flows. Inbound is where data is received. It also includes data which is made available to or by a party or individual (i.e. it is incoming whether physical transfer or is data that becomes known by a new receiving party).

List ALL flows, where possible in sequential order in **Table 14**. See Guidance below.

State Yes or No if there is no Inbound flowing data	No
--	----

Table 14: Details - Inbound Data

Inbound data flows – list all inbound flows whether internal or external to the organisation. List ALL flows, where possible in sequential order in **Table 15**.

Flow No	Name of Data Sender	Data Format	Purpose	Method of sending	Name of Receiver
N/A	N/A	N/A	N/A	N/A	N/A

Table 15: Details - Inbound Data Flows

9.3 Aggregated Data

Aggregated data will be used for some of the data metrics collected in *Section 9.1*, as the requirement is to report as a trust rather than as individual organisations. There are plans to look at aggregation in future stages of the development when automated data is achieved, however for stage 1 the aggregated data will be entered manually by each organisation's user.

9.4 Data View

The screenshots below are an example of how the data will look when entering data into the dashboard and what the dashboard will look like after development.

The product is still in development and stage 1 is due to be completed before Winter 2022, therefore the screenshots below are from the Prototype so may change slightly in the final version

9.4.1 Data View - Data Entry Screen

The screenshot below highlights a typical Data Entry Screen for a partner where the metrics that will be displayed need to be entered. There is also the opportunity to upload the last set of figures that was entered to save time if little or no change.

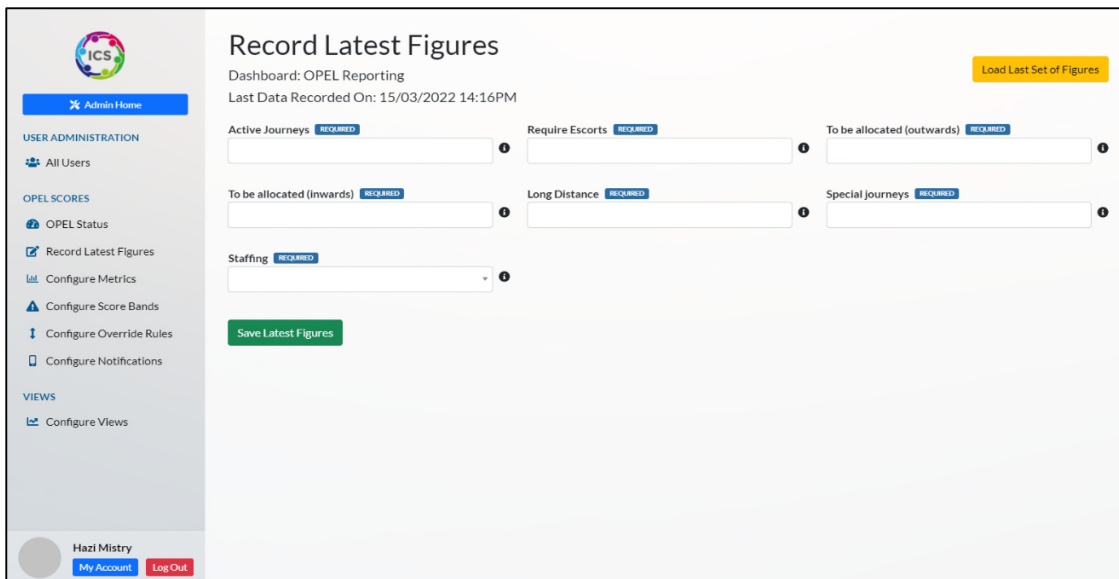


Figure 1: Data View - OPEL Data Metric Entry Screen

9.4.2 Data View - OPEL Status Page

Figure 2 shows a screenshot of the OPEL status screen that will show the metric data current and before allowing the user to identify if the figures to help identify a trend of figures increasing, reducing or staying the same. It will also allow the user to see the automated OPEL Score prior to submission or give the User the option to override the automated OPEL Score and to allow them to enter another score

