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	*RTT + Patient Led Validation – DPIA FDP Full*		
Directorate / Programme	FDP Programme	Product Name	*Referral To Treatment (RTT) Validation Tool*
Document Reference No	*[Insert IG Reference Number]*	Information Asset Register Number	*[Insert]*
Information Asset / Product Owner Name	*[Insert]*	Version	5.0 Final Approved
Author(s)	Template: NHS England *[Insert]*	Version issue date	*09/05/2025*

FDP Product Data Protection Impact Assessment – Referral To Treatment (RTT) Validation Tool

Document Management

Revision History

Version	Date	Summary of Changes
1.0	19/03/2024	Updated to reflect comments from stakeholders
1.1	26/03/2024	Updated to reflect comments from DGG
1.2	08/09/2024	Update to document
1.3	03/10/2024	Transfer of DPIA to latest version of FDP Local DPIA
2.0	21/10/2024	Final DPIA clean version
2.1	06/01/2025	Addition of Patient Led Validation module
3.0	10/01/2025	Final updated document
4.0	18/02/2025	New field added to the clinic letter field
4.1	09/05/2025	Update to wording regarding the clinic and referral letters
5.0	09/05/2025	Final Updated Approved DPIA

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version

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 Product 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.

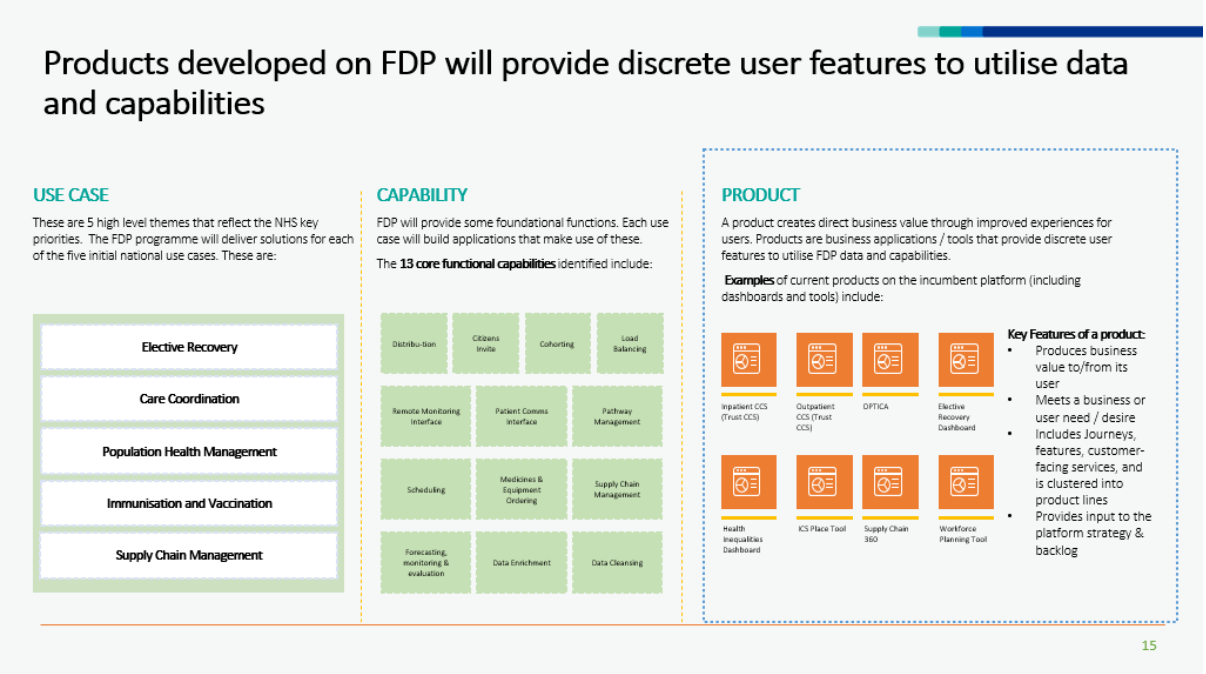
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

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 objective of the Referral to Treatment Validation Tool (RTT) of the Federated Data Platform (FDP), is to reduce waiting times and drive elective recovery across participating NHS organisations. With over 5 million patients on waiting lists post-COVID, reducing these times is considered a priority for NHS recovery. This programme specifically facilitates NHS Trusts integrating pre-defined datasets to manage and reduce waiting lists for appointments in the acute sector. Updated 08/09/2024: Implementation of a new "diagnostic waitlist entry" dataset into the input data specs. This represents important pathway activity that users are currently having to look up outside of the tool. This will be represented to users in a similar way to linked inpatient and outpatient waitlist entries. Please see attached the proposed schema but please note that we are still finalizing the full list of properties. Update 06/01/2025 – This update only applies to the PLV Module Pilot sites. The Patient Led Validation (PLV) Pilot module is designed to manage patient messaging campaigns to confirm waiting lists and thus further assist with elective recovery by cleaning waiting lists of unnecessary entries. PLV works by integrating waitlist data from a Trust's source electronic health record (EHR) into a central interface where PLV teams can configure cohorts of patients, based on any property that has been ingested into the platform, for messaging campaigns. PLV is then able to integrate with the Trust's messaging provider, like DrDoctor, as well as their letter provider, through HL7 messages to the Trust Integration Engine (TIE), to orchestrate the campaigns end-to-end within a single system. Patient responses are also able to be ingested from the messaging provider

for subsequent review by clinicians to decide the appropriate next steps on the pathway or if the patient can be safely discharged based on their response.

