This is a Local Product for Local NHS Organisations (for example NHS Trusts) who will be the Controllers for the data processed within this Product. NHS England has no access to the data or processing activities.

This document has been created by NHS England as a template for Local NHS Organisations to utilise when completing their own Data Protection Impact Assessment (DPIA) therefore this document may not be implemented by the Local NHS Organisation or used in its entirety. There are highlighted sections throughout the document which require specific information to be completed by the Local NHS Organisation.

Template Version	NHS England FDP Local DPIA Template (Identifiable) version 1.1 240424		
Document filename	FDP Local DPIA Template (Identifiable Direct Care) – Optica Acute 2.0 Final approved		
Directorate / Programme	FDP Programme	Product Name	Optica Acute
Document Reference No	*[Insert IG Reference Number]*	Information Asset Register Number	*[Insert]*
Information Asset / Product Owner Name	[redacted]	Version	2.0 Final Approved
Author(s)	Template: NHS England [redacted]	Version issue date	15/11/2024

Redaction Rationale – *The information above for 'Information Asset/Product Owner' and 'Author(s)' has been redacted as this includes personal information, this has been completed in line with Section 40 (2) of the Freedom of Information Act 2000.*

FDP Product Data Protection Impact Assessment – OPTICA Acute

Document Management

Revision History

Version	Date	Summary of Changes
0.1	18/02/2024	Initial draft
0.2	23/02/2024	NECS input to document
0.3	26/02/2024	Update and review
0.4	11/03/2024	Further updates to document
0.5	05/04/2024	Addition of data specifications and data flow
0.6	07/05/2024	Transfer to new template and additions following DGG review
1.0	14/05/2024	Final version
1.1	24/10/2024	NECS review and update to document
1.2	29/10/2024	FDP IG review and update
1.3	30/10/2024	Clean version for DGG
1.4	06/11/2024	DGG comments
1.5	12/11/2024	Response to DGG Comments
1.6	12/11/2024	Further DGG comments added and responded to
1.7	13/11/2024	NECS review and input
1.8	14/11/2024	Clean version for NHS E approval
2.0	15/11/2024	Final Approved

Reviewers

Redaction Rationale – *The information below has been redacted as this includes personal information, this has been completed in line with Section 40 (2) of the Freedom of Information Act 2000.*

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
DGG		10/04/2024	0.1 DRAFT
[redacted]	Head of IG - FDP	31/05/2024	0.6
DGG		06/11/2024	1.3
[redacted]	Deputy Director, IG Risk and Assurance	15/11/2024	1.8

Approved by

Redaction Rationale – *The information below has been redacted as this includes personal information, this has been completed in line with Section 40 (2) of the Freedom of Information Act 2000.*

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version

Jackie Gray	Director of Privacy and Information Governance	14/05/2024	0.6
[redacted]	Deputy Director, IG Risk and Assurance	15/11/2024	1.8

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS England demonstrate how we comply with data protection law.

DPIAs are also a legal requirement where the Processing of Personal Data is "*likely to result in a high risk to the rights and freedoms of individuals*". If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the Processing you are carrying out is regarded as high risk.

Generally, a DPIA will not be required when Processing Operational Data which is not about individuals. However, a DPIA may be required when Processing Aggregated Data which has been produced from Personal Data, in order to provide assurance that the Aggregated Data is no longer Personal Data.

By completing a DPIA you can systematically analyse your Processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

Defined Terms used in this DPIA

Defined terms are used in this DPIA where they are capitalised. When drafting the DPIA, those defined terms should be used for consistency and clarity. The defined terms and their meanings are set out in **Annex 1**. Not all terms in Annex 1 may be used in the DPIA.

Standard wording in this DPIA

Standard wording has been suggested in certain parts of this DPIA and highlighted yellow with square brackets around the text. You should select the wording that reflects the Processing of Data for the specific Product you are assessing and remove the square brackets, highlighting and wording you do not need to use eg:

- [For Data ingested into the FDP to create the Product]
- [For Data ingested into the Product to create the Product]

You would amend this where Data is ingested into the Product as follows:

- ~~[~~For Data ingested into the FDP to create the Product~~]~~
- ~~[For Data ingested into the Product to create the Product]~~

The aims of the Federated Data Platform (FDP)

Every day, NHS staff and clinicians are delivering care in new and innovative ways, achieving better outcomes for patients, and driving efficiency. Scaling and sharing these innovations across the health and care system in England is a key challenge for the NHS.

Harnessing the power of digital, Data and technology is the key to recovering from the pandemic, addressing longer-term challenges, and delivering services in new and more sustainable ways.

The future of our NHS depends on improving how we use Data to:

- care for our patients;
- improve population health;
- plan and improve services; and
- find new ways to deliver services.

The Federated Data Platform (FDP)

A ‘Data platform’ refers to software which will enable NHS organisations to bring together Data – currently stored in separate systems – to support staff to access the information they need in one safe and secure environment so that they are better able to coordinate, plan and deliver high quality care.

A ‘federated’ Data platform means that every hospital trust and integrated care board (ICB) (on behalf of the integrated care system (ICS)) will have their own platform which can connect and collaborate with other Data platforms as a “federation” making it easier for health and care organisations to work together.

A digitised, connected NHS can deliver services more effectively and efficiently, with people at the centre, leading to:

1. Better outcomes and experience for people

A more efficient NHS ultimately means a better service for patients, reduced waiting times and more timely treatment. The platform will provide ICBs with the insights they need to understand the current and future needs of their populations so they can tailor early preventative interventions and target health and care support. Patients will have more flexibility and choice about how and where they access services and receive care, helping them to stay healthy for longer.

2. Better experience for staff

NHS staff will be able to access the information they need in one secure place. This reduces the time they spend chasing referrals, scheduling appointments, and waiting for test results and allows them to work more flexibly to deliver high quality care for their patients.

3. Connecting the NHS

The connectivity of the platforms is extremely important as it will enable us to rapidly scale and share tools and applications that have been developed at a local level – in a secure way – supporting levelling up and reducing variation across England.

Federation means that each Trust and ICB has a separate Instance of the platform for which they are the Controller. Access for each Instance will be governed and managed by each individual organisation.

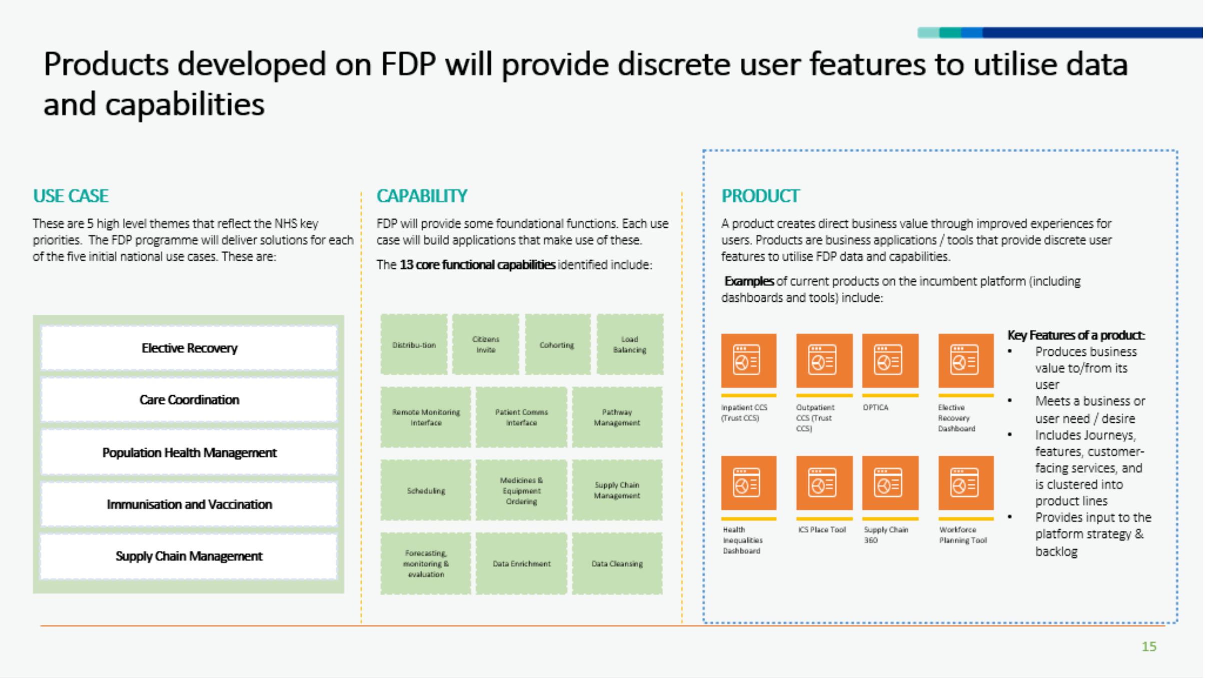
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

The FDP will not only provide the cutting-edge software to Trusts and ICBs to continue to innovate but the connectivity will enable NHS England (NHSE) to rapidly scale and share innovative solutions that directly addresses the challenges most pressing for the NHS. This will transform the way the NHS delivers its services enabling organisations to communicate and collaborate more effectively and provide better care for patients.

The ‘Product’ Data Protection Impact Assessment (DPIA)

As part of the roll out of FDP, NHS England wants to enable Trusts and ICBs to use standard FDP Products as this will reduce burden for those organisations in creating their own analytical tools and will provide a consistent approach to how Data is used in relation to the five use cases and capabilities as shown in the diagram below.

A Product DPIA is part of a suite of DPIAs for FDP that sit under the overarching FDP DPIA and provide a mechanism for assessing data protection compliance at a detailed Product level. NHS England teams have created template Product DPIAs to help NHS England, NHS Trusts and ICBs comply with UK GDPR and the FDP IG Framework.