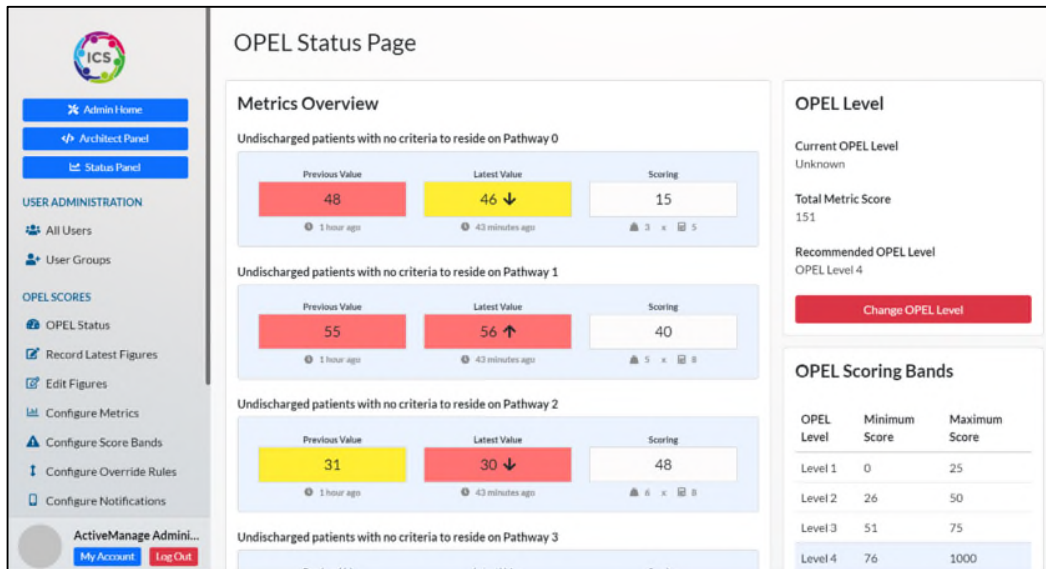


Figure 2: Data View - OPEL Status Screen

9.4.3 Data View - Dashboard Screen

The picture in **Figure 3** shows what the dashboard screen will look like when presenting all the data entered from the organisation. Each metric will be visualised using a BRAG (Black, Red, Amber, Green) status to visually indicate if service/level is in low or high escalation to allow Users / organisations to predict flow or to highlight pressure areas.

