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	Transport Cancellation – FDP Local DPIA		
Directorate / Programme	FDP Programme	Product Name	*Transport Cancellation*
Document Reference No	*FDP 099L*	Information Asset Register Number	*[Insert]*
Information Asset / Product Owner Name	*[Insert]*	Version	1.0 Final Approved
Author(s)	[redacted]	Version issue date	*13/12/2024*

Redaction Rationale – *The information above 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 – Transport Cancellation

Document Management

Revision History

Version	Date	Summary of Changes
0.1	04/11/2024	Information added to DPIA
0.2	12/11/2024	Further update
0.3	25/11/2024	Review and update
0.4	26/11/2024	Further update
0.5	27/11/2024	Review and final updates
0.6	27/11/2024	Clean version for DGG review
0.7	04/12/2024	DGG Comments
0.8	10/12/2024	Update to DPIA
0.9	11/12/2024	Clean version
0.10	13/12/2024	Review and minor amendment with NHS E Review
1.0	13/12/2024	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
[redacted]	Deputy Director, IG Risk and Assurance	13/12/2024	V0.9

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
[redacted]	Deputy Director, IG Risk and Assurance	13/12/2024	V0.9

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.

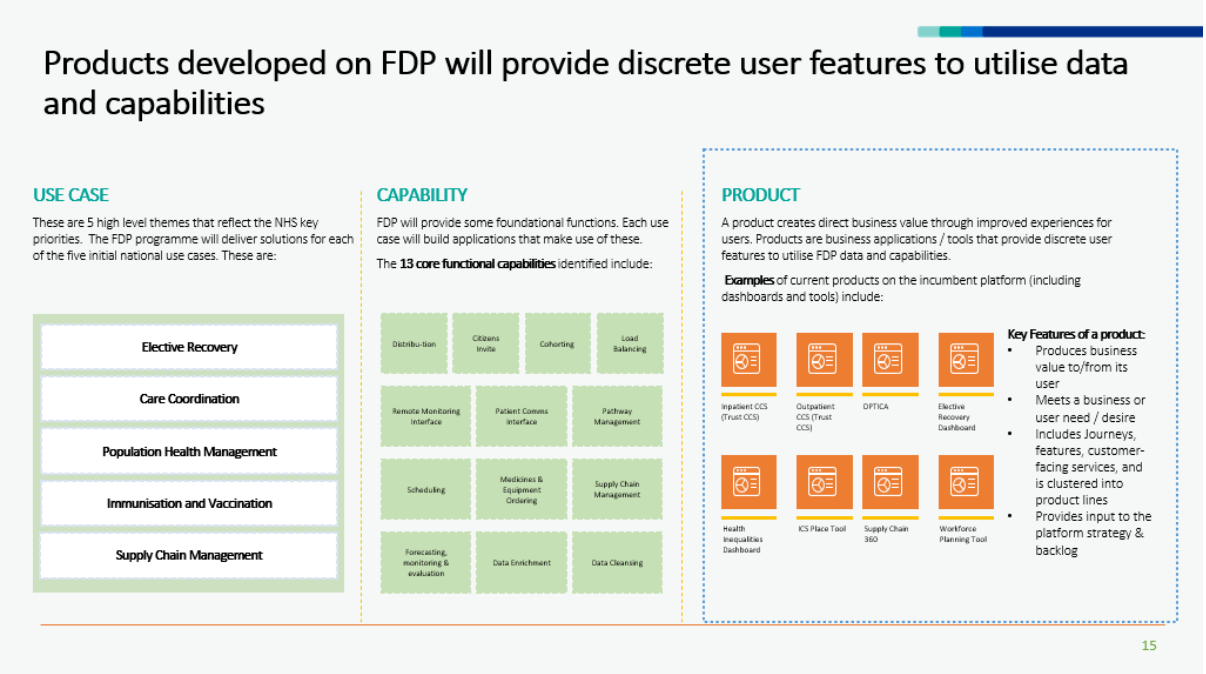
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

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.



