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 3.0 Final		
Document filename	*Cancer 360 – FDP Local DPIA Template*		
Directorate / Programme	FDP Programme	Product Name	*Cancer 360*
Document Reference No	*[Insert IG Reference Number]*	Information Asset Register Number	*[Insert]*
Information Asset / Product Owner Name	*[Insert]*	Version	3.0 Final Approved
Author(s)	Template: NHS England [redacted] [redacted]	Version issue date	*13/05/2025*

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 Local Template – Cancer 360

Document Management

Revision History

Version	Date	Summary of Changes
V0.1	16/07/2024	DPIA draft template created
V0.2	22/07/2024	DPIA draft template updated to make this generic
V0.3	29/07/2024	DPIA reviewed and updated by Palantir
V0.4	29/07/2024	DPIA reviewed and updated by FDP IG team
V0.5	31/07/2024	Final update for DGG
V0.6	07/08/2024	DGG review and comments
V0.7	09/08/2024	Update and response to comments
V0.8	09/08/2024	Clean version
V0.9	09/08/2024	Review and update of DPIA - GC
V0.10	12/08/2024	Update and response to comments
V0.11	12/08/2024	Clean version
V1.0	13/08/2024	Finalisation of document
V1.1	05/11/2024	Update to DPIA to include Benefits Dashboard
V2.0	05/11/2024	Finalisation of document
V2.1	08/05/2025	Update to include granular data specification
V2.2	13/05/2025	Further updates to the document
V3.0	13/05/2025	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]	Head of Information Governance (IG)– Federated Data Platform	28/07/2024	V0.5
Data Governance Group		07/08/2024	V0.6
[redacted]	Deputy Director, IG Risk and Assurance	09/08/2024	V0.9
[redacted]	Deputy Director, IG Risk and Assurance	12/08/2024	V0.11
[redacted]	Head of Information Governance (IG)– Federated Data Platform	05/11/2025	V1.1
[redacted]	Head of Information Governance (IG)– Federated Data Platform	08/05/2025	V2.1
[redacted]	Head of Information Governance (IG)– Federated Data Platform	13/05/2025	V2.2

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	12/08/2024	V0.11
[redacted]	Head of Information Governance (IG)– Federated Data Platform	05/11/2025	V1.1
[redacted]	Head of Information Governance (IG)– Federated Data Platform	13/05/2025	V2.2

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 Product includes any Processing of Personal Data.

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.

This document has been created as a template for local organisations who are Data Controllers to utilise when implementing the Product covered in this DPIA, as such this DPIA can be amended for local use. There are highlighted sections throughout this document that are to be completed and/or reviewed by the local organisations, prior to their own internal sign off.

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 e.g.:

- [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 organisation 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.

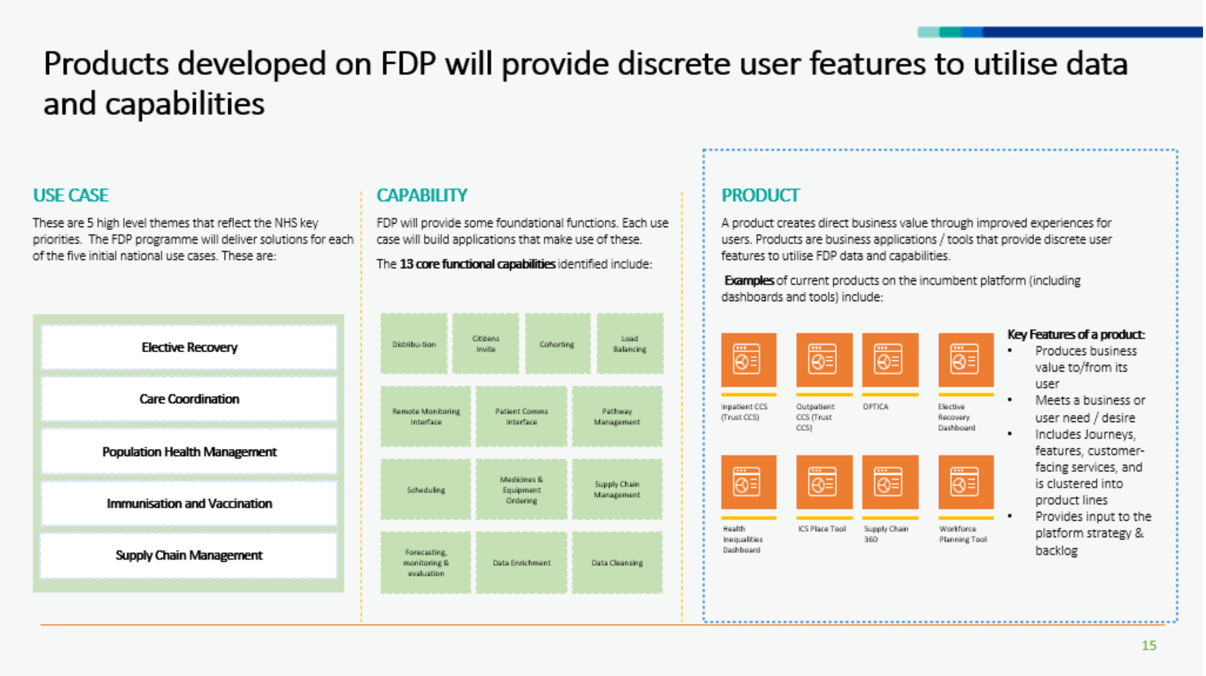
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