Products developed on FDP will provide discrete user features to utilise data and capabilities

USE CASE

These are 5 high level themes that reflect the NHS key priorities. The FDP programme will deliver solutions for each of the five initial national use cases. These are:

- Elective Recovery
- Care Coordination
- Population Health Management
- Immunisation and Vaccination
- Supply Chain Management

CAPABILITY

FDP will provide some foundational functions. Each use case will build applications that make use of these.

The **13 core functional capabilities** identified include:

- Distribu-tion
- Citizens Invite
- Cohorting
- Load Balancing
- Remote Monitoring Interface
- Patient Comms Interface
- Pathway Management
- Scheduling
- Medicines & Equipment Ordering
- Supply Chain Management
- Forecasting, monitoring & evaluation
- Data Enrichment
- Data Cleansing

PRODUCT

A product creates direct business value through improved experiences for users. Products are business applications / tools that provide discrete user features to utilise FDP data and capabilities.

Examples of current products on the incumbent platform (including dashboards and tools) include:

- Inpatient CCS (Trust CCS)
- Outpatient CCS (Trust CCS)
- OPTICA
- Elective Recovery Dashboard
- Health Inequalities Dashboard
- ICS Place Tool
- Supply Chain 360
- Workforce Planning Tool

Key Features of a product:

- Produces business value to/from its user
- Meets a business or user need / desire
- Includes Journeys, features, customer-facing services, and is clustered into product lines
- Provides input to the platform strategy & backlog

15

Key information about the Product
Purpose of the Product - Overview
The aim of the product is to ensure that patients do not stay in a hospital bed any longer than is absolutely necessary and that tasks which could prevent the safe and timely discharge of a patient are completed in advance of the patient being assessed as 'Ready for Discharge'. This is achieved by linking the care teams responsible for the safe discharge of the patients together within OPTICA to complete the tasks associated with providing a full discharge package. Update – October 2024 An update has been made to this document to clarify that NHS North of England Care System Support (NECS) are acting as a sub processor on behalf of Palantir.
Local or National Product

Local	☒	National	☐

Product falls under the following Use Case(s)		
Care co-ordination	☒	To ensure that health and care organisations all have access to the information they need to support the patient, enabling care to be coordinated across NHS services.
Elective Recovery	☐	To get patients treated as quickly as possible, reducing the backlog of people waiting for appointments or treatments,

		including maximising capacity, supporting patient readiness and using innovation to streamline care.
Vaccination and Immunisation:	☐	To ensure that there is fair and equal access, and uptake of vaccinations across different communities.
Population Health Management	☐	To help local trusts, Integrated Care Boards (on behalf of the integrated care systems) and NHS England proactively plan services that meet the needs of their population.
Supply Chain	☐	To help the NHS put resources where they are needed most and buy smarter so that we get the best value for money.
Categorisation of the Data used to create the Product		**How the different Categories of Data are used in relation to the Product**
Directly Identifiable Personal Data	☒	For Data ingested into the FDP to create the Product For Data displayed or shared with users of the Product
Pseudonymised Data	☐	
Anonymised Data	☐	
Aggregated Data	☒	For Data ingested into the FDP to create the Product For Data displayed or shared with users of the Product
Operational Data	☐	
Type of Data used in the Product		
No Personal Data	☐	
Personal Data	☒	For Data ingested into the FDP to create the Product For Data displayed or shared with users of the Product
Special Category Personal Data	☒	For Data ingested into the FDP to create the Product For Data displayed or shared with users of the Product

The Product DPIAs describe:

- the purpose for the creation of the Product;
- the Data which has been processed to create the Product. Where Aggregated Data is ingested into FDP, a DPIA is still carried out to provide assurance that the Aggregated Data is not Personal Data;

- the supporting legal basis for the collection, analysis and sharing of that Data;
- the Data flows which support the creation of the Product, and;
- the risks associated with the Processing of the Data and how they have been mitigated.

National Product DPIAs

The Products described in the national Product DPIAs relate to NHS England's use of the Product and related Data in the national Instance of the platform, and therefore all risks and mitigations of those risks contained within the DPIA are only applicable to NHS England.

Local Product DPIAs

The Products described in the template local Product DPIAs relate to an NHS Trust or ICB use of the Product and related Data in a local Instance of the platform, and therefore all risks, and mitigations of those risks, contained within the DPIA are only applicable to Trusts and ICBs.

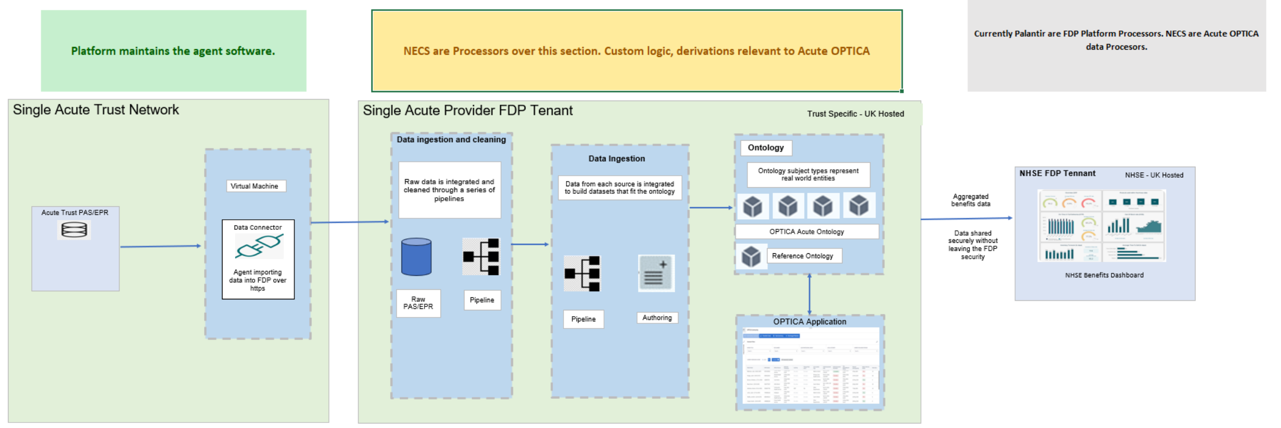
NHS Trusts and ICBs who use the Products made available to them are responsible for adopting and updating the template local Product DPIA or producing their own DPIA to reflect their specific use of the Product and to assess any specific risks relating to their organisation's use of the Product.

1. Consultation with Stakeholders about the Product

The OPTICA product was developed by NECS in collaboration with local clinicians and care providers including Local Authority partners of the incubator Trust to ensure the product aligned to local operational discharge processes and helped the wider discharge teams (health and social care) to minimise missed opportunities to discharge patients who no longer meet the criteria to reside. The learning from implementing OPTICA in subsequent was incorporated into subsequent iterations of the product. A Customer Forum was used as a primary vehicle for identifying new feature requests to improve the product and add additional value to end users.

Trusts implementing OPTICA Acute should consider the need for patient engagement prior to implementation.

2. Data Flow Diagram


Platform maintains the agent software.
NECS are Processors over this section. Custom logic, derivations relevant to Acute OPTICA
Currently Palantir are FDP Platform Processors. NECS are Acute OPTICA data Procesors.
Single Acute Trust Network
Acute Trust PAS/EPR
Virtual Machine
Data Connector
Agent importing data into FDP over https
Single Acute Provider FDP Tenant
Trust Specific - UK Hosted
Data ingestion and cleaning
Raw data is integrated and cleaned through a series of pipelines
Raw PAS/EPR
Pipeline
Data Ingestion
Data from each source is integrated to build datasets that fit the ontology
Pipeline
Authoring
Ontology
Ontology subject types represent real world entities
OPTICA Acute Ontology
Reference Ontology
OPTICA Application
Aggregated benefits data
Data shared securely without leaving the FDP security
NHSE FDP Tennant
NHSE - UK Hosted
NHSE Benefits Dashboard

HTTPS TLS 1.2+ Outbound (required Data only) for ingestion from trust network to FDP

NECS will be providing technical support to the use of the Product, as a sub Processor to Palantir.

The Data included in OPTICA Acute is also utilised within the Timely Care Hub Product. Further detail on this can be found in the Timely Care Hub DPIA.

3. Description of the Processing

Nature and scope of the processing:

Patient Directly Identifiable Personal Data will flow directly from primarily two source systems into the Trust's FDP instance. One flow is typically from the Patient Administration System (PAS) / Electronic Patient Record (EPR) and the other is from the pathology system (ICE) which only flows the COVID status of each patient. The COVID status is still required as this significantly alters the direct care that is required at discharge. Both data flows link to FDP via a 'data connector'. This module can connect directly to internet-accessible source systems or sit securely within the Trust network and transfer data back to FDP via encrypted outbound https requests.

In order to facilitate OPTICA, the Trusts in-patient list is pulled from the EPR to OPTICA (which is held within the Trusts own Instance of FDP). Only identified Trust staff have access to this information for the purpose of identifying patients that will be part of this discharge programme.

Once the patients have been identified, the Trust can provide access to other organisations to those identified patients to facilitate the discharge of the patient using the OPTICA tool.

Within the FDP local Instance, the ICE and PAS/EPR data flows link using NHS number, to validate the correct COVID status with the correct patient. All admitted patients are visible and identifiable within OPTICA. Those who are identified on the PAS/ EPR as not meeting the 'Criteria To Reside' (NC2R) or have one or more OPTICA discharge tasks are automatically filtered into a sub-set and presented in the Discharge Patient Tracking List (DPTL) dashboard of OPTICA. Each individual FDP user in the DPTL has their own 'Overview' set of tabs where discharge tasks get added by discharge team members from across health and social care, ie Trust staff can add tasks and the relevant Local Authority staff can also add tasks, creating a single shared, mutually agreed list of tasks that need to be completed for the patient so the patient can be discharged in a safe and timely manner once Discharge Ready. This shared list of tasks is regularly updated in OPTICA by the task owners (Trust and Local Authority) and then discussed routinely by MDTs to check progress and add additional tasks accordingly if agreed. The Trust whose instance of FDP the Product is in remains Controller to their own patient Directly Identifiable Personal Data within OPTICA.