Key information about the Product

Purpose of the Product - Overview

The Transport Cancellation Product (the Product) was originally an ‘Incubator Site’ Product. An Incubator Site is a test site used to innovate and create new Products and where programme support is provided from NHS England and from the Suppliers. This product is now being rolled out further across the FDP to other user organisations and consequently this DPIA is being uplifted to reflect the wider roll-out. The Product was initially designed to be used by administrative staff at CWFT.

This is now being rolled out as a wider pilot to North West London Trusts. A further update will be required to this DPIA prior to being available for Trusts outside this pilot area. This will be implemented on each Trusts instance of FDP, there is no sharing between Trusts.

It provides a list of patients who have upcoming appointments and have booked transport, along with the patient's contact information and transport details. The main feature of this Product is displaying flags for appointments that may require transport cancellation due to the patient being an inpatient or deceased, or the appointment being cancelled or rescheduled.

Data provided to users:

- Patient demographics: Name, NHS number
- Appointment details: Date, time, location, status (cancelled, rescheduled)
- Transport details: Date, time, pick-up/drop-off location
- Inpatient/deceased status (if applicable)

What this enables users to do:

- Quickly identify appointments with booked transport that need to be cancelled due to appointment cancellation or rescheduling.
- Easily validate the need for transport with patients who have upcoming appointments.
- Reduce the number of aborted transport journeys, leading to cost savings for the NHS.
- Improve efficiency for administrative staff by streamlining the process of managing transport cancellations.

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 ingested into the Product to create the Product For Data displayed or shared with users of the Product
Pseudonymised Data	☐	

Anonymised Data	☐	
Aggregated Data	☐	
Operational Data	☒	For Data ingested into the FDP to create the Product For Data ingested into the Product to create the Product For Data displayed or shared with users of the Product
Type of Data used in the Product		
No Personal Data	☐	
Personal Data	☒	For Data ingested into the FDP to create the Product For Data ingested into the Product 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 ingested into the Product 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.

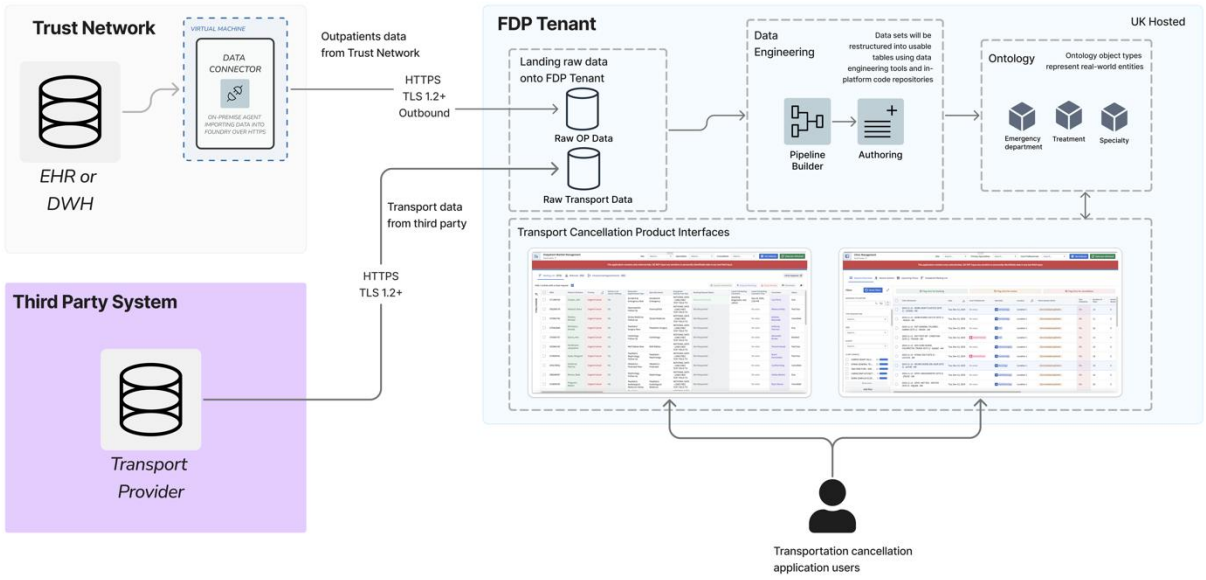
NHS Trusts and ICBs who use the Products made available to them are responsible for adopting and updating the template local Product DPIA or producing their own DPIA to reflect their specific use of the Product and to assess any specific risks relating to their organisation's use of the Product.