The FDP will not only provide the cutting-edge software to organisations 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 Local Organisation 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 Local Organisations 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 objective of the Cancer 360 Product is to enable Trusts to integrate Data held in disparate systems into pre-defined cancer pathway datasets, in a central location, to coordinate cancer care and effectively manage their cancer backlog, reduce waiting times, and drive elective recovery across Trusts.

This Product was initially developed as an Incubator Product in August 2022, by Chelsea and Westminster Hospital NHS Foundation Trust, and has been operationally deployed since December 2022 to support NHS England's Cancer programme. The vision at incubation was to "Create a Pathway Management Solution with a single point of access". This was initially implemented in Foundry and then transitioned into FDP. This Product is now being made available to Trusts within the UK.

Hospitals have a legal responsibility to ensure that patients that are suspected of having Cancer are treated within a certain timeframe. However, in order to diagnose and determine treatment, information typically must be manually gathered from disparate systems, such as:

- The Cancer registry
- EPR (Electronic Patient Record)
- Radiology Information Systems

- Histology Systems
- Pathology Results Systems
- Endoscopy Information Systems
- Oncology Information System
- Patient Communication Systems

This makes it time-consuming and difficult to ascertain where patients are on a particular pathway and where delays may be occurring. To solve this issue, the Product pulls all the relevant cancer pathway information into one place so that the Trust can track patients effectively and prevent delays.

The Product was developed to provide better visibility of patients requiring a Cancer diagnosis across the full diagnosis pathway along with the status of actions required to achieve that diagnosis. It aims to deliver improvements in the timeliness of Cancer diagnosis by enabling earlier identification of bottlenecks and by enabling the Cancer services to shift resources from gathering information about the status of individual patients to ensuring that all required actions are being delivered in as timely a manner as possible.

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 (ICS)) 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

Personal Data that can directly identify an individual.		
Pseudonymised Data *Personal Data that has undergone Pseudonymisation (See Annex 1)*	☐	
Anonymised Data *Personal Data that has undergone Anonymisation (See Annex 1)*	☐	
Aggregated Data *Counts of Data presented as statistics so that Data cannot directly or indirectly identify an individual.*	☒	For Data displayed or shared with users of the Product
Operational Data *Items of operational Data that do not relate to individuals e.g.eg stocks of medical supplies.*	☒	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 Screening Questionnaire is carried out to provide assurance that the Aggregated Data is not Personal Data prior to being ingested into FDP;
- 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 Local Organisations 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 NHS Local Organisations.

NHS Local Organisation 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

This Product was initially created as an 'Incubator' Product within North West London, Chelsea and Westminster Hospital NHS Foundation Trust (CWFT). The Key Stakeholders within the Trust, being the Heads of Cancer services along with representatives from clinical and operational teams involved in the delivery of Cancer services.

The Incubator Product was initially rolled out at pace to manage the large waitlists and delays caused by COVID-19.