Update February and May 2025:

The addition of the Letter Content Field to the CDM Clinic and Referral Letters field to bring up the actual content of letters in the Product and perform keyword searches and lookups on the letters to inform them on the next action to take for the patient pathway. By incorporating the letter content and the searching functionality, this module reduces the need for RTT users to switch back to old source systems for this information.

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

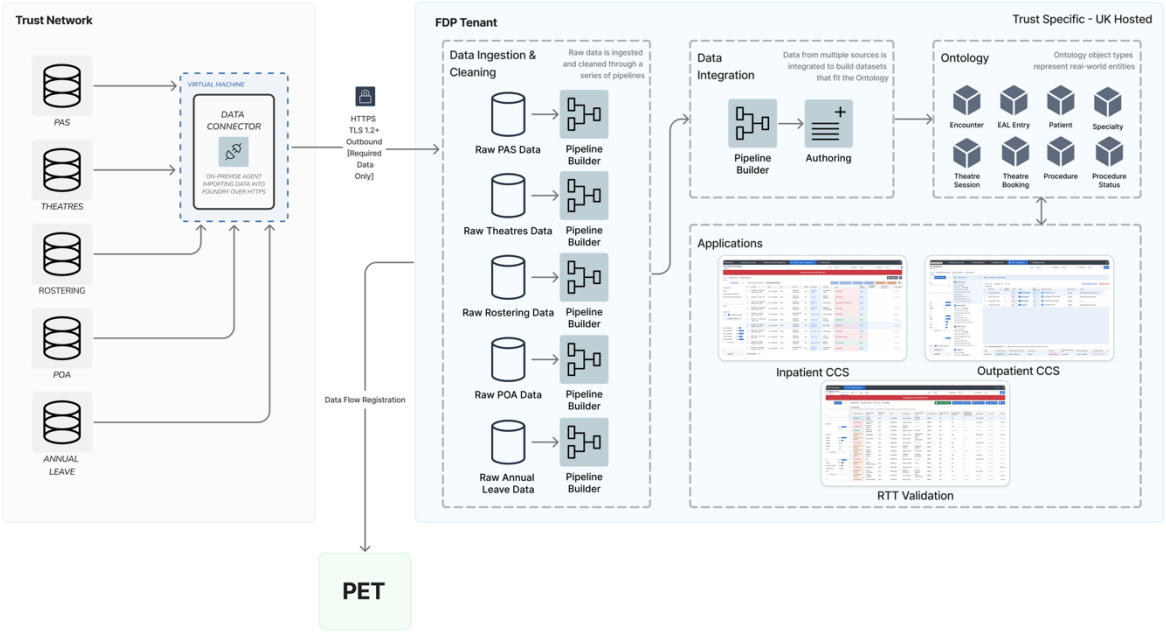
1. Consultation with Stakeholders about the Product

This Product is an existing Data Flow that is operational on the Improving Elective Care Co-ordination for Patients IECCP Foundry platform and is now migrating to the Federated Data Platform (FDP). Prior to this being introduced on the Foundry platform engagement took place with stakeholders and this has continued to support the transfer to FDP.

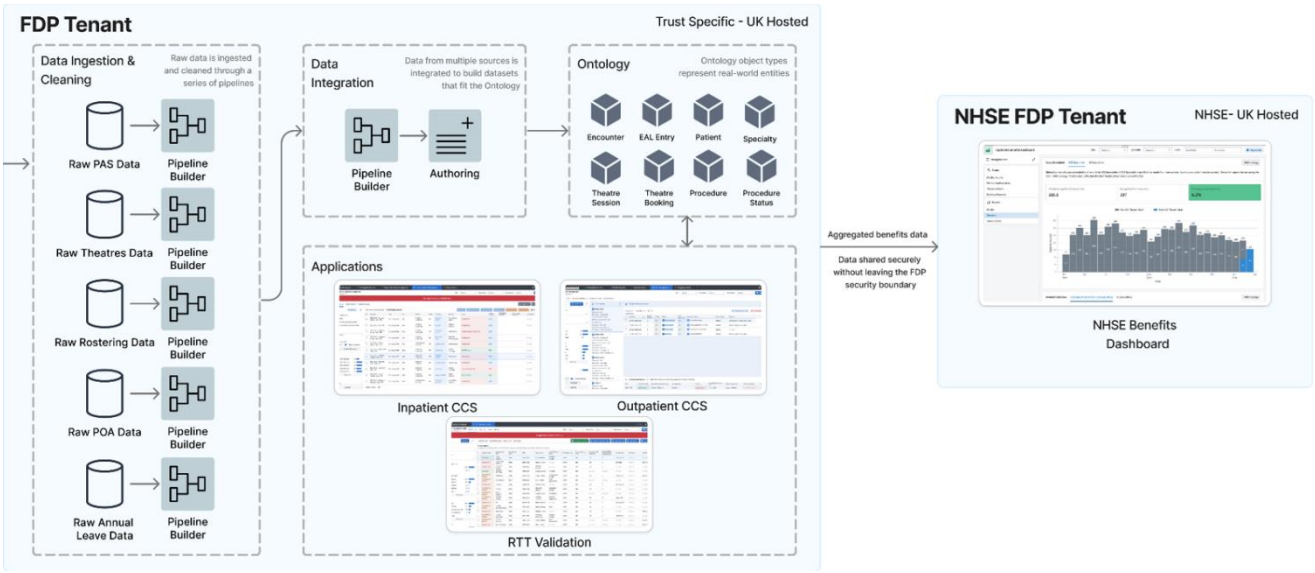
[Insert any further Stakeholder Engagement that Trust has carried out including Patient Engagement]