1. Consultation with Stakeholders about the Product

The Key Stakeholders for this product include senior representatives from operational teams involved in management of patient transport and they continue to be pivotal in the design and initial rollout of this Product.

As this Product is currently in an early stage of development, there has not yet been any consultation with the public. When appropriate, the project team will engage with the public at later stages of the product lifecycle.

2. Data Flow Diagram



When Data is ingested into FDP, PET registers the Data, this does not include any Personal Identifiable Data it is simply Metadata.

All processing within the “Trust FDP Tenant” will be handled by both Palantir engineers and Chelsea and Westminster Hospital NHS Foundation Trust engineers.

The organisations mentioned above are both acting as Processors.

The “third party system” is the Trust’s transport provider.

3. Description of the Processing

There are two main data flows:

1. A flow of patient demographic, speciality, and appointment information on outpatients and inpatients from Trust's Data Warehouse or directly from their EHR to FDP.
2. A flow of information about booked transport directly from the Trust provider for non-emergency patient transport.

Data is combined to identify changes that need to be made to non-emergency patient transport due to changes in the status of a patient or their appointment. Administrative

and operational staff use the worklists generated by the tool to review transport bookings that may need to be amended, and track actions related to those reviews and requested changes.

Two types of administrative information are recorded in the Product:

- Create and amend actions – this includes creation and modification of requests to cancel, modify and create transport bookings.
- Comments related to administrative actions – a manual review of the status of each patient is performed before any changes are made to existing bookings. The output of these reviews is recorded in a short form comments field that is part of the form to request that changes to a booking are made.

Requests to create, cancel or amend individual bookings are made to the transport provider directly in their system separate from the Product in FDP (i.e. there is no automated egress of data from the Product to any other system). Additionally, the Product provides the ability to create a daily report that can be exported from the system and manually shared with the transport provider as part of the end-of-day communication between the Trust and the Provider.

All processing will be handled by both Palantir engineers and Chelsea and Westminster Hospital NHS Foundation Trust engineers with both organisations acting as Processors.

4. Purpose of Processing Personal Data for this Product

The key objectives of the Product and associated dashboards are to:

- Quickly identify appointments with booked transport that need to be cancelled due to appointment cancellation or rescheduling.
- Easily validate the need for transport with patients who have upcoming appointments.
- Reduce the number of aborted transport journeys, leading to cost savings for the NHS and a reduction in the Trust's carbon footprint.
- Improve efficiency for administrative staff by streamlining the process of managing transport cancellations.

The purpose of processing Directly Identifiable Personal Data is to support Direct Care. This Product allows the Trust to easily identify, monitor and resolve instances where the non-emergency transport booked to/from the Trust needs to be changed. The Product facilitates this process by providing:

- Worklists with journeys that needs to be reviewed
- The ability to raise/modify/close actions related to these worklists
- The ability to centrally record the evidence of manual reviews that have been carried out to confirm whether changes to transport are required
- The ability to export a list of journeys that need to be changed / cancelled
- The ability to monitor overall status of the worklists through dashboards.

No other data source within the Trust provides the capabilities outlined above. This visibility is critical for ensuring that patients are not unnecessarily transported to hospital and that the transport capacity is appropriately allocated to where it is needed.

The attached user guide provides a detailed walk-through of the functionality available in the Product and how it is used. This includes screenshots of the Product.

Transport Cancellation Handbook Screenshots

All screenshots within this document 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.

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).
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 insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures.
6	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.