One barrier of existing information systems is that Trusts don't want to provide Local Authority access to their PAS/EPR as it's difficult to restrict data access and similarly, Local Authorities don't want to provide Trust staff access to their case management systems for the same reasons. OPTICA's robust access controls enables the relevant details to be shared to benefit the patient regarding their discharge.

Staff data i.e. name, is manually added to the individual discharge checklist tasks allocated to them within the Multi-Disciplinary Team (MDT). Discharge checklist Tasks may include Tasks assigned to non-Trust staff (such as Social Workers) who are members of the MDT. The data within the Checklist Task section does not flow anywhere else within the FDP and is governed through robust Permission Based Access Controls PBAC.

NECS will be providing technical support to the use of the Product, as a sub Processor to Palantir.

The Data included in OPTICA Acute is also utilised within the Timely Care Hub Product. The Timely Care Hub Product was developed to help facilitate discharge and management of wards, further detail on this can be found in the Timely Care Hub DPIA.

Context of the processing:

The OPTICA Application

The Discharge Patient Transfer List (DPTL): This is used to manage the flow of patients on Pathways 0,1, 2 or 3 (explained below) through the creation of patient-specific tasks which are recorded on the individual patient tab and allocated to named individual members of the MDT across organisational boundaries. The tasks generated within DPTL area of OPTICA do not flow back to the PAS or EPR. It is the responsibility of the MDT member to ensure that any data generated within OPTCIA Acute is also documented within their organisations EPR. The discharge pathways are defined by the Discharge Team and partner organisations

Admitted Patient List: This provides the named list of every patient residing within the hospital at any time on pathways 0-3. This list cannot be edited within OPTICA.

1. pathway 0: discharges home or to a usual place of residence with no new or additional health and/or social care needs
2. pathway 1: discharges home or to a usual place of residence with new or additional health and/or social care needs
3. pathway 2: discharges to a community bed-based setting which has dedicated recovery support. New or additional health and/or social care and support is required in the short-term to help the person recover in a community bed-based setting before they are ready to either live independently at home or receive longer-term or ongoing care and support
4. pathway 3: discharges to a new residential or nursing home setting, for people who are considered likely to need long-term residential or nursing home care. Should be used only in exceptional circumstances

Defined in Department of Health and Social Care Statutory guidance “Hospital and community support guidance” Updated 26 January 2024

Discharged Patient List: This is the archive list of all patients within OPTICA who were on the DTPL and have been discharged. All tasks relating to their discharge planning are retained for future reference should they be readmitted. This list cannot be edited. If an individual is readmitted, OPTICA then pulls through the previous admission information for that individual from the PAS/EPR. The list is replicated within the EPR, clinicians are responsible for ensuring any tasks added within OPTICA are also documented in the EPR..

OPTICA Reports:

Access to all reports is controlled through robust PBAC controls set by the Trust (the Controller).

Admitted Patients & Discharged Patient Reports – include patient Directly Identifiable Personal Data used by operational care teams within the Trust to support direct patient care

Admitted Patients & Discharged Patient Executive Reports – include Aggregated Data used by executive teams within the Trust to identify potential missed opportunities

The acute discharge situation report (the SitRep) is an NHSE statutory data collection that collects Aggregated Data in a report on the inpatient population of each acute Trust and their discharge status by submitting a template through the NHS England Strategic Data Collection Service (SDCS) portal.

Part of this submission requires Trusts to collect information on the reason why patients who reside in hospital with a length of stay over 7 days who do not meet the criteria to reside remain in hospital and how many days they are delayed after not meeting the criteria to reside on behalf of all system partners. OPTICA enables Trusts to rapidly provide the underpinning Aggregated Data for this national submission by mapping the national codes against the current task that is holding the patient up.

This report is Aggregated Data and does not contain any patient information. This is sent to NHSE in line with the Covid-19 EPRR Acute Daily Discharge SitRep Technical Specification May 2021 outside of the Product and FDP.

Optica Acute has completed a robust clinical assurance process both at a project level and within the FDP Clinical Assurance Framework.

Data Specifications:

Please see below the attached data specifications for OPTICA Acute on page 18

Use Case:

OPTICA Acute falls within the Care Co-Ordination use case of FDP as it brings together disparate information regarding a patient in one place where all of the patients care team both from within the Trust and outside organisations to work together in one space to ensure that the patient in discharged in a timely manner ensuring that they have all of the support, equipment and care in place to be successful.

4. Purpose of Processing Personal Data for this Product

The key driver for this Product is to ensure that patients do not stay in a hospital bed any longer than is absolutely necessary and that tasks which could prevent the safe and timely discharge of a patient are completed in advance of the patient being assessed as 'Ready for Discharge'.

OPTICA has been developed by the NHS for use by local organisations to support the timely discharge of patients. Trusts (as Controllers) completely control which users get access to their own patient Directly Identifiable Personal Data. The initial ingestion of the inpatient list is only visible to the Trust staff within their Instance and the subsequent access to that information is determined by the Trust. It is important that Hospital Transfer of Care Hubs (TCHs) have access to all patients. Non-Trust staff working in TCHs will be authenticated by a secure multi factor process and will be authorised by the Trust to access this data for Direct Care, via Data Sharing Agreements which will list participating non-Trust organisations. TCHs need to determine which pathway each patient is to be discharged on and the Multi-Disciplinary Teams (MDTs) need to determine what tasks need to be completed to facilitate a safe and timely discharge for every patient, avoiding unnecessary delays once the patient is discharge ready.

Access to records is restricted based on clearly defined Permission Based Access Controls (PBAC). Local Authority employees who don't work for a TCH but work alongside the TCH to assist in the discharge process, only have access to admitted patients who are registered with a GP aligned with that Local Authority.

OPTICA enables faster, more informed decisions based on real-time data. The application brings together information currently held in disparate data systems as identified below and information regarding the patient from a number of organisations (also identified below) in one accessible, application. OPTICA enables data from complex systems such as the hospital EPR and lab result platforms such as WEBICE along with Local Authority case management systems if appropriate (subject to a Data Sharing Agreement with the Local Authority), to be viewed in one single interface. The Trust remains Controller for all data held within OPTICA [*subject to the data from Local Authorities, for which the Trust and Local Authority are joint controllers*]. Purpose based access control (PBAC) is used to ensure staff can only view information which is relevant to them. OPTICA displays key discharge metrics such as pathway data, discharge ready data, bed capacity and tasks which are frequently delaying discharges and focuses the user on potential missed opportunities.

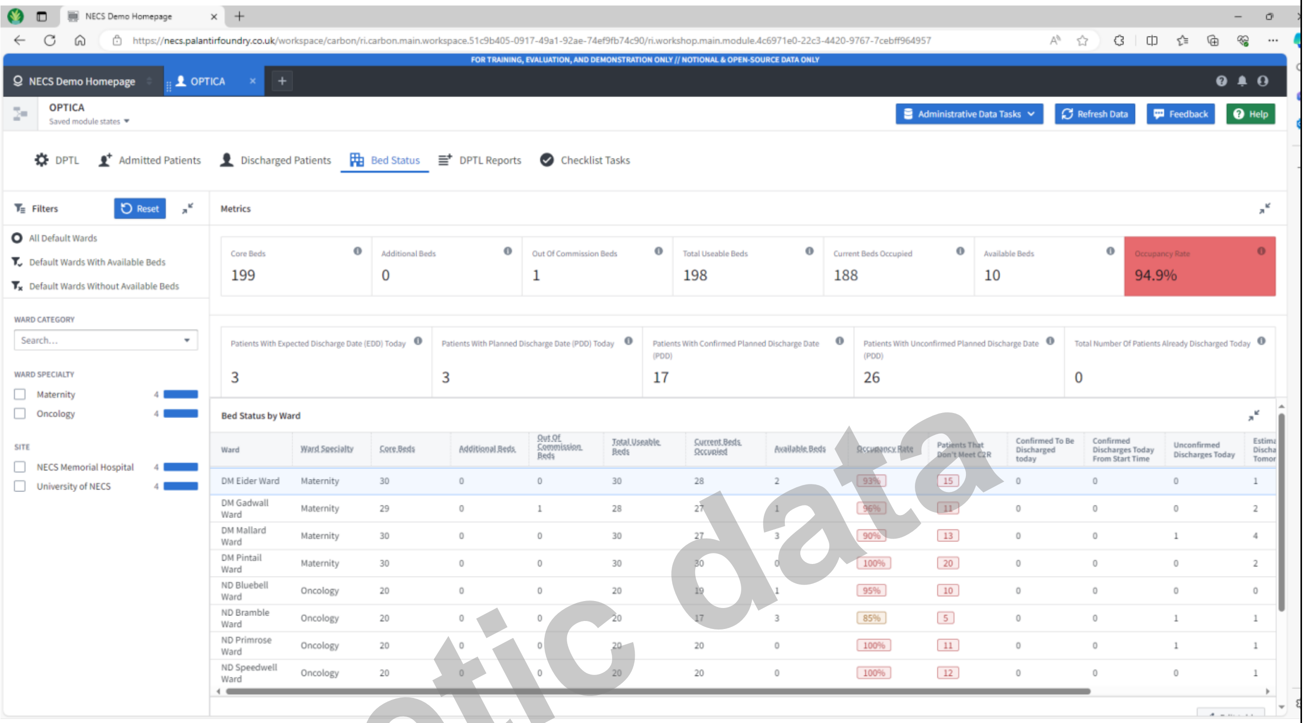
The application provides real-time visibility of admitted patients and the associated discharge-related activity to enable timely discharges and effective collaboration between the Care Team by ensuring transparent, key information is available to inform patient centred decision making and reduce administrative tasks.