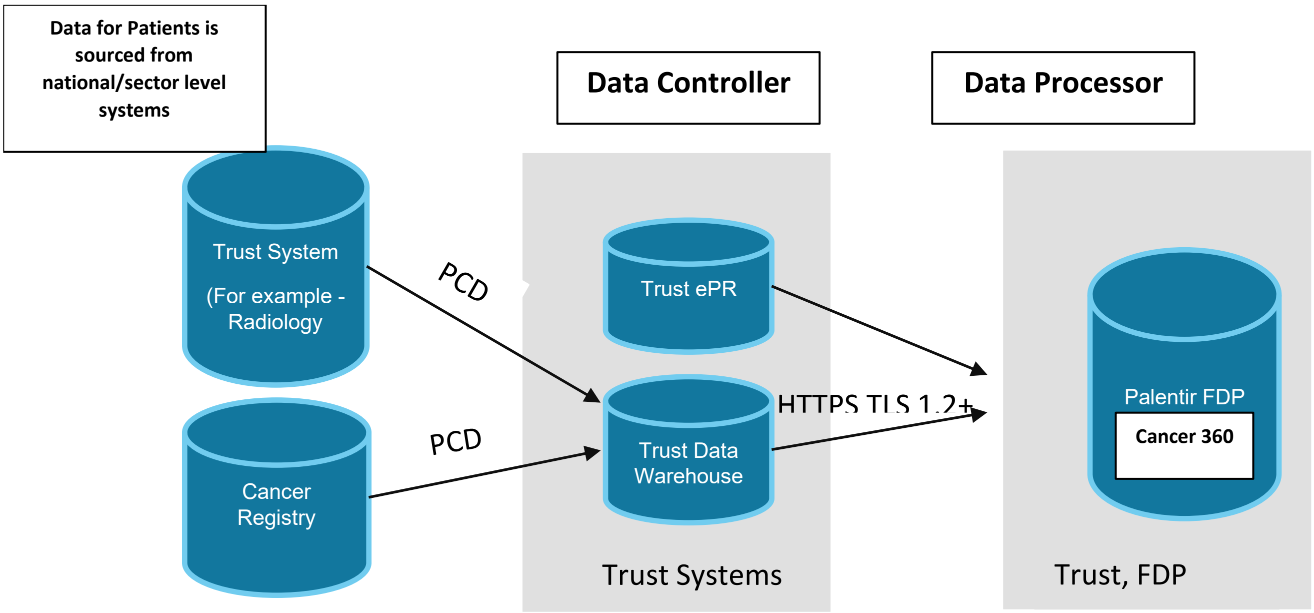
Although public and patient engagement has not yet taken place, engagement with patients should begin and continue throughout the course of this Product being live. The seeking and understanding of the views of the public and patients is an integral part of the NHS Federated Data Platform and as such this has been added as an action within Section 20 of this DPIA.

Prior to roll out, engagement has taken place with service delivery stakeholders within the Trust and this will continue throughout the pilot.

The Key Stakeholders are FDP programme team, the Cancer service team at the Trust including representatives from clinical and operational teams involved in the kick-off and will be involved in delivery of product.

2. Data Flow Diagram

[THE BELOW IS A TEMPLATE DIAGRAM TO BE UPDATED BY EACH TRUST TO INCLUDE THE SYSTEMS THAT DATA IS INGESTED FROM INTO THE TRUST DATA WAREHOUSE]



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

The Product conforms to the Data architecture standards of the Local FDP Data Flows (as outlined in the Overarching DPIA for FDP) and takes Data from the following systems:

The Cancer Registry holds patient Data which supports healthcare professionals' management of patient pathways. [Enter Trust Name] [Enter System Name] Cancer registry, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Cancer pathways;
- Tracking notes/comments;
- MDT meetings;
- MDT notes;
- MDT bookings;
- IPT (Inter-provider transfers).

The EPR (Electronic Patient Record) system holds patient data which supports the booking and management for inpatient and outpatient activity at the trust, as well as key contact information and demographic information about a patient. [Enter Trust Name] [Enter System Name] EPR System, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Demographic data;

- Patient contact information;
- Outpatient appointments;
- Inpatient procedures.

The Radiology Information System holds patient data which the trust utilises to monitor and record patient care within radiology. [Enter Trust Name] [Enter System Name] Radiology Information System, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Radiology exams;
- Radiology booking status;
- Radiology report text.

The Histology System contains details of the histology samples taken and the reports written indicating the results of testing and review of those samples. [Enter Trust Name] [Enter System Name] Histology System, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Histopathology samples;
- Histopathology diagnostic reports.

The Pathology Results System contains diagnostic tests and test results ('clinical investigations'). [Enter Trust Name] [Enter System Name] Pathology Results System, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Test results.

The Endoscopy Information System holds patient data which the trust utilises to monitor and record patient care within endoscopy. [Enter Trust Name] [Enter System Name] endoscopy information system, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Endoscopy exams;
- Endoscopy booking status;
- Endoscopy report text.