7	There is a risk of failure to provide appropriate transparency information to the data subject by the Trust.
8	There is a risk that increased access to Special Category Personal Data is given to Trust staff who would not normally access that Data within their role.
9	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.
10	[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].
11	There is a risk that users will attempt to access FDP and the Product from outside the UK, increasing the data security risk.
12	There is a risk that users will not have their permissions revoked when they leave their role/organisation.
13	There is a risk that when upgrades to source systems are completed this does not sync with FDP

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 21 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 – examples 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 – examples 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 – examples below. If more than one, 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].
- Deceased Patient Data is processed to ensure the cancellation of patient transport preventing distress of relatives, if this transport was to attend the patient's property. There is a reasonable expectation of the individual when they were alive that their Data would be processed in this manner, this is supported by the continuation of their implied consent of the living patient that this would occur.

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 manage and the patients who have transport scheduled but may be an inpatient, deceased or their appointment has been cancelled or rescheduled, which falls within Care Co-ordination. The impact for individuals of us Processing this Data is ensuring that they have the appropriate transport at the appropriate time to ensure they attend the appointments scheduled. This in turn allows capacity for the transport provider.

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

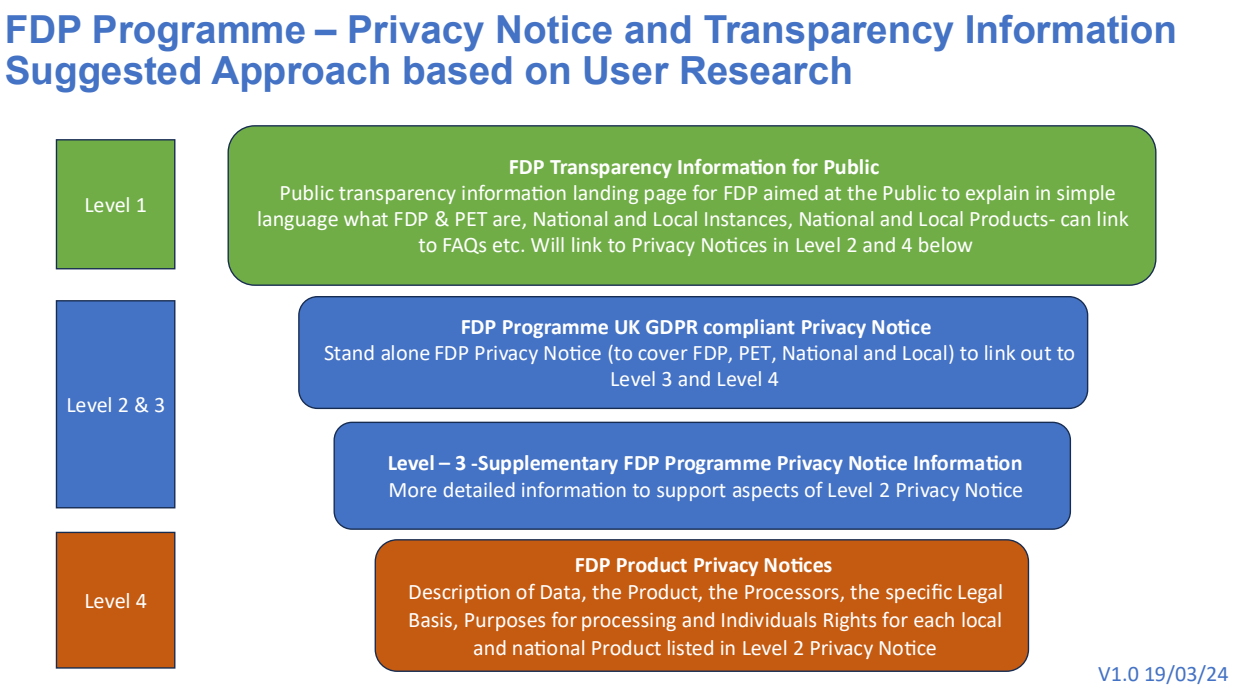
There is a range of information available on the NHS England website about FDP and how it works. This is Level 1 Transparency information.