Intended Outcomes

- Reduction in avoidable delay days i.e. additional days that patients occupy a bed after they have been assessed as ready for discharge by ensuring that all organisations involved in a patients discharge (such as Local Authority, Occupational Therapy and Ward Staff) can review the discharge plan in one place as an when required.
- Optimised patient flow and increased bed utilisation enabling more patients to be cared for with the same resources (beds and staff)
- Less clinical time spent in Multi-Disciplinary Team (MDT) meetings due to increased visibility of discharge tasks and the contemporary status
- Optimising bed occupancy through improved patient flow
- Reduced wait times in A&E due to freeing up beds that were occupied by patients who were waiting to be discharged because tasks had not been completed.
- Similar to the above, alleviating pressures in A&E would improve ambulance handover delays and ambulance turnaround times.
- Increased capacity to support systems with mutual aid and ambulance diverts.
- Improve outcomes for patients by minimising the risk of hospital acquired infections and associated deconditioning through avoidable extended lengths of stay in hospital.

NECS will be providing technical support to the use of the Product, as a sub-Processor to Palantir. There is a Data Processing Agreement in place to allow this processing.

Please see example of the dashboards below. Where names are shown, this is synthetic data and does not relate to any individual. It is not Personal Data and is provided as part of the demo functionality for the Product only:


NECS Demo Homepage
https://necs.palantirfoundry.co.uk/workspace/carbon/ri.carbon.main.workspace.51c9b405-0917-49a1-92ae-74ef9fb74c90/ri.workshop.main.module.4c6971e0-22c3-4420-9767-7cebff964957
FOR TRAINING, EVALUATION, AND DEMONSTRATION ONLY // NOTIONAL & OPEN-SOURCE DATA ONLY
NECS Demo Homepage
OPTICA
OPTICA
Saved module states
Administrative Data Tasks
Refresh Data
Feedback
Help
DPTL
Admitted Patients
Discharged Patients
Bed Status
DPTL Reports
Checklist Tasks
Filters
Reset
Metrics

○ All Default Wards
Default Wards With Available Beds
Default Wards Without Available Beds

WARD CATEGORY
Search...

WARD SPECIALTY
☐ Maternity 4
☐ Oncology 4

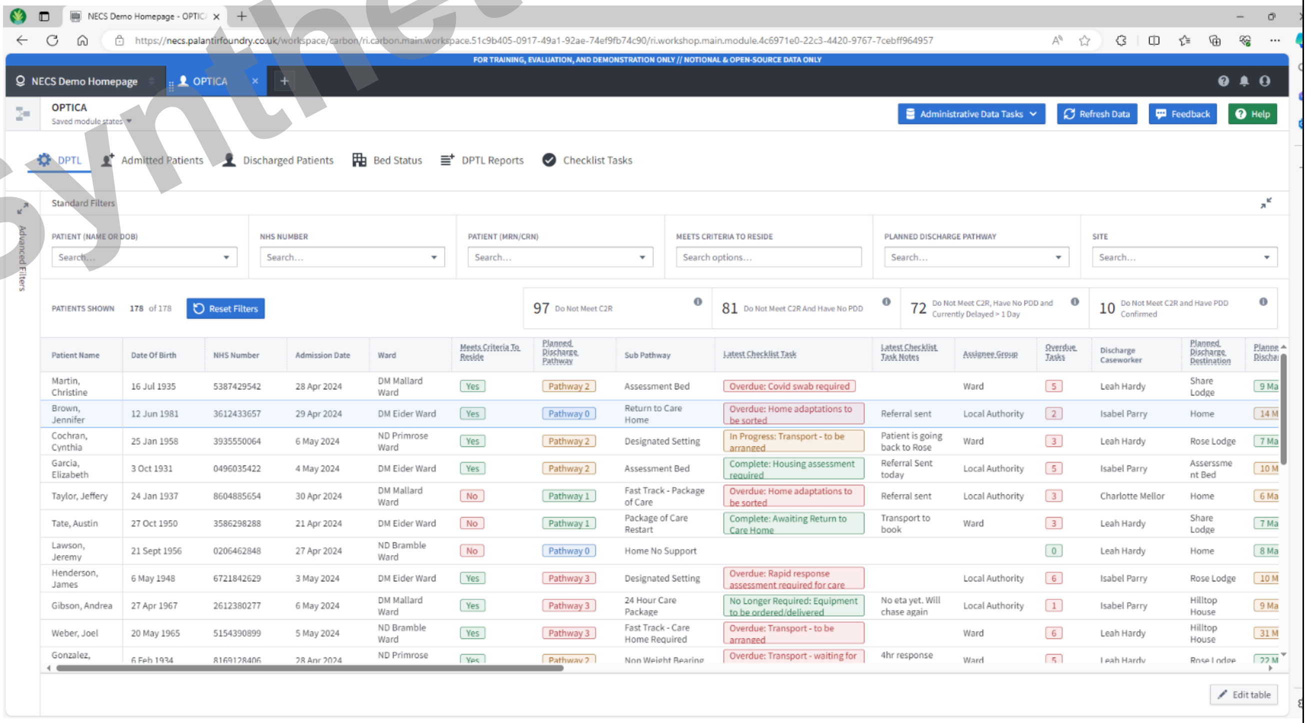
SITE
☐ NECS Memorial Hospital 4
☐ University of NECS 4

Core Beds	Additional Beds	Out Of Commission Beds	Total Useable Beds	Current Beds Occupied	Available Beds	Occupancy Rate
199	0	1	198	188	10	94.9%

Patients With Expected Discharge Date (EDD) Today	Patients With Planned Discharge Date (PDD) Today	Patients With Confirmed Planned Discharge Date (PDD)	Patients With Unconfirmed Planned Discharge Date (PDD)	Total Number Of Patients Already Discharged Today
3	3	17	26	0

Bed Status by Ward

Ward	Ward Specialty	Core Beds	Additional Beds	Out Of Commission Beds	Total Useable Beds	Current Beds Occupied	Available Beds	Occupancy Rate	Patients That Don't Meet C2R	Confirmed To Be Discharged today	Confirmed Discharges Today From Start Time	Unconfirmed Discharges Today	Estima Discha Tomor
DM Eider Ward	Maternity	30	0	0	30	28	2	93%	15	0	0	0	1
DM Gadwall Ward	Maternity	29	0	1	28	27	1	96%	11	0	0	0	2
DM Mallard Ward	Maternity	30	0	0	30	27	3	90%	13	0	0	1	4
DM Pintail Ward	Maternity	30	0	0	30	30	0	100%	20	0	0	0	2
ND Bluebell Ward	Oncology	20	0	0	20	19	1	95%	10	0	0	0	0
ND Bramble Ward	Oncology	20	0	0	20	17	3	85%	5	0	0	1	1
ND Primrose Ward	Oncology	20	0	0	20	20	0	100%	11	0	0	1	1
ND Speedwell Ward	Oncology	20	0	0	20	20	0	100%	12	0	0	0	1


NECS Demo Homepage - OPTIC
https://necs.palantirfoundry.co.uk/workspace/carbon/ri.carbon.main.workspace.51c9b405-0917-49a1-92ae-74ef9fb74c90/ri.workshop.main.module.4c6971e0-22c3-4420-9767-7cebff964957
FOR TRAINING, EVALUATION, AND DEMONSTRATION ONLY // NOTIONAL & OPEN-SOURCE DATA ONLY
NECS Demo Homepage
OPTICA
OPTICA
Saved module states
Administrative Data Tasks
Refresh Data
Feedback
Help
DPTL
Admitted Patients
Discharged Patients
Bed Status
DPTL Reports
Checklist Tasks
Standard Filters
Advanced Filters
Reset Filters
Edit table

PATIENT (NAME OR DOB)	NHS NUMBER	PATIENT (MRN/CRN)	MEETS CRITERIA TO RESIDE	PLANNED DISCHARGE PATHWAY	SITE
Search...	Search...	Search...	Search options...	Search...	Search...