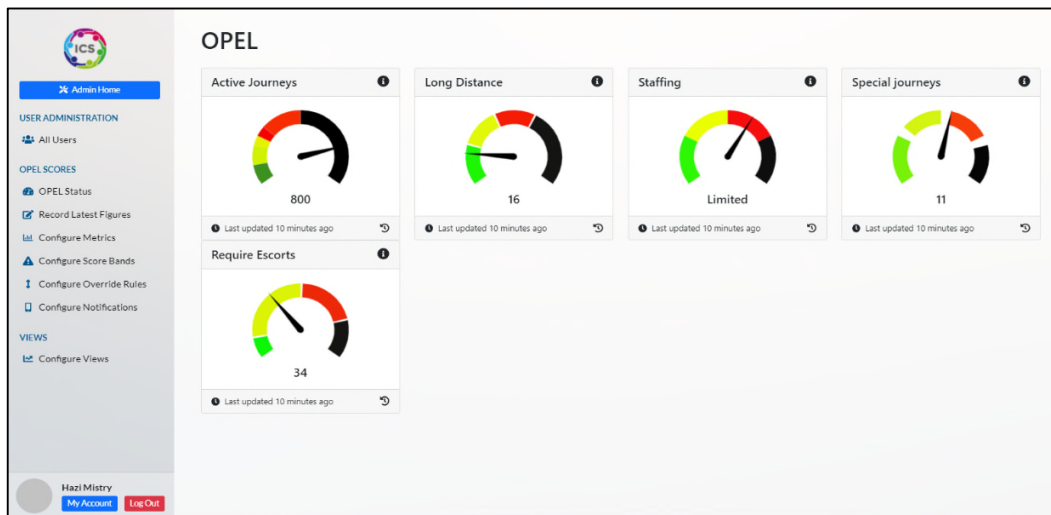


Figure 3: Data View - OPEL Dashboard View

10 Data - Activities

Does the project include any of the following activities in **Table 16**, Yes/No

Srl	Activity	Yes/No
A	Retrieval, obtaining, recording or holding information or data	Yes
B	Alignment, matching, combining, organisation, adaptation, alteration of data	Yes
C	Blocking, erasure or destruction of information or data	No
D	Disclosure or sharing of information or data	No

Table 16: Details - Data Activities

11 Data - Personal

11.1 Personal Data - Purposes

Collected for specified, explicit and legitimate purposes. State the ‘purpose(s)’ clearly and completely for which personal data is being obtained/accessed/ processed. The purpose should be clear so that is it easy to understand the legal basis for the processing

Srl	Detail	Yes/No
A	Purpose 1 - N/A	
B	Purpose 2 - N/A	
C	Purpose 3 - N/A	
Further processing		
Confirm that no further use is intended to be made of the data		Yes
Comments: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard		
Confirm that the National Data Opt Out does not apply		Does Not Apply
If the National Data Opt Out applies comment here how Opt Outs will be upheld. (<i>Ensure any associated risks are captured in the risk table in Sect 15</i>).		

Table 17: Details - Personal Data Purposes

11.2 Personal Data - Processing

Minimising the personal data collected to fulfil purposes

Srl	Question	Yes/No
A	Is the personal data being obtained or accessed, the minimal amount necessary to fulfil the purposes above – Yes/No. (if No please explain reasons why)?	No
B	Comments: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard	

Table 18: Details - Personal Data Processing

11.3 Personal Data - Pseudonymisation or Anonymisation

Pseudonymised data can be linked back to the individual. Anonymisation, meanwhile is when the information does not relate to al identifiable person and been process in such a way that the individual is no longer identifiable.

Srl	Question	Yes/No
A	Will pseudonymisation or anonymisation processes take place – Yes/No (if yes, please describe)?	No
B	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 19: Details - Pseudonymisation or Anonymisation

11.4 Personnel Data – Free Text

The current methodology for entering organisations OPEL scores into the system allows for a free text box to be used to clarify and quantify some of the data metrics and if required give a summary of that particular data metric score.

The new software will provide this feature for the same use. However the same procedures by the users should be adopted to ensure no personal data is entered into eh free text box. There will be a warning sign next to the box to re-iterate that no personal data is to be entered.

11.5 Personal Data - Accuracy

Accuracy of the data and where necessary that the data is kept upto date.

Srl	Question	Yes/No
A	Confirm that there is a process in place for ensuring that personal data is accurate and is reviewed where necessary – Yes/No (Please describe process)	No
B	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 20: Details - Accuracy of Personal Data

11.6 Personal Data - Retention

Retention of the data and ensure the data is stored appropriately and the data is not held longer than is necessary

Srl	Question	Yes/No
A	The process effectively manages retention of personal data & is aligned to the Organisation’s (of the Data Controller) published retention schedule. See guidance	N/A
B	List the relevant Retention Period(s):	N/A
C	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 21: Details - Personal Data Retention

Guidance:

The NHS Records Management Code of practice is found here which includes the guidance for records retention periods: [Records Management Code of Practice 2020 - NHSX](#)

12 Legal

Lawfulness of Processing. Tick all relevant conditions which apply to the processing of personal and special category data. To ensure the processing can be done lawfully at least one of the conditions must apply in **Section 12.2** in relation to all personal data and, if processing special categories of personal data, at least one must apply in **Section 12.3**.