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



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]

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 ensure correct journeys are being validated / amended
Postcode	Yes	This Data is required to ensure correct journeys are being validated / amended
Date of Birth	Yes	Directly Identifiable Personal Data is required to provide Direct Care to patients.
Age	Yes	Directly Identifiable Personal Data is required to provide Direct Care to patients. This is ingested by default through date of birth and is required as part of good clinical practice to prevent mistakes and correctly identify the correct patient.
Sex	Yes	Directly Identifiable Personal Data is required to provide Direct Care to patients.
Marital Status	No	
Gender	No	
Living Habits	No	
Professional Training / Awards / Education	No	
Email Address - Patient	No	
Email Address - Staff	Yes	This Data is required to allow staff access onto the systems and to record which staff members performed specific actions
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	Yes	To enable the patient to be contacted regarding transport.
Mobile Phone / Device No / IMEI No - Staff	No	
Location Data (Travel / GPS / GSM Data)	No	
Device MAC Address (Wireless Network Interface)	No	
Deceased individuals who have appointments booked.	Yes	This Data is ingested into FDP to detail the reason for appointment cancellation.
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	This specialty and appointment Data is ingested into FDP to support the decision making on how best to reschedule transport.
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:

Transport Cancellation Data Specifcation

Object 1 – Appointment with Transport

Description	Type	Primary Key / Title	Expected values
Title	string	Title	Patient Name | Appt type - Appt Date
NHS_number	string		
Age	String		
Date of Birth	String		
Sex	String		
Appointment_Type	string		
Priority	string		Routine; Urgent; Two-week wait
Appointment_Date_&_Time	timestamp		
Appointment_status	string		Booked; Cancelled; Rescheduled
Attendance_ID	string	PK	
Days_to_act	integer		
Reason_for_request	string		
Suggested_action	string		Check - Other booked appointment on that day; Reschedule both journeys; Check - Patient currently in hospital; Cancel both journeys
Inward_JourneyID	string		
Inward_AppointmentTime	string		
Inward_BookingStatus	string		Active; Cancelled; Aborted
Request_Status	string		
PLV_-Need_transport_val.	boolean		
PLV_-_Appt_confirmation	boolean		
PLV_-_Message_sent	boolean		
PLV_status	string		Reminder Sent - no response; Reminder sent - Partial response; Confirmed; Address needs changing; PLV - Transport not needed
Comment	string		

Cancel._Request_Status	string		No Request; Dismissed; Requested; Requested*
Pathway_ID	string		
Specialty	string		
Patient_Name	string		
Patient_ID	string		
date_time_cancelled	timestamp		
HospitalSite	string		CW; WMUH
IN_Bed_name	string		
IN_enc_type	string		
IN_specialty	string		
IN_anticipated_dx_date	date		
NextAppt_start_date_time	timestamp		
NextAppt_booking_status	string		
NextAppt_attendance_id	string		
deceased	boolean		
Outward_JourneyID	string		
Outward_AppointmentTime	string		
Outward_BookingStatus	string		Active; Cancelled; Aborted
Count_Appt	integer		
Booked_Appt_on_same_day	integer		
Attendance_ID_bis	string		

Object 2 – Transport Journey

Description	Type	Primary Key / Title	Expected values
journey_id	string	PK	
attendance_ids	array		
canc_request_status	string		Not Requested, Requested, Cancelled
direction	string		
drop_off_address	string		
drop_off_postcode	string		
hats_status	string		Active, Cancelled, Aborted
initials	string		

nhs_number	string	
patient_id	string	
pick_up_address	string	
pick_up_postcode	string	
pick_up_time	string	
title	string	Title

Object 3 – Transport cancel request log

Description	Type	Primary Key / Title	Expected values
request_id	string	PK	
action_type	string		Cancel, Reschedule, Check
appointment_time	timestamp		
attendance_id	array		
attendance_id_1	string		
comment_evidence	string		
expected_hats_status	string		Active, Aborted, Cancelled
journey_id	string		
latest_hats_journey_id_hats_status	string		Active, Aborted, Cancelled
nhs_number	string		
pick_up_planned_time	timestamp		
request_status	string		Updated in HATS, Requested to HATS, Dismissed, Not requested to HATS
request_timestamp	timestamp		
requested_by	string		
rescheduled_appointment_date	timestamp		
resolved_by	string		
resolved_timestamp	timestamp		
title	string	Title	
updated_in_pas	boolean		