PATIENTS SHOWN 178 of 178

97 Do Not Meet C2R

81 Do Not Meet C2R And Have No PDD

72 Do Not Meet C2R, Have No PDD and Currently Delayed > 1 Day

10 Do Not Meet C2R and Have PDD Confirmed

Patient Name	Date Of Birth	NHS Number	Admission Date	Ward	Meets Criteria To Reside	Planned Discharge Pathway	Sub Pathway	Latest Checklist Task	Latest Checklist Task Notes	Assignee Group	Overdue Tasks	Discharge Caseworker	Planned Discharge Destination	Planne Discha
Martin, Christine	16 Jul 1935	5387429542	28 Apr 2024	DM Mallard Ward	Yes	Pathway 2	Assessment Bed	Overdue: Covid swab required		Ward	5	Leah Hardy	Share Lodge	9 Ma
Brown, Jennifer	12 Jun 1981	3612433657	29 Apr 2024	DM Eider Ward	Yes	Pathway 0	Return to Care Home	Overdue: Home adaptations to be sorted	Referral sent	Local Authority	2	Isabel Parry	Home	14 M
Cochran, Cynthia	25 Jan 1958	3935550064	6 May 2024	ND Primrose Ward	Yes	Pathway 2	Designated Setting	In Progress: Transport - to be arranged	Patient is going back to Rose	Ward	3	Leah Hardy	Rose Lodge	7 Ma
Garcia, Elizabeth	3 Oct 1931	0496035422	4 May 2024	DM Eider Ward	Yes	Pathway 2	Assessment Bed	Complete: Housing assessment required	Referral Sent today	Local Authority	5	Isabel Parry	Asserssment Bed	10 M
Taylor, Jeffery	24 Jan 1937	8604885654	30 Apr 2024	DM Mallard Ward	No	Pathway 1	Fast Track - Package of Care	Overdue: Home adaptations to be sorted	Referral sent	Local Authority	3	Charlotte Mellor	Home	6 Ma
Tate, Austin	27 Oct 1950	3586298288	21 Apr 2024	DM Eider Ward	No	Pathway 1	Package of Care Restart	Complete: Awaiting Return to Care Home	Transport to book	Ward	3	Leah Hardy	Share Lodge	7 Ma
Lawson, Jeremy	21 Sept 1956	0206462848	27 Apr 2024	ND Bramble Ward	No	Pathway 0	Home No Support				0	Leah Hardy	Home	8 Ma
Henderson, James	6 May 1948	6721842629	3 May 2024	DM Eider Ward	Yes	Pathway 3	Designated Setting	Overdue: Rapid response assessment required for care		Local Authority	6	Isabel Parry	Rose Lodge	10 M
Gibson, Andrea	27 Apr 1967	2612380277	6 May 2024	DM Mallard Ward	Yes	Pathway 3	24 Hour Care Package	No Longer Required: Equipment to be ordered/delivered	No eta yet. Will chase again	Local Authority	1	Isabel Parry	Hilltop House	9 Ma
Weber, Joel	20 May 1965	5154390899	5 May 2024	ND Bramble Ward	Yes	Pathway 3	Fast Track - Care Home Required	Overdue: Transport - to be arranged		Ward	6	Leah Hardy	Hilltop House	31 M
Gonzalez,	6 Feb 1934	8169128406	28 Apr 2024	ND Primrose	Yes	Pathway 2	Non Weight Bearing	Overdue: Transport - waiting for	4hr response	Ward	5	Leah Hardy	Rose Lodge	22 M

The screenshot above contains synthetic, notional data only. It is fictional data which does not relate to real people. The screenshot has been added to aid understanding of the Product

FDP Benefit Metrics Data

NHSE can be provided with FDP Benefit Metrics Data, as part of the Processing of Data within this Product. FDP Benefit Metrics Data is Aggregated Data or Operational Data about the use of the Product. Where agreed by the local FDP User Organisation, the FDP Benefit Metrics Data is sent from the FDP User Organisation's local Instance to NHSE's national Instance, where it is aggregated with FDP Benefits Data from other FDP User Organisations into an NHSE FDP Benefit Metrics Data dashboard to enable NHSE to evaluate the efficacy and use of the Product across all Instances.

5. Identification of risks

This section identifies inherent risks of your Data Processing and potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised Data, etc.

This section is used to detail the risks arising from the proposed Processing Data if there are no steps in place to mitigate the risks. The sections below will then set out the steps you will take to mitigate the risks followed by a second risk assessment which considers the residual risk once the mitigation steps are in place.

Risk No	**Describe source of the risk and nature of potential impact on individuals** *The highlighted text are the most identified risks in the programme. Please amend and delete as appropriate and add Product specific risks.*
1	There is a risk that Personal Data may be accidently misused by those with access.
2	There is a risk that Personal Data will be processed beyond the appropriate retention period.
3	There is a risk that insufficient organisational measures are in place to ensure appropriate security of the Personal Data (e.g. policies, procedures, disciplinary controls) in Trust and Non-Trust organisations.
4	There is a risk that insufficient technical measures are in place to ensure appropriate security of the Personal Data (e.g. encryption, access controls).
5	There is a risk that unique data is generated within OPTICA Acute which is then not shared back into the clinical systems
6	There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures.
7	There is a risk that Subject Access Requests will not include a search of FDP or the Product, preventing individuals from having access to all Personal Data held about them by the Trust.
8	There is a risk of failure to provide appropriate transparency information to the data subject by the Trust.

9	There is a risk that increased access to Special Category Personal Data is given to Trust and Non-Trust staff who would not normally access that Data within their role.
10	There is a risk that the platform becomes inaccessible to users which could cause delays in the management of patient care and availability of Data.
11	There is a risk that inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product.
12	There is a risk that users will attempt to access FDP and the Product from outside the UK, increasing the data security risk.
13	There is a risk that Trust and Non-Trust users will not have their permissions revoked when they leave their role/organisation.

6. Compliance with the Data Protection Principles - for Processing Personal Data only

Compliance with the Data Protection Principles in relation to the Processing of Personal Data, as set out in Article 5 of the UK General Data Protection Regulation, are addressed in this DPIA in the following sections:

Data Protection Principle	Section addressed in this DPIA
Lawfulness, fairness and transparency	Section 7 (Lawfulness); Section 8 (Fairness); Section 9 (Transparency) and 11 (Processors)
Purpose limitation	Section 4
Data minimisation	Section 10
Accuracy	Section 14
Storage limitation	Section 13
Integrity and confidentiality (security)	Section 12 & 16
Accountability	Accountability is addressed throughout the DPIA. In particular, section 2S includes approval of the residual risks by the Information Asset Owner and on behalf of the SIRO.

7. Describe the legal basis for the Processing (collection, analysis or disclosure) of Data?

Legal basis under UK GDPR & Data Protection Act 2018 (DPA 2018):

Article 6 – Personal Data
To be completed by the Controller – suggested legal basis below. If more than one, then explain what Processing activity or Data the legal basis applies to.

- Article 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller by virtue of the statutory functions referred to above (Public Task).

Article 9 – Special Category Personal Data

To be completed by the Controller – suggested legal basis below. If more than one, then explain what Processing activity or Data the legal basis applies to.

- Article 9 (2) (h) processing is necessary for medical diagnosis, the provision of health care, or the treatment or management of health care services and system (Health Care) plus Schedule 1, Part 1, Paragraph 2 '*Health or social care purposes'* of DPA 2018.

Common Law Duty of Confidentiality

To be completed by the Controller – suggested legal basis below based on Direct Care use only. If more than those below, then explain what Processing activity or Data the legal basis applies to.

- **Implied consent** – we are able to rely on implied consent to Process Confidential Patient Data in this Product as we are using the Confidential Patient Data for the provision of Direct Care to patients. We are also able to rely on implied consent to provide members of the Care Team outside of our organisation with access to the Product for the purposes of providing Direct Care to patients.
- **Not applicable -** The FDP Benefit Metrics Data shared with NHSE is Anonymous Aggregated or Operational Data and is not Confidential Patient Data.

8. Demonstrate the fairness of the Processing

Fairness means that we should handle Personal Data in ways that people would reasonably expect and not use it in ways that have an unjustified adverse impact on them.

The Product will have its own transparency information which sets out why the Processing is fair in what it is intended to achieve to improve the care of patients. Further information is set out in section 9 below.

Regarding the impact on individuals, the purpose of the Product is to bring together all of the information about the patients discharge in one place for the whole care team to organise the services required for a timely discharge which falls within the Care Co-ordination use case. The impact for individuals of us Processing this Personal Data is to make sure that patients are discharged from hospital as soon as possible ensuring that they have all the support, equipment and care they need.

9. What steps have you taken to ensure individuals are informed about the ways in which their Personal Data is being used?

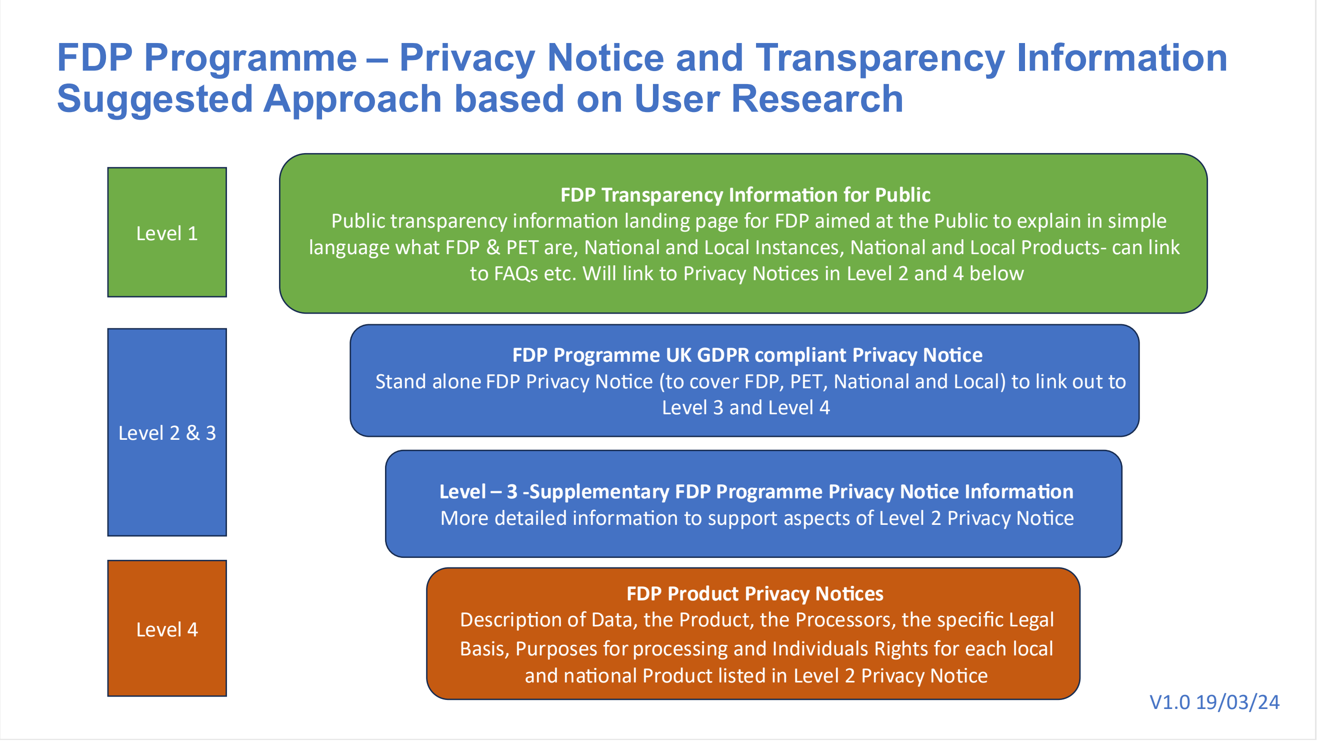
There is a range of information available on the NHS England website about FPD and how it works. This is Level 1 Transparency information.