The Oncology Information System holds patient data which the trust utilises to monitor and record cancer treatment and care. [Enter Trust Name] [Enter System Name] Oncology Information System, provides data refreshed every [Update As Appropriate:] hour [Delete As Appropriate:] via a direct API connection to [Enter System Name] or via [Enter Trust Name] data warehouse. This includes the following datasets:

- Cancer treatments;
- Cancer treatments booking status;

There is direct entry of information into the Product that is not written back to source systems. This is purely Operational Data related to actions required by different teams to progress patients through a diagnostic pathway and comments related to those actions. The information held only in the Product includes:

- Action description (e.g. book imaging)
- Action detail (e.g. CT, MRI, USS, x-ray)
- Latest action comment (e.g. CTC booked [date])
- Owner (team member name)
- Cancer PTL Team (e.g. Imaging Team WM)
- Status (e.g. completed)
- Days open (# days)
- Created at (date)
- Created by (name)
- Due Date (date)
- Escalation Status (is escalated y/n)
- Escalation reason (e.g. patient unavailable)
- Escalation date (date)
- Escalated by (team member name)
- Escalation Team (e.g. Imaging Managers Team)
- Last updated at (timestamp)
- Last updated by (team member name)
- Completed at (timestamp)

There are four applications which are created from the same dataset. They each contain Directly Identifiable Personal Data (explained in detail below) are read/write access to the dataset exclusively to enable actions to be created, updated and edited Any clinical information that is required to be input into the patient record is input directly to the record. The information that must be entered into the clinical system, is entered into the source systems by Healthcare Professionals at the point of care.

3. Description of the Processing

The nature of the processing is in support of clinical and operational activities related to Cancer care. The current version of the Product supports the management of pathways for patients from point of referral with suspected Cancer through to referral to treatment or communication that no Cancer has been identified.

This pathway management requires processing of Directly Identifiable Personal Data from Clinical Systems as outlined above, in order to provide clinical and operational teams with an accurate and up-to-date view of the exact status of patients on a suspected Cancer pathway, and the actions required for those patients to progress along that pathway.

Data in the Product is used to facilitate Direct Care through the following functions Applications:

Application 1: Cancer PTL (Patient Tracking List)

Provides a consolidated view of all patients on a Cancer pathway (with or without a Cancer diagnosis) that can be accessed by all teams involved in Cancer care. This 'single source of truth' for the PTL can be filtered according to need and is regularly refreshed so that information such as appointments or results update automatically when there is a status change. It is configurable specifically for each Cancer site and pathway allowing for flexibility in the information provided and reducing risk of manual error.

The Product also provides the ability to drill down to pathway-level information from both the Cancer PTL lists and the Cancer PTL Action Tracker. This provides the Cancer teams with access to all of the relevant information about each patient (e.g. full list of actions, appointments, reports, etc.) and the ability to create action requests for care teams.

Application 2: Cancer Actions

Enables rapid and auditable communication for teams to support the steps a patient requires for efficient movement through a diagnostic Cancer pathway. Functionality in this Dashboard enables actions to be created and sent to specific teams; assignment of users to particular actions. This provides both visibility and an audit trail for assigned actions. Updates to actions made in this application will be displayed throughout Cancer 360 against the relevant pathway.

Application 3: Service Overview

Overview of the service performance across the key milestones on the cancer pathway. This allows for bottlenecks and patterns of delay to be identified as areas for improvement. The application displays top line metrics about when an event is happening on average and compares it to past performance for similar events. It covers events such as:

- First Outpatient Appointment;
- Radiology;
- Inpatient Diagnostics;
- Outpatient Diagnostics;
- Endoscopy;
- Histology;
- Follow-up Outpatient Appointments;
- Inter-Provider Transfers
- Cancer Treatment

Application 4: Team Performance

High level summary of actions requested of each team across the Trust. It provides insights into the number and proportion of actions across Cancer sites as well as a view of all actions requested for each team. Visibility of team performance and management of actions is possible from this view. This allows for oversight from management about request and how they are being managed. This application is not used for performance management of staff, however it does provide operational oversight of the service.

The Trust has Purpose Based Access Controls in place through the FDP system to ensure that the access to the Applications is provided to only those staff members who require this access for their job role.

4. Purpose of Processing Personal Data for this Product

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

- Support provision of Direct Care using Directly Identifiable Personal Data
- Allow the Trust to meet or work towards 'Faster Diagnosis Standard' (FDS) which sets target timelines from point of initial referral to diagnosis and either onward referral to Cancer treatment or communication of an 'all clear' outcome to the patient. Trusts are measured on their performance against this standard as part of the overall assessment of Cancer performance.
- Provide better visibility of patients requiring a Cancer diagnosis across the full diagnosis pathway along with status of actions required to achieve that diagnosis.
- Deliver improvements in the timeliness of Cancer diagnosis by enabling earlier identification of bottlenecks and by enabling the Cancer services to shift from gathering information about the status of individual patients to ensuring that all required actions are being delivered in as timely a manner as possible.
- Allow multiple teams to access information and communicate on a single system, making it a streamlined and time effective processes and preventing delays from occurring.