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. The Platform Contract has 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 FDP Annex here once agreed]

Chelsea and Westminster NHS Foundation Trust (CWFT) will also act as a processor for this product. Each Trust that takes this product onto their own FDP instance, will need to have a separate Data Processing Agreement between the Trust and CWFT. This is in addition to the FDP Annex which instructs Palantir to Process Data on behalf of the Trust. *[Insert reference to CWFT DPA].*

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:

- Administrative staff who have access to Personal Data and who use the Product to ensure non-emergency patient transport is correctly booked (and cancelled where it is not needed)
- Managerial staff who produce lists of booked journeys that need to be amended or cancelled. These lists are exported from the tool and shared with the non-emergency transport provider.

Access is granted by [*explain process*]

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

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

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.

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

The information that is collected solely in this Product is Directly Identifiable Personal Data to support clinical pathway management, all Data is maintained within the source systems. This Product is used in regular status meetings to review transport scheduled for patients who may now be an inpatient, deceased or have their appointment cancelled or rescheduled, by virtue of this use, the necessary levels of Data accuracy in the system are maintained.

All Data is collected and recorded in source systems and is kept up to date via the processes used to maintain Data accuracy in those systems.

Any updates or amendments to Data are feedback into the clinical record system of the Trust and amended on FDP.

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 where appliable, the NHS-PET Solution).

Business Continuity Plans
[If the Product is unavailable, provide a description of the criticality of this on patient care/service and local arrangements for accessing Data by other means if required].

[Specific Access controls for this Product

Provide details of different views applicable to different users. How users are authenticated etc]

The IAO will be required to approve user access based on the Purpose Based Access Controls in place for the Product [*described here: [insert where available – otherwise add as an Action to the DPIA to be produced and inserted]*

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 not derived from GP Data.

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)	[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. 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
4	Insufficient technical measures are in place to ensure appropriate	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	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
	security of the Personal Data (e.g. encryption, access controls)	*[4. Any additional Product specific measures]*					
5	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 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*]]	Set out in the Overarching FDP DPIA and Section 3, 12 & 16 above	Tolerate	Remote	Minimal	Low
6	There is a risk that Subject Access Requests will not include a search of FDP preventing	[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];	Section 15	Treat	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
	individuals from having access to all data held about them by the Trust	[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].					
7	There is a risk of failure to provide adequate transparency information to the data subject by the Trust	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 alongside Trust's Privacy Notices/have been linked to from the Trust's Privacy Notices to the NHSE website].	Sections 8 and 9	Tolerate	Remote	Significant	Low
8	There is a risk that increased access to Special Category Personal Data is given to Trust staff who would not normally	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

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
	access that data within their role.						
9	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
10	[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	[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	Section 14	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
	reliability of the Data in the Product.]	the source patient record systems for maintaining accuracy].					
11	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. 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.	Section 17	Treat	Remote	Significant	Low
12	Users will not have their permissions revoked when they leave their role/ organisation and may	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

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
	continue to have access to Data they are no longer entitled to access.]						
13	There is a risk that when upgrades to source systems are completed this does not sync with FDP	The Trust is to inform the Processor of any updates to source systems prior to update so that they can ensure the data is pulled across appropriately and in a timely manner.	[TRUST TO COMPLETE]	[TRUST TO COMPLETE]	[TRUST TO COMPLETE]	[TRUST TO COMPLETE]	[TRUST TO COMPLETE]

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	[Update DPIA to explain how Purpose Based Access Controls will be applied for this Product, including who will authorise analyst access and user dashboard access].	[1, 3], 8 & 12	[*Insert name of IAO/Product owner]*	[*Insert date]*
2	[Provide details of the process in place to review access to the Product and to remove access where users change role or leave the organisation]	[12]	[*Insert name of IAO/Product owner]*	[*Insert date]*
3	[Add Business Continuity Plans in place into the DPIA]	*[9]*	*[Insert name of IAO/Product owner]*	*[Insert date]*
4	[*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]*
5	A Data Processing Agreement must be put in place between Chelsea and Westminster NHS Trust and the other NWL Trusts within this Pilot	*[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