There is a general FDP Privacy Notice which has been published via the NHS England webpages which also explains what FDP is and how it works in more detail. This is Level 2. It has a layered approach which has further detail in Level 3.

NHS England » NHS Federated Data Platform privacy notice

There is also a privacy notice specifically for this Product at Level 4 published on the NHSE website available via this link:

NHS England » FDP products and product privacy notices



FDP Programme – Privacy Notice and Transparency Information Suggested Approach based on User Research

Level 1

FDP Transparency Information for Public
Public transparency information landing page for FDP aimed at the Public to explain in simple language what FDP & PET are, National and Local Instances, National and Local Products- can link to FAQs etc. Will link to Privacy Notices in Level 2 and 4 below

Level 2 & 3

FDP Programme UK GDPR compliant Privacy Notice
Stand alone FDP Privacy Notice (to cover FDP, PET, National and Local) to link out to Level 3 and Level 4

Level – 3 -Supplementary FDP Programme Privacy Notice Information
More detailed information to support aspects of Level 2 Privacy Notice

Level 4

FDP Product Privacy Notices
Description of Data, the Product, the Processors, the specific Legal Basis, Purposes for processing and Individuals Rights for each local and national Product listed in Level 2 Privacy Notice

V1.0 19/03/24

Trust Specific Transparency Information

In addition to the above, we have also published the following information about FDP and the Product on our website:

[Insert links to additional local privacy information]

There is a specific OPTICA Acute privacy notice in place to inform patients of the nature of processing including the organisations roles which is available on the Trust's website here [*add link]*

10. Is it necessary to collect and process all Data items?

Data Categories [*Information relating to the individual's*]	**Yes/No**	**Justify** *[there must be justification for Processing the Data items. Consider which items you could remove, without compromising the purpose for Processing]*
Personal Data		
Name	Yes	Directly Identifiable Personal Data is required to provide Direct Care to patients.
Address	Yes	This Data is required to contact patients
Postcode	Yes	This Data is required to contact patients
Date of Birth	Yes	This Data is required to provide Direct Care to patients, as well as Data verification.
Age	Yes	This Data is required to provide Direct Care to patients.
Sex	Yes	This Data is required to provide Direct Care to patients.
Marital Status	No	
Gender	Yes	This Data is required to provide Direct Care to patients.
Living Habits	Yes	Information relating to living arrangements, type of accommodation, cohabitation in to ensure that the right support is provided on discharge
Professional Training / Awards / Education	No	
Email Address - Patient	No	
Email Address - Staff	Yes	This Data is required to allow staff access onto the systems
Physical Description	No	
General Identifier e.g. NHS No	Yes	NHS Number to enable information to be matched to the correct patient and their record. Also, local system identifier number to enable information to be matched to the correct patient and their record in local systems
Home Phone Number	No	
Online Identifier e.g. IP Address/Event Logs	No	
Mobile Phone No – Patient	No	
Mobile Phone / Device No / IMEI No - Staff	No	
Location Data (Travel / GPS / GSM Data)	No	
Device MAC Address (Wireless Network Interface)	No	
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	Patients diagnosis, test results, medications required on discharge , frailty status which are all required to ensure the correct discharge pathway is used. This information is required to provide Direct Care to patients
Sexual Life / Orientation	No	
Religion or Other Beliefs	No	
Racial / Ethnic Origin	No	
Biometric Data (Fingerprints / Facial Recognition)	No	
Genetic Data	No	
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences	No	

Please see the detailed Data Specification below which identifies the source Datasets and specific Data items for this Product.

- Data specification

11. Provide details of Processors who are Processing Personal Data in relation to this Product

- The Platform Contractor is a Processor acting on behalf of the Trust as a Controller in relation to Processing Data held on the Platform, and which is used in the Product.
- NECS, as the organisation who created the Product, is a sub-processor acting on behalf of Palantir, for the purpose of implementation and ongoing product support.

- The Platform Contract includes the required Data Processing provisions in it which meet the requirements of UK GDPR. In addition, a separate Data Processing Annex providing specific Processing instructions to the Platform Contractor for this Product will be issued. A copy of this Data Processing Annex is attached here:

  [Insert copy of the Annex here once agreed]

- [*Insert any additional third-party processor. Identify who they are, what Data they are processor for, what Data Processing agreement is in place (attach a copy of it) to cover the Processing].*

12. Describe if Data is to be shared from the Product with other organisations and the arrangements in place for this

Users of the dashboard may include:

- Clinicians within the Trust who have access to Directly Identifiable Personal Data and who use the dashboard to arrange the patients discharge from the acute setting
- Members of the wider MDT who have access to Directly Identifiable Personal Data and who use the dashboard for to arrange the patients discharge from the acute setting.

Users of the OPTICA reports may include:

- Executive teams within the Trust receive Aggregated Data reports to identify potential missed opportunities
- Submission to NHSE as part of the statutory SitRep collection of Aggregated Data reports relating to inpatient populations. This report and data shared is outside of the Product and FDP.

NECS will be providing technical support to the use of the Product, as a sub Processor to Palantir. There is a Data Processing Agreement in place between Palantir and NECS to allow the Processing.

Access is granted by [*explain process*]

Access is reviewed by [*explain how, by who and how frequently*]

Access is revoked [*explain how, by who and triggers for this eg from HR systems*]

FDP Benefit Metrics Data

In addition, where the NHS Trust agrees to provide the Data, the FDP Benefit Metrics Data is shared from the local Instance to NHSE's national Instance to enable NHSE to understand the usage of the Product, track the benefits metrics and evaluate the efficacy and use of the Product across all Instances. This is Aggregated Data and Operational Data.

13. How long will the Data be retained?

The Data will be kept in line with the Trust's requirements for the purposes of using the Product in line with the NHS Records Management Code of Practice 2021. [*Explain how long this is for the data in question. Explain how this data will be reviewed and destroyed during the life of the contract and use of FDP*]

At the point that the Product is decommissioned, a further assessment will be undertaken to ascertain whether the Data can be destroyed, or a retention period agreed by the Trust in line with the NHS Records Management Code of Practice 2021.

It is the responsibility of the member of the MDT managing the patients discharge to ensure that data that is generated within OPTICA Acute is also captured within their organisations EPR.

14. How will you ensure Personal Data is accurate and if necessary, kept up to date

The Product will only collect a sub-set of Personal Data from source systems about inpatients to be discharged. The Product will not collect Personal Data directly from individuals. Please see the statement below for the description of ensuring the accuracy and up to date nature of information:

[Trust to provide details of how data accuracy is maintained. When inaccuracies are identified, what is the process for updating Data in the Product and reporting inaccuracies in source systems? What will be the protocol for ensuring that data corrections and updates are implemented in FDP and the Product?]

15. How are individuals made aware of their rights and what processes do you have in place to manage requests to exercise their rights?

General privacy information regarding the FDP is available in the FDP Privacy Notice on the NHSE website together with a Product specific Privacy Notice which sets out the rights which apply in relation to this Product.

The following rights under UK GDPR apply to the Processing of Personal Data within this Product:

- Right to be informed
- Right of access
- Right to rectify
- Right to object

We also have additional information about patients' rights and how to exercise them available on our website here:

[*Add link to any specific Trust Privacy Notices, including for FDP and this Product]*

Any requests to exercise these rights would be handled in accordance with our existing standard processes by [*insert details and how the risk of FDP and Products being missed is addressed]*

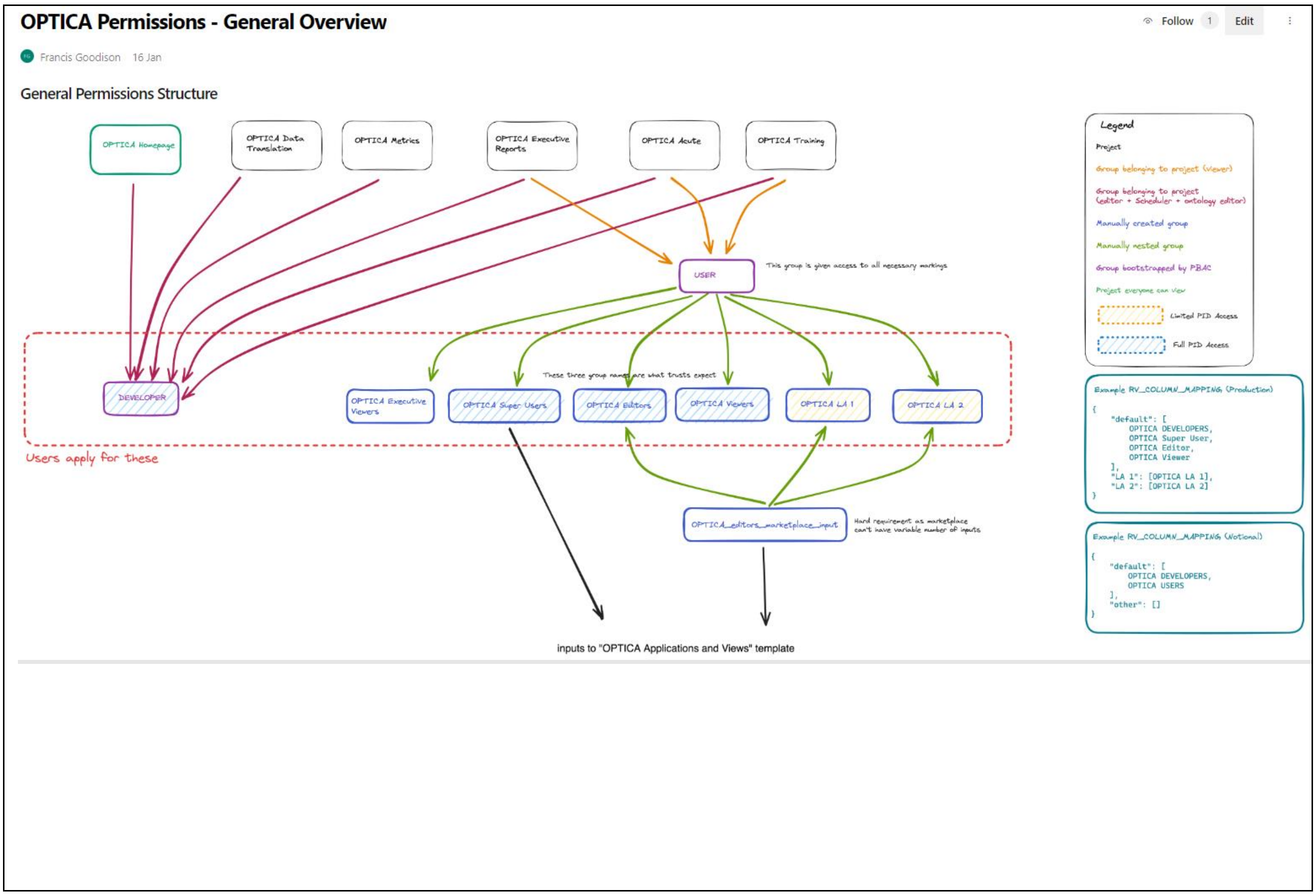
16. What technical and organisational controls in relation to information security have been put in place for this Product?