12.1 Personal Data - Processing

For the processing of “personal data” to be lawful, you need to identify at least one of the following – Identified Yes or No in **Table 22**

Srl	Question	Yes/No
A	The data subject has given consent for the purpose. This is often the last option. Find an alternative if possible. (<i>Refer to DPIA guidance</i>).	N/A
B	The processing is necessary for the performance of a contract to which the data subject is a party	N/A
C	The processing is necessary for the compliance with a legal obligation to which the controller is subject (be prepared to identify and state what that is)	N/A
D	Necessary to protect the vital interests of the data subject (life or death)	N/A
E	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (be prepared to reference what the official authority is)	N/A
F	Necessary for the legitimate interests pursued by the controller (<i>not applicable to public bodies for processing except for some instances of disclosure</i>)	N/A
G	Please provide explanatory information here, e.g. the necessity; the legal obligation; contract, etc: Comment: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard	

Table 22: Details - Personal Data Processing

12.2 Personal Data - Special Category

For the processing of “special categories” of data to be lawful, you need to identify at least one of the following – Identified Yes/No:

Srl	Question	Yes/No
A	Explicit consent of the data subject unless consent is prohibited under law	N/A
B	Necessary for the carrying out of obligations under employment, social security, or social protection law	N/A
C	Necessary for the vital interests of the data subject who is physically or legally incapable of giving consent	N/A

DATA PROTECTION IMPACT ASSESSMENT

D	Not-for-profit body with a particular aim (as specified under the Act) where the subject is a member or former member and provided there is no disclosure to a third party without consent	N/A
E	Made public by the data subject	N/A
F	Necessary for the establishment, exercise or defence legal claims/ courts acting in their judicial capacity	N/A
G	Necessary for reasons of substantial public interest which is proportionate and has necessary safeguards in place	N/A
H	Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or management of health or social systems and services based on law or contract with a health professional	N/A
I	Necessary for reasons of public interest in the area of public health	N/A
J	Archiving scientific and historical research purposes or statistical purposes in the public interest	N/A
K	Please provide explanatory information here, e.g. the necessity; the legal obligation; contract, etc: Comment: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard	

Table 23: Details - Special Category

12.3 Common Law Duty of Confidence (CLDC)

Common law duty of confidence, state whether the individual to whom the information relates has given consent for its use and whether this is implied or whether explicit consent has been granted in

Table 24

Srl	Consent	Implied/Explicit
A	The individual to whom the information relates has given consent	N/A

Table 24: Details - CLDC Consent

Where a duty of confidence is owed to the individual and the legal basis for processing under GDPR is **not** consent please indicate how the CLDC will be met by answering questions in **Table 25**:

Srl	Process	Yes/No
B	The disclosure is in the overriding public interest	No
C	There is a legal duty to do so, for example a court order	No
D	There is a statutory basis that permits disclosure such as approval under Section 251 NHS Act 2006	No
E	Please provide explanatory information here: (e.g. consent particulars; public interest reason; specific legal duty, etc.): No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard	

Table 25: Details - CLDC Process

12.4 Other Legislation

List any applicable legislation that applies to the processing in the table below (*add more as required*)

Srl	Legislation
A	Nil

Table 26: Details - Other Legislation

13 Consent, Privacy and Rights

If consent is being relied upon or used, then please state in **Table 27** whether this consent is **verbal**, in writing (**written**) or **both** verbal and written

Srl	Question	Verbal/Written/Both
A	Is consent obtained through (written or verbal means)	N/A
B	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 27: Details - Consent Type

Further expand on consent, privacy and rights by answering the questions laid out in **Table 28**

Srl	Consent	Yes/No
A	Is consent recorded?	N/A
B	If answered Yes , state how the consent will be collected and recorded: Comment: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	
C	Can the individuals withdraw or opt-out from their data being processed?	N/A
D	How will the withdrawal or opt-out be managed and recorded? Comment: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	
E	Notice was provided to the individuals prior to collection of data	N/A
F	The data will be used for the following purposes Comment: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 28: Details - Consent

13.1 Individual’s Rights

Does the processing support the right in **Table 29**, below (See DPIA Guidance when answering Yes/No). Provide comments where required.