Attached are screenshots of the dashboards:

Cancer 360 – 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.

The application is made up of four main Applications:

1. **Cancer PTL:** This provides Directly Identifiable Personal Data relating to an individual to Healthcare Professionals involved in their care which is managed through Purpose Based Access Controls, detailing the below Data;
   - Days Since Pathway Start
   - Full Name
   - NHS Number
   - Medical Records Number (MRN)
   - Cancer Site
   - Cancer Sub Site

- Hospital Site
- Action information
  - Number of open actions
  - Latest Action Description
  - Recent Action Update Flag
- Latest Tracking comment (e.g. Surgery did not go ahead, treatment plan pending etc.)
- Pathway Status
- Breach information
  - 28-Day Breach
  - 31-day Breach
  - 62-day breach
- Outpatient Appointments
  - Firest Outpatient Appointment Attended Date
  - Next Outpatient Appointment Attended Date
- Latest Histology Sample Taken Date
- Latest Radiology Attended Date
- Latest Inpatient Procedure TCI Date
- Latest MDT Status
- Latest Interprovider Transfer (IPT)
- Matching Pathway Tags (populated if the pathway meets a tag criteria)
- Watchlist Reason (if pathway is on the watchlist)

2. **Cancer PTL Actions:** This provides Directly Identifiable Personal Data relating to an individual to Healthcare Professionals involved in their care which is managed through Purpose Based Access Controls, detailing the below Data:
   - Patient information
     - Name,
     - Date of Birth
     - MRN and NHS Number
   - Action information:
     - Due Date
     - Action Description
     - Days Open
     - Action Detail
     - Action Owner
     - Assigned
     - Action Comments
     - Action Status:
       - Awaiting Assignment
       - Open
       - Escalated - including reason for escalation
       - Completed
       - Revoked
     - Staff member who last updated the action
   - Pathway information:
     - Cancer Site
     - Hospital Site
     - Breach information
       - 28-Day Breach
       - 31-day Breach
       - 62-day breach

        - Pathway Status
    - Diagnostic and Appointment information
        - First Outpatient Appointment Date
        - Next Outpatient Appointment Date
        - Latest Radiology Date
        - Latest Histology Date
        - Latest Inpatient Procedure Date

3. **Service Overview:** This provides Aggregated Data and the underlying row level data to both Healthcare Professionals and Service Managers within the Trust to allow for the management of the service, detailing the below in Aggregate form which is managed through Purpose Based Access Controls. This will enable Trust's Service Managers to provide overview of service performance to identify opportunities for service improvement, to support the management of specific patient cohorts and to provide insights into performance. The Aggregated Data items provided are:

    - Number of Open Pathways by Cancer Site – split by pathway age or Cancer subsite
    - Number of Open Pathways over Time - split by pathway age
    - Number of Open Pathways by Tag – split by pathway age or Cancer site
    - Number of Open Pathways by Pathway Type – split by pathway age or Cancer Site
    - Number of Open Actions by Action Type
    - Number of Open Actions by Assigned Team – split by action age
    - Historic Analysis of Mean Pathway Closed Day
    - Historic Analysis of Cumulative Action Creation and Completion Volumes
    - Metrics for Completed Outpatient Appointments
        - Mean Order Day
        - Mean Scheduled Day
        - Mean Attended Day
        - Mean Turn Around Time
        - Historic analysis of the above measures
    - Metrics for Completed Inpatient Procedures
        - Mean Order Day
        - Mean Scheduled Day
        - Mean Attended Day
        - Mean Turn Around Time
        - Historic analysis of the above measures
    - Metrics for Completed Radiology Exams – broken down by modailty
        - Mean Order Day
        - Mean Scheduled Day
        - Mean Attended Day
        - Mean Report Day
        - Mean Turn Around Time
        - Mean Report Turn Around time
        - Historic analysis of the above measures
    - Metrics for Completed Histology Samples
        - Mean Sample Taken Day
        - Mean Report Day
        - Mean Report Turn Around time
        - Historic analysis of the above measures