The Overarching FDP DPIA (and where applicable, NHS-PET DPIA) sets out the technical and organisational controls for the Platform and the NHS-PET Solution.

Business Continuity Plans
If OPTICA Acute became unavailable the Trust would revert to existing systems to ensure that timely discharge of patients continued, once OPTICA Acute was operational any information created would be manually input into OPTICA Acute.

Specific Access controls for this Product
OPTICA uses the Purpose-Bases Access Control (PBAC) capability within the FDP platform. The access to data within OPTICA is governed based on the locally configured Permissions Matrix which allocates staff their purpose rather than their role within the organisation. The Product Owner within the Trust is responsible for allocating roles within the matrix to purpose permissions This enables greater sophistication of access rather than the use of role alone. OPTICA Acute PBAC allows the Trust to partition the platform into secure containers, which are then allocated in accordance with the agreed Permissions Matrix. Precisely which data enters the platform and is transferred between these containers can be carefully controlled to manage re-identification risks. The current PBAC group structure is illustrated below.

The IAO will be required to approve user access based on the Purpose Based Access Controls in place for the Product described above



OPTICA Permissions - General Overview

Francis Goodison 16 Jan

General Permissions Structure

Follow
1
Edit
OPTICA Homepage
OPTICA Data Translation
OPTICA Metrics
OPTICA Executive Reports
OPTICA Acute
OPTICA Training
USER
This group is given access to all necessary markings
DEVELOPER
These three group names are what trusts expect
OPTICA Executive Viewers
OPTICA Super Users
OPTICA Editors
OPTICA Viewers
OPTICA LA 1
OPTICA LA 2
Users apply for these
OPTICA_editors_marketplace_input
Hard requirement as marketplace can't have variable number of inputs
inputs to "OPTICA Applications and Views" template
Legend
Project
Group belonging to project (viewer)
Group belonging to project (editor + Scheduler + ontology editor)
Manually created group
Manually nested group
Group bootstrapped by PBAC
Project everyone can view
Limited PID Access
Full PID Access

Example RV_COLUMN_MAPPING (Production)

```
{
    "default": [
        OPTICA DEVELOPERS,
        OPTICA Super User,
        OPTICA Editor,
        OPTICA Viewer
    ],
    "LA 1": [OPTICA LA 1],
    "LA 2": [OPTICA LA 2]
}
```

Example RV_COLUMN_MAPPING (Notional)

```
{
    "default": [
        OPTICA DEVELOPERS,
        OPTICA USERS
    ],
    "other": []
}
```

17. In which country/territory will Data be stored or processed?

All Processing of Data will be within the UK only, this is a contractual requirement and one of the key principles of the FDP IG Framework.

18. Do Opt Outs apply to the Processing?

The National Data Opt Out policy does not apply to this Product as the Confidential Patient Information Processed in this Product is used and shared for the purposes of the Direct Care of patients.

Type 1 Opt Outs do not apply to this Product because the Confidential Patient Information Processed in this Product is used and shared for the Purposes of the Direct Care of patients.

19. Risk mitigations and residual risks

Section 4 of this DPIA sets out the inherent risks arising from the proposed Data Processing. This section summarises the steps to mitigate those risks (which are explained in detail above) and assesses the residual risks, i.e. the level of risk which remains once the mitigations are in place.

Against each risk you have identified at section 4, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
1	Personal Data may be accidently misused by those with access	1. External suppliers are Processors on contracts with relevant security and data protection clauses contained within the agreements. Internal security and data protection processes are in place within the Trust 2. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Personal Data to only those with a legitimate need eg [relevant members of the Multi-Disciplinary Care Team]. 3. The FDP access audit logs ensure that all access is logged and can be fully audited. FDP audit logs enable sophisticated searching against agreed criteria in response	Section 12 & 16	Tolerate	Remote	Significant	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
2	Personal Data may be processed beyond the appropriate retention period.	1.Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place. 2. [*Explain what steps are taken as per section 13 to review and delete information that is no longer required].*	Section 13	Tolerate	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the Personal Data (e.g. policies, procedures, disciplinary controls) in Trust and Non-Trust organisations.	[1.Appropriate organisational measures in relation to Data controls and governance are in place to ensure the security of the Data. Additional local SOPs are in place to ensure that all existing policies are underpinned by new SOPs relating to the FDP Instance, including but not limited to SAR searches; and data breach management. This should include specific training for Trust and Non-Trust staff members when being provided with access to the Product. 2. Organisational measures are adhered to across the Data platform. Any breaches are reported in line with these. 3. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Data.]	Set out in the Overarching FDP DPIA and Section 12 & 16 above	Tolerate	Remote	Minimal	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
4	Insufficient technical measures are in place to ensure appropriate security of the Personal Data (e.g. encryption, access controls)	1. Data is encrypted in storage 2. All Data to and from the platform is encrypted in transit using at least TLS1.2 3. SLSP in place *[4. Any additional Product specific measures]*	Set out in the Overarching FDP DPIA and Section 12 & 16 above	Tolerate	Remote	Minimal	Low
5	There is a risk that unique data is generated within OPTICA Acute which is then not shared back into the clinical systems	Members of the MDT creating unique data within OPTICA Acute are responsible for ensuring this data is also catalogued in their EPR Training will be provided by the OPTICA Acute team to ensure this takes place	Section 13	Tolerate	Possible	Significant	Medium
6.	There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures	1. Details are described in the Overarching FDP DPIA. [2. For local Products migrating from Foundry to FDP, there is no change in the Product, its operation or the technical measures supporting it. New governance processes for migrating existing Products have been put in place, including approval of relevant DPIAs by the DGG. This updated DPIA has also been put in place to assess	Set out in the Overarching FDP DPIA and Section 3, 12 & 16 above	Tolerate	Remote	Minimal	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
		the risks consistently with other local users of the Product.] 3. [*Insert details of any local testing of Products carried out before they go live, including interface with local SOPs*]]					
7	There is a risk that Subject Access Requests will not include a search of FDP preventing individuals from having access to all data held about them by the Trust	[1. IG and Medical Records teams responsible for coordinating SAR responses need appropriate levels of access through the Role Based and Purpose Based Access Controls/Permissions Matrix]; [2. Existing SOPs relating to clinical system searches in response to SARs have been revised to include FDP and the Products sitting within the Trust's local Instance of the platform.] [3. There is no additional Personal Data in the Product that is not contained within Trust source IT systems which would already be searched in response to a SAR].	Section 15	Treat	Remote	Minimal	Low
8	There is a risk of failure to provide adequate transparency information to	1. We have reviewed the Trust Privacy Notice and added additional text required for the Processing of Personal Data in this Product. 2. We have ensured that the NHSE General FDP and Product Privacy Notices [have been published	Sections 8 and 9	Tolerate	Remote	Significant	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
	the data subject by the Trust	alongside Trust's Privacy Notices/have been linked to from the Trust's Privacy Notices to the NHSE website].					
9	There is a risk that increased access to Special Category Personal Data is given to Trust and Non-Trust staff who would not normally access that data within their role.	1. Role Based and Purpose Based Access Controls are in place. The addition of the Restricted View function to sit over the Purpose Based Access Controls ensures only those who need access to Special Category Personal Data are able to access this.	Section 12 & 16	Treat	Possible	Minimal	Low
10	There is a risk that the platform becomes inaccessible to users which could cause delays in the management of patient care and availability of Data.	1. The FDP Contractor is required to have Business Continuity Plans in place. 2. [The Trust has Business Continuity Plans in place which cover the inaccessibility/unavailability of the Product].	Section 16	Tolerate	Remote	Significant	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
11	[There is a risk that inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product.]	[1. The Product will only collect a sub-set of Personal Data from existing Trust patient record systems. The Product will not collect Personal Data directly from individuals.] [2. It is our responsibility to ensure that all Data that is ingested into FDP for use in this Product is up to date and accurate for the purposes for which it is Processed within the Product. We will use our existing processes relating to the source patient record systems for maintaining accuracy].	Section 14	Tolerate	Remote	Significant	Low
12	There is a risk that users will attempt to access FDP and the Product from outside the UK, increasing the data security risk.	1. It is clearly articulated within the FDP IG Framework that no personal/patient data should leave the UK without the express prior approval from the Data Governance Group.	Section 17	Treat	Remote	Significant	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
		2. It is within the contract that no access to the system should take place from outside the UK. 3. There are technical security measures in place to prevent access from outside the UK.					
13	[There is a risk that Trust and Non-Trust users will not have their permissions revoked when they leave their role/organisation.]	1. [*Insert details of local policy/process on migration and ongoing process or refer to Section 12 where this is set out]*	Section 12 & 16	Treat	Remote	Significant	Low

20. Actions

This section draws together all the actions that need to be taken in order to implement the risk mitigation steps that have been identified above, or any other actions required.