Srl	Process	Yes/No	Comments
A	The Right to be Informed	N/A	See below
B	The Right of Access	N/A	See below
C	The Right to Rectification	N/A	See below
D	The Right to Erasure	N/A	See below
E	The Right to restrict Processing	N/A	See below
F	The Right to Data Portability	N/A	See below
G	The Right to Object	N/A	See below
H	Rights related to automated decision making and profiling	N/A	See below
I	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>		

Table 29: Details - Individuals Rights

13.2 Privacy Notice

Data Subjects must be made aware PRIOR to the use of their data in a new/ unexpected way

Srl	Question	Yes/No
A	Are Data Subjects advised about this use of their data?	No
B	How are Data Subjects made aware (list all methods) Comment: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 30: Details - Privacy Notice

13.3 Data Subject consultation

Describe any consultation with Data Subjects about this processing of personal data in the table below.

Srl	Consultation	Yes/No
A	Has any consultation been undertaken with Data Subjects? (i.e. wide pre- project discussions/ forum/consultation)	Yes
B	Comments: <i>Consultation has been done with IG teams, partners, programme board and technical departments to clarify what could be personal data. No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 31: Details - Data Subject Consultation

14 Security

Appropriate Security is in place, both organisational and technical controls, to protect the personal data.

14.1 Organisational Controls

Contractual Control details are in **Table 32**

Srl	Control	Yes/No
A	Confirm the processing is or will be covered by a contract or agreement?	No
B	Confirm the contract or agreement contain the necessary detail in respect of the processing activities	N/A
C	Confirm the contract/ agreement stipulate arrangements for return, handover or disposal of data following cessation of the contracted services	N/A

Table 32: Details - Organisational Controls

14.2 Other Organisational Controls

Other organisational controls are highlighted in **Table 33**

Srl	Other Control	Yes/No
A	All parties are aware of incident reporting requirements	N/A
B	All parties have an adequate and up to date Information Security policy in place	N/A
C	All parties will ensure the necessary training is undertaken by staff to ensure competency	N/A
D	Confirm the relevant processes are documented and available to staff	N/A

Table 33: Details - Other Organisational Controls

14.3 Processing Activity

State the period over which the processing activity will take place in table below, add comment as required.

Start Date:	01 Mar 2022	End Date:	No end date
Comments: <i>The data required will always be required. Process will be reviewed as required.</i>			

Table 34: Details - Processing Activity Period

14.4 Technical Controls

Security and Continuity plans are contained in **Table 35**:

Srl	Plan	Yes No
A	Confirm business continuity plans are in place in case of data loss or damage (as a result of human error, virus, network failure, theft, fire, floods etc)	
B	How will users escalate cyber security, data security or data breaches in a timely manner? <i>Comment: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 35: Details - Technical Controls

14.5 Access Controls

Srl	Control	Yes/No
A	Confirm that the Access Controls in place will effectively ensure that only those with a valid need to access the data can do so.	Yes
B	Confirm that the Access Controls in place are effective and ensure appropriate permissions to view, create, amend and delete data	Yes
C	<i>Comments: Access control is in place although No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard</i>	

Table 36: Details - Access Control

14.6 Security

14.6.1 Security - Data Storage

Srl	Detail	Yes/No
A	What appropriate technical security (appropriate to the sensitivity of the data) is in place to protect the data at rest e.g. encryption, strong access controls, breach or attempted unauthorised access alerts, etc.	Yes
B	<i>Comments: For data at rest, all data written to the Azure storage platform is encrypted through 256-bit AES encryption and is FIPS 140-2 compliant. Proper key management is essential. By default, Microsoft-managed keys protect your data, and Azure Key Vault helps ensure that encryption keys are properly secured</i> <ul style="list-style-type: none"> • Azure SQL data is encrypted at rest. – see https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql • Clients such as SQL Server Management Studio that connect to the database need to have their IP address whitelisted on the Azure SQL Firewall - https://docs.microsoft.com/en-gb/azure/azure-sql/database/firewall-configure?view=azuresql 	