- Metrics for Completed Endoscopy Exams
    - Mean Order Day
    - Mean Scheduled Day
    - Mean Attended Day
    - Mean Report Day
    - Mean Turn Around Time
    - Mean Report Turn Around time
    - Historic analysis of the above measures
- Metrics for Completed Cancer Treatment - broken down by treatment type
    - Mean Order Day
    - Mean Scheduled Day
    - Mean Attended Day
    - Mean Turn Around Time
    - Historic analysis of the above measures
- Metrics for Completed and In-Progress Inter-Provider Transfers (IPT) – broken down by IPT reason
    - Number of Received IPTs
    - Number of Received IPTs Before Day 38
    - Number of Received IPTs After Day 38
    - % of IPTs Received before Day 38
    - Number of Sent IPTs
    - Number of Sent IPTs Before Day 38
    - Number of Sent IPTs After Day 38
    - % of IPTs Sent before Day 38
    - Historic analysis of the above measures

4. **Team Performance:** This provides Aggregated Data to both Healthcare Professionals and Service Managers within the Trust to allow for the management of the service, detailing the below in Aggregate form which is managed through Purpose Based Access Controls. This will enable Trust's Service Managers to provide overview of team performance to identify opportunities for service improvement, to support the management of specific patient cohorts and to provide insights into performance. The Aggregated Data items provided are:
    - Overview of
        - The Total Number of Open Actions
        - The Mean Open Action Age in Days
    - Leaderboard of the 3 highest:
        - Teams with the most 10 day old open actions
        - Teams with the most completed actions in the last week
        - Individual Staff members who have requested the most actions in the last week
        - Breakdown by Team of open actions, days open and number completed and created that week
    - Breakdown by Team of:
        - open actions
        - open actions by days open
        - number completed that week
    - Number of Open Actions by Action Type
    - Number of Open Actions by Assigned Team – split by action age
    - Number of Open Actions by Cancer Site
    - Historic Analysis of Cumulative Action Creation and Completion Volumes

In every application within Cancer 360 it is possible to drill down from any aggregated or tabular data views to pathway and patient level information. This ensures Cancer teams have access to all the relevant information about each patient.

In the drill down views Healthcare Professionals are provided with Directly Identifiable Personal Data relating to an individual, which is managed though Purpose Based Access Controls, detailing the below Data items:

- Name
- MRN
- NHS Number
- Phone Number
- Address
- Postcode
- Date of Birth
- Date of Death (if deceased)
- Sex
- Age
- Patient Name
- Pathway ID
- Pathway start date
- Cancer site
- Cancer sub site
- Hospital site
- Pathway type (e.g. 62 day standard, Upgrade, Screening)
- Pathway closed date
- Breach and milestone information (28-day breach, 62-day breach, 31-day breach)
- Diagnosis History
- Action information and history (e.g. book diagnostic test due: 14th May, escalated due to lack of capacity)
- Outpatient appointment information (Key dates, Status, Appointment Type)
- Inpatient procedure information (Key dates, Status, Procedure Type)
- Histology sample information (Key dates, Sample type, Status, Report text)
- Radiology exam information (Key dates, Status, Exam type, Report text)
- MDT notes and outcomes
- Pathway tracking comments (e.g. Surgery did not go ahead, treatment plan pending etc.)
- Test Results (Test type, Key dates, Result value)
- Communication and referral information (i.e. Date First Seen, Date Informed, Date of First Treatment, tertiary date / type, diagnosis code, ITR sent date(s), care ID, MDT status, MDT meeting dates)

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).
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 unsuppressed small numbers in Aggregated Data [ingested into the Product and/or made available via the Product dashboard] could lead to the identification of an individual
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 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 users will not have their permissions revoked when they leave their role/organisation.
14	There is a risk that users will input clinical information into the system that should be input into the patient's medical record.

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 – 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].[We are also able to rely on implied consent to provide people with a legitimate relationship to the patient to provide their care outside of our organisation with access to the Product for the purposes of providing Direct Care to patients].
- **[Not applicable -** The Data disclosed [via the [ ] dashboard] is Anonymous Aggregated Data or Operational Data and is not Confidential Patient Data].
- 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.

Regarding the impact on individuals, the purpose of the Product is to bring together actions and allow communications for teams within Trusts providing Cancer care from initial referral to treatment or communication of 'all clear' to patients, which falls within Elective Recovery. The impact for individuals of the Data Processing is the improvement of services and enabling all Healthcare Professionals who are responsible from providing Direct Care with shared and rapid access to appropriate Data and actions relating to the Patients Cancer pathway, in a single system.