Action No	**Actions required.** (Date and responsibility for completion)	**Risk No impacted by action**	**Action owner** (Name and role)	**Date to be completed**
1	[Ongoing review of unsuppressed Data to ensure it remains Anonymous Aggregated Data or Operational Data when any new Data items are added to the Product, or when any changes are made the dashboard visualisations and reports].	[6]	*[Insert name of IAO/Product owner]*	[Ongoing at each change of the Product and update to this DPIA]
2	[*Trusts to add any actions required to produce information to supplement/update the DPIA or further mitigate risks]*	*[Identify]*	*[Insert name of IAO/Product owner]*	*[Insert date]*
3	*The Trust must ensure that Information Sharing Agreements with Local Authorities are implemented prior to access being granted*	*[Identify]*	*[Insert name of IAO/Product owner]*	*[Insert date]*

21.Completion and signatories

The completed DPIA should be submitted to the [Data Protection Officer/Information Governance Team] via [*add email address*](for review).

The IAO (Information Asset Owner) should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the Processing, including new Data items Processed, change of purpose, and/or system changes)

The DPIA accurately reflects the Processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Name	
Signature	
Date	

FOR [DATA PROTECTION OFFICER] USE ONLY

22. Summary of high residual risks

Risk no.	High residual risk summary

Summary of Data Protection Officer advice:

Name	
Signature	
Date	
Advice	

Where applicable: ICO (Information Commissioners Office) consultation outcome:

Name	
Signature	
Date	
Consultation outcome	

Next Steps:

- **DPO to inform stakeholders of ICO consultation outcome**
- **IAO along with DPO and SIRO (Senior Information Risk Owner) to build action plan to align the Processing to ICO's decision**

Annex 1: Defined terms and meaning

The following terms which may be used in this Document have the following meaning:

Defined Term	Meaning
Aggregated Data	Counts of Data presented as statistics so that Data cannot directly or indirectly identify an individual.
Anonymisation	Anonymisation involves the application of one or more anonymisation techniques to Personal Data. When done effectively, the anonymised information cannot be used by the user or recipient to identify an individual either directly or indirectly, taking into account all the means reasonably likely to be used by them. This is otherwise known as a state of being rendered anonymous in the hands of the user or recipient.
Anonymised Data	Personal Data that has undergone Anonymisation.
Anonymous Data	Anonymised Data, Aggregated Data and Operational Data.
Approved Use Cases	Means one of the five initial broad purposes for which Products in the Data Platform can be used as outlined in Part 1 of Schedule 2 (Approved Use Cases and Products) of the IG Framework, or any subsequent broad purpose agreed to be a use case through the Data Governance Group
Categorisation of Data	Means one of the following categories of Data: • Directly Identifiable Personal Data • Pseudonymised Data • Anonymised Data, • Aggregated Data • Operational Data In the case of Directly Identifiable Personal Data or Pseudonymised Data this could be Personal Data or Special Category Personal Data.
Common Law Duty of Confidentiality	The common law duty which arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
Confidential Patient Data	Information about a patient which has been provided in circumstances where it is reasonable to expect that the information will be held in confidence, including Confidential Patient Information.

Defined Term	Meaning
Confidential Patient Information	Has the meaning given in section 251(10) and (11) of the NHS Act 2006. See Appendix 6 of the National Data Opt Out Operational Policy Guidance for more information[1]
Controller	Has the meaning given in UK GDPR being the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (subject to Section 6 of the Data Protection Act 2018)
Data Governance Group	Means a national group established by NHS England to provide oversight to the approach to Data Processing and sharing across all Instances of the Data Platform and NHS-PET which will include membership from across FDP User Organisations
Data Platform or Platform	The NHS Federated Data Platform
Data Processing Annex	The annex to the schedule containing Processing instructions in the form set out in the FDP Contracts.
Data Protection Legislation	The Data Protection Act 2018, UK GDPR as defined in and read in accordance with that Act, and all applicable data protection and privacy legislation, guidance, and codes of practice in force from time to time
Direct Care	A clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care[2].
Directly Identifiable Personal Data	Personal Data that can directly identify an individual.
DPIA(s)	Data Protection Impact Assessments in a form that meets the requirements of UK GDPR
FDP	Federated Data Platform
FDP Contract	The NHS-PET Contract and the Platform Contract
FDP Contractor(s)	The NHS-PET Contractor and/or the Platform Contractor

[1] https://digital.nhs.uk/services/national-Data-opt-out/operational-policy-guidance-document/appendix-6-confidential-patient-information-cpi-definition

[2] See the National Data Guardian Direct Care Decision Support Tool: https://assets.publishing.service.gov.uk/media/5f2838d7d3bf7f1b1ea28d34/Direct_care_decision_support_tool.xlsx

Defined Term	Meaning
FDP Programme	The NHS England Programme responsible for the procurement and implementation of the FDP across the NHS
FDP User Organisations	NHS England, ICBs, NHS Trusts and other NHS Bodies (including a Commissioned Health Service Organisation) who wish to have an Instance of the Data Platform and who have entered into an MoU with NHS England. In the case of a Commissioned Health Service Organisation, the MoU is also to be entered into by the relevant NHS Body who has commissioned it
General FDP Privacy Notice	A privacy notice providing information on the Personal Data Processed in the Data Platform and by NHS-PET generally, including the Approved Use Cases for which Products will Process Personal Data
ICB	Integrated Care Board
ICS	Integrated Care System
Incident	An actual or suspected Security Breach or Data Loss Incident
Instance	A separate instance or instances of the Data Platform deployed into the technology infrastructure of an individual FDP User Organisation
National Data Opt Out	The Department of Health and Social Care's policy on the National Data Opt Out which applies to the use and disclosure of Confidential Patient Information for purposes beyond individual care across the health and adult social care system in England. See the National Data Opt Out Overview[3] and Operational Policy Guidance for more information[4]
NHS-PET Contract	The Contract between NHS England and the NHS-PET Contractor relating to the NHS-PET Solution dated 28 November 2023 as may be amended from time to time in accordance with its terms
NHS-PET Contractor	IQVIA Ltd
NHS-PET Solution	The privacy enhancing technology solution which records Data flows into the Data Platform and where required treats Data flows to de-identify them.
Ontology	Is a layer that sits on top of the digital assets (Datasets and models). The Ontology creates a complete picture by mapping Datasets and models used in Products to object types, properties, link types, and action types. The Ontology

[3] https://digital.nhs.uk/services/national-Data-opt-out/understanding-the-national-Data-opt-out

[4] https://digital.nhs.uk/services/national-Data-opt-out/operational-policy-guidance-document

Defined Term	Meaning
	creates a real-life representation of Data, linking activity to places and to people.
Operational Data	Items of operational Data that do not relate to individuals eg stocks of medical supplies.
Personal Data	Has the meaning given in UK GDPR being any information relating to an identified or identifiable natural person (‘Data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . For the purposes of this DPIA this also includes information relating to deceased patients or service users. Personal Data can be Directly Identifiable Personal Data or Pseudonymised Data.
Personal Data Breach	Has the meaning given in UK GDPR being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed
Platform Contract	The agreement between NHS England and the Platform Contractor in relation to the Data Platform dated 21 November 2023 as may be amended from time to time in accordance with its terms
Platform Contractor	Palantir Technologies UK Ltd
Product	A product providing specific functionality enabling a solution to a business problem of an FDP User Organisation operating on the Data Platform.
Product Privacy Notice	A privacy notice providing information on the Personal Data Processed in the Data Platform and by NHS-PET in relation to each Product, including the purposes for which the Product Processes Personal Data
Process or Processing	Has the meaning given in UK GDPR being any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction
Processor	Has the meaning given in UK GDPR being a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller
Programme	The Programme to implement the Data Platform and NHS-PET across NHS England, NHS Trusts and ICBs

Defined Term	Meaning
Pseudonymisation	Has the meaning given in UK GDPR being the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person
Pseudonymised Data	Personal Data that has undergone Pseudonymisation
Purpose Based Access Controls or PBAC	Means user access to Data is based on the purpose for which an individual needs to use Data rather than their role alone as described more fully in Part 2 of Schedule 3
Role Based Access Controls or RBAC	Means user access is restricted to systems or Data based on their role within an organisation. The individual's role will determine what they can access as well as permission and privileges they will be granted as described more fully in Part 2 of Schedule 3
Special Category Personal Data	Means the special categories of Personal Data defined in Article 9(1) of UK GDPR being Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic Data, biometric Data for the purpose of uniquely identifying a natural person, Data concerning health or Data concerning a natural person's sex life or sexual orientation.
Transition Phase	Is the first phase of rolling out the Data Platform which involves NHS England and local FDP User Organisations who currently use Products, moving their existing Products onto the new version of the software that is in the Data Platform. There is no change to the Data that is being processed, the purposes for which it is processed or the FDP User Organisations who are Processing the Data during the Transition Phase. The Transition Phase will start in March 2024 and is expected to run until May 2024.
UK GDPR	UK GDPR as defined in and read in accordance with the Data Protection Act 2018