Table 37: Details - Security of the Data within Systems

DATA PROTECTION IMPACT ASSESSMENT

14.6.2 Security – Data Transferred or Transmitted

Srl	Detail	Yes/No
A	Confirm that appropriate technical security (appropriate to the sensitivity of the data) is in place to protect the data in transit from threats	Yes
B	Comments: TLS (https) encryption is used on the web app to encrypt data in transit between Users web browser and the web application.	

Table 38: Details - Security of the Data Transferred/Transmitted

14.6.3 Security – Physical Measures

Srl	Detail	Yes/No
A	Confirm that appropriate physical measures have been undertaken to protect the data.	Yes
B	Describe the measures: Data stored is in Azure data centres. Azure Data centre will be UK South so data kept within the UK.	

Table 39: Details - Physical Security Measures

15 Disclosure and Sharing

Transfer of personal data to countries outside the EEA are contained in **Table 40**

Srl	Details	Yes/No
A	Confirm here if data is being transferred or processed outside the UK, or if it is planned that data will be processed outside the UK If "NO" go to the next table.	No
B	Confirm here that adequate steps have been taken to meet the required standards for data transferred or processed outside the UK. If unsure you must declare this.	No
C	Comments: No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard. Data will remain in Azure data centre within the UK.	

Table 40: Details - Disclosure and Sharing

15.1 Information Sharing

Srl	Detail	Yes/No
A	Will the project involve information sharing across organisations?	Yes
B	If so, is information sharing agreement in place?	N/A
C	Comments: <i>No personal identifiable data will be obtained, accessed, or processed as part of the project. Only high-level data is used on the dashboard. The high-level data will be stored and shared across all partners within the ICS, including reusing the high-level data for further analytical requirements by the System Analytical and Insight Unit.</i>	

Table 41: Details - Information Sharing

16 Risk Management

Some examples of risk management to consider are provided to help.

Srl	Data Protection Risks	Risk to Individual	Compliance Risk	Corporate Risk
1	integrity and confidentiality (security) – also includes data quality, processed securely with authorised/approved access	Significant, or even irreversible, consequences due to the Trust enabling the non-legitimate sharing of information with inappropriate staff or organisations. Loss of personal data due lack of appropriate security of the personal data, including protection against unauthorised or unlawful processing and against loss, accidental loss, destruction, or damage, using appropriate technical or organisational measures.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
2	purpose limitation – only being used for a specific purpose	Significant, or even irreversible, consequences due to the Trust enabling illegitimate access to data. Individuals’ personal data provided unlawfully or linked unlawfully or processed unlawfully for other purposes	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
3	accuracy – data quality, accurate and reliable information	Significant, or even irreversible, consequences due to inappropriate decisions being made based on the use of incorrect or misleading data.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
4	storage limitation – only held for specified purpose with set storage and retention requirements	Significant, or even irreversible, consequences due to the Trust’s non-adherence to storage and retention requirements.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
5				
6				

Table 42: Details - Risk Management

17 Risk Assessment

The Risk Assessment containing the project data processing processes are contained in **Table 43** below:

Srl	Risk Description	Likelihood	Impact	Rating	Mitigating Actions	Rating with Mitigation	Risk Owner	Review Date	Status
1	Sharing of Personnel Information/data. There is no personal data collected as only strategic data (numerical) data required. However there is the ability to enter free text which could lead to other data being entered.	2	3	6	Partners entering the data into the system need to be current in IG/Data Security Training and ensure checks in place to ensure personal data not entered.	6	SFH	01-Jul-22	Open
2	Accuracy of data. Data is currently entered manually in most cases until automated data paths have been achieved. There is always the chance of human error in entering incorrect details.	2	3	6	Partners currently enter the data manually which is checked before a report is published, therefore Users are to ensure data is checked prior to submission and regular checks are conducted to ensure accuracy of data as per existing policies and procedures	4	SFH	01-Jul-22	Open
3	Storage limitation. Again, no personal data is being collected/requested from system partners. The high-level data (ie - Numbers) are stored within a database to enable it to be re-purposed by other departments for analytical/modelling/reporting requirements.	1	2	2	The database has been designed to allow frequent data updates from all partners and to allow partners (with correct IG approval) to access data and re-purpose as required.	1	SFH	01-Jul-22	Open
4									
5									

		IMPACT				
Score		1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Significant)	5 (Catastrophic)
LIKELIHOOD	1 (Rare)	1	2	3	4	5
	2 (Unlikely)	2	4	6	8	10
	3 (Possible)	3	6	9	12	15
	4 (Likely)	4	8	12	16	20
	5 (Certain)	5	10	15	20	25

Score	Likelihood	
1	Rare	0% - 5% Chance
2	Unlikely	6% - 20% Chance
3	Possible	21% - 50% Chance
4	Likely	51% - 80% Chance
5	Certain	81% + Chance

Score	Impact	
1	Insignificant	0% - 5% Chance
2	Minor	6% - 20% Chance
3	Moderate	21% - 50% Chance
4	Significant	51% - 80% Chance
5	Catastrophic	81% + Chance

Table 43: Details - Risk Assessment

18 Associated Documentation

Please reference any relevant documents in **Table 44** below
 Please note these documents may need to be provided upon request at any point.
 This section and the documents within will not be routinely published with the DPIA but can be requested from Project Lead as/if required.

Srl	Document	Title
1	Business Case	Capacity and Flow-System Wide View-Business Case-v1.3
2	Initiation Document	Capacity and Flow-System Wide View-PID-v1.0
3	Design Document	Capacity and Flow Application Specification 24-01-2022 v0.92

Table 44: Details - Associated Documentation

19 Review Periods

Regularity of reviews. The processing activity will be reviewed regularly. State review period and comments in **Table 45** below:

Review Period (6mth, 12mth, 24mth Etc)	6 Month Review
<p>Comments: The project deadline to go live for Stage 1 deliverables is 1 Nov 22 using mainly manual data entry and a small amount semi automation of some data metrics. After this timeline work will start to look at automating the data direct from source and therefore this assessment will need to be reviewed and amended as required.</p>	

Table 45: Details - Review Periods

19.1 Review Outcomes

Add additional sections for each review conducted as required.

19.1.1 Review One

Srl	Detail	Yes/No
A	Date review conducted:	
B	Confirm that the processing as initially approved in this assessment remains unchanged	
C	All mitigations remain in place and are effective and appropriate to the level of risk	
D	No further action is required as a result of the review	
E	Comment:	

Table 46: Details - Review One

19.1.2 Review Two

Srl	Detail	Yes/No
A	Date review conducted	
B	Confirm that the processing as initially approved in this assessment remains unchanged	
C	All mitigations remain in place and are effective and appropriate to the level of risk	
D	No further action is required as a result of the review	
E	Comment:	

Table 47: Details - Review Two

20 Approvals

Function/Role	Name	Date	Comments
Data Protection Officer	Jacque Widdowson	13 th September 2022	None
Project Lead	Jeremy Baxter	21 st July 2022	None
Information Asset Owner	Rachel Eddie	23 rd September 2022	None
Caldicott Guardian	Dr David Selwyn	20 th September 2022	None
Senior Information Risk Owner	Shirley Higginbotham	6 th October 2022	None
Chief Digital Information Officer	Richard Walker	15 th September 2022	None

Table 48: Details - Approvals