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.

9. Automated Decision Making

Could the processing result in a decision being made about the data subject solely because of Automated Decision Making (including profiling)?	No
If no, please justify why there is no Automated Decision Making included.	This Product processes information only via human intervention and does not automate any process.
If yes, is the decision:	Not Applicable

• Necessary for entering into, or performance of, a contract between the data subject and a data controller • Authorised by law • Based on the data subject's explicit consent?	
Please describe the logic involved in any Automated Decision Making.	Not Applicable
Please set out how you will comply with the safeguards required in Article 22 (3) UK GDPR when using Automated Decision Making	Not Applicable
If Automated Decision Making has been identified, please describe your approach to opt outs for this matter.	Not Applicable
Please describe your approach to be able to process the Data without Automated Decision Making, if the Data Subjects upholds their right to withdraw their Data from Automated Decision Making?	Not Applicable

10. 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.

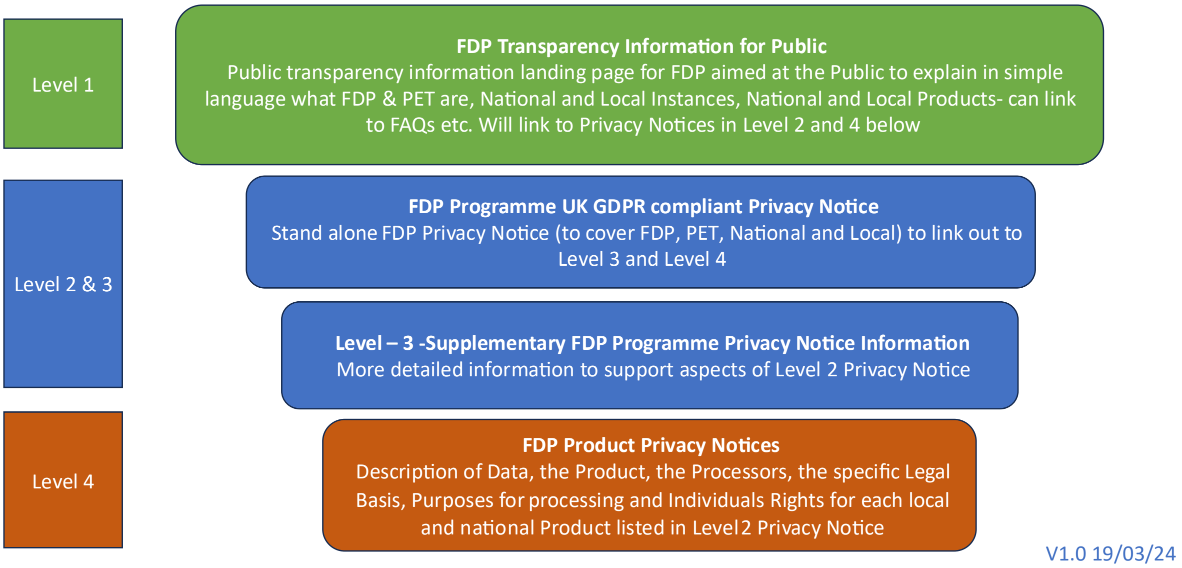
There is a general FDP Privacy Notice which has been published via the NHS England webpages which also explains what FDP is and how it works in more detail. This is Level 2. It has a layered approach which has further detail in Level 3.

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 Level2 Privacy Notice

V1.0 19/03/24

Local Organisation 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]

11. 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. This is also required to ensure activity and clinical Data shown in the Product is for the correct patient and to ensure operational /

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]*
		clinical conversations that use the Data in the Product are for the correct patient.
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	No	
Living Habits	No	
Professional Training / Awards / Education	No	
Email Address - Patient	Yes	This Data is required to contact patients
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 and the Trust Medical Record Number (MRN) are required to enable information to be matched to the correct patient and their record.
Home Phone Number	Yes	This Data is required to contact patients
Online Identifier e.g. IP Address/Event Logs	No	
Mobile Phone No – Patient	Yes	This Data is required to contact patients
Mobile Phone / Device No / IMEI No - Staff	No	
Location Data (Travel / GPS / GSM Data)	No	
Device MAC Address (Wireless Network Interface)	No	
Date of Death	Yes	This Data is required to ensure patients waiting lists are kept up to date and in correct priority.
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	The Product has been designed to facilitate sharing of Data related to patients referred to the Trust with suspected Cancer. Information about the condition is required to deliver aspects of Direct Care that the Product supports.
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:

Cancer 360 Data Specification

12. 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 *Local Organisation* 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 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].*

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

Users of the Dashboards will include:

- Healthcare Professionals working on behalf of the Trust who access to Directly Identifiable Personal Data for the purpose of providing Direct Care.
- Senior Management, within the Team, who work on behalf of the Trust, who have access to Aggregated Data and use the dashboard for service planning.

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*]

[FDP Benefit Metrics Data
In addition, 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].

14. How long will the Data be retained?

The Data will be kept in line with the Local Organisation'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 Local Organisation in line with the NHS Records Management Code of Practice 2021.

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

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:

The Product sources information from the Trust's internal systems, [Enter name of system] and from external systems ([Enter name of systems]) via the Trust's Data Warehouse. Where Data is sourced from 'external systems' the Data collection is restricted to information for patients whose treatment is the responsibility of the Trust.

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 progress of patients on Cancer pathways so, 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.

16. 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 Local Organisation 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]*

17. 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 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]*

18. 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.

19. Do Opt Outs apply to the Processing?

The National Data Opt-Out 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
- No Confidential Patient Information will be disclosed to users of the Product [via the [   ] dashboard which only provides access to Anonymous Aggregated Data].

Type 1 Opt Outs do not apply to this Product because the Datasets used to create the Product does not contain Confidential Patient Information that has been collected by NHS England from GP Practices.

20. 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 unsuppressed small numbers in Aggregated Data [ingested into the Product and/or made available via the Product dashboard] could lead to the identification of an individual]	[As the Aggregated Data [ingested into the Product and/or made available via the Product dashboard] has small numbers included, a risk assessment was undertaken to ascertain if the Data continue to be Personal Data. [Whilst small numbers are [included/shown], they have been further aggregated at *[describe how eg at month, organisational, regional level*] and therefore it would not be possible to re-identify an individual in the Data or for the output to be linked with other Data which would enable re-identification to the users of the dashboard. The Data is therefore considered to be Aggregated Data which is Anonymous].	Section 3 & 7	Tolerate	Remote	Minimal	None

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
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 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
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 [	[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 [ENTER TRUST NAME]'s local Instance of the platform.]	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
	ENTER TRUST NAME]	[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].					
8	There is a risk of failure to provide adequate transparency information to the Data subject by [ENTER TRUST NAME]	1. We have reviewed [ENTER TRUST NAME]'s 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 [ENTER TRUST NAME]'s Privacy Notices to the NHSE website].	Sections 8 and 9	Tolerate	Remote	Significant	Low
9	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.	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
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. [[ENTER TRUST NAME] has Business Continuity Plans in place which cover the inaccessibility/unavailability of the Product].	Section 16	Tolerate	Remote	Significant	Low
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

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
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. 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
13	Users will not have their permissions revoked when they leave their role/ organisation and may continue to have access to Data they are no longer entitled to access.	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
14	There is a risk that users will input clinical information into the system that should be input into the patients medical record.	[TO BE COMPLETED BY TRUST]	[TO BE COMPLETED BY TRUST]	[TO BE COMPLETED BY TRUST]	[TO BE COMPLETED BY TRUST]	[TO BE COMPLETED BY TRUST]	[TO BE COMPLETED BY TRUST]

21. 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	5	*[Insert name of IAO/Product owner]*	*[Ongoing at each change of the Product and update to this DPIA]*
2	Update Section 16 of this DPIA to explain how Purpose Based Access Controls will be applied for this Product, including who will authorise analyst access and user dashboard access	[6 & 8]	[*Insert name of IAO/Product owner]*	[*Insert date]*
3	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	[6 & 8]	[*Insert name of IAO/Product owner]*	[*Insert date]*
4	Commence and continue with patient engagement	*[8]*	*[Insert name of IAO/Product owner]*	*[Insert date – within 6 months of adopting this Product]*
5	Update Section 16 of this DPIA to explain what Business Continuity Plans are in place for this Product	*[9 & 10]*	*[Insert name of IAO/Product owner]*	*[Insert date]*

22.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

23. 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
Automated Decision Making	Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.
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

Defined Term	Meaning
	information will be held in confidence, including Confidential Patient Information.
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

[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 Contract	The NHS-PET Contract and the Platform Contract
FDP Contractor(s)	The NHS-PET Contractor and/or the Platform Contractor
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

[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
	mapping Datasets and models used in Products to object types, properties, link types, and action types. The Ontology 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

Defined Term	Meaning
Programme	The Programme to implement the Data Platform and NHS-PET across NHS England, NHS Trusts and ICBs
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