2. Data Flow Diagram

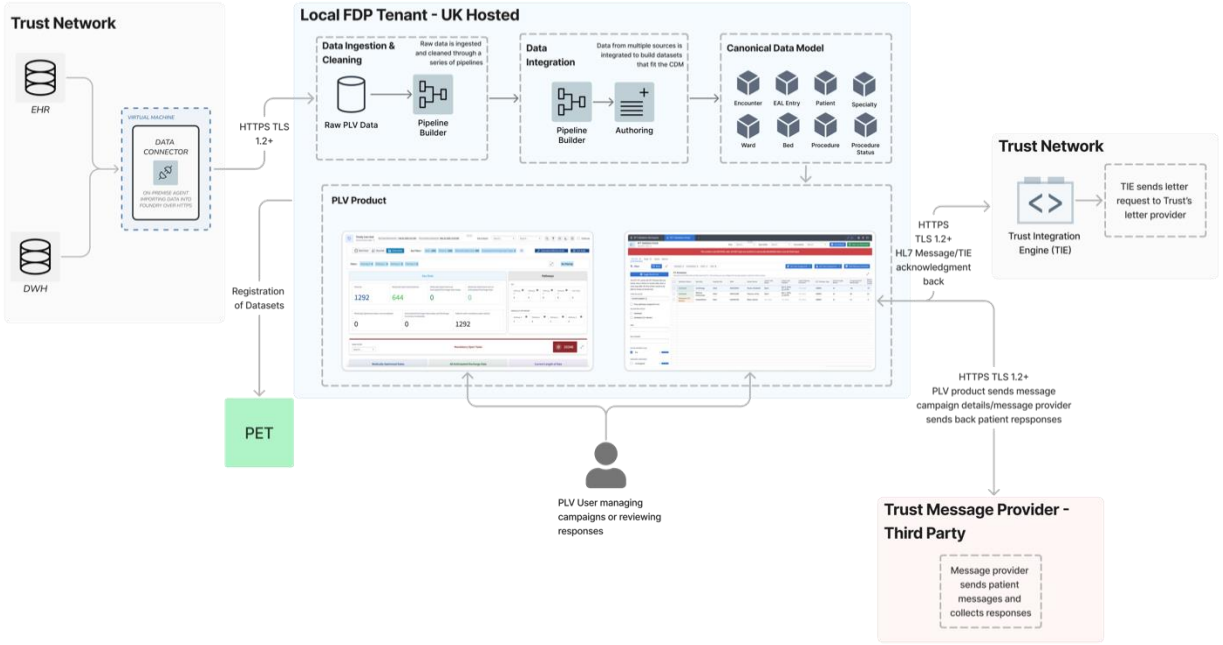
Data flows into the local FDP Instance



Data flows out of the local FDP Instance



Patient Led Validation data flow:



Below is a power point of the benefits dashboard which will be created using aggregate data

3. Description of the Processing

This programme aims to reduce wait times and drive elective recovery across NHS Organisations. The information processed will be of patients who have an open RTT pathway, the aim is to move patients along their pathways as quickly as possible and avoid them breaching the RTT target dates.

This is to identify both patients who either no longer need to be on the waiting list or whose waiting list entry has potential data quality or care issues associated with it as well as providing a single source of operational truth for coordinating RTT patient care decisions across teams.

Administration of user (Trust staff) data will also be processed.

Detailed descriptions of the module functionality are provided in section 3 earlier in this document.

Patient data relating to RTT Periods and associated patient pathways and referrals will be used by Trust Validation teams to review and assess;

a) whether the patient is still waiting for treatment (a 'confirmed waiter') and,
b) what, if any, actions can be taken to accelerate their pathway.

The validation team needs access to Inpatient and Outpatient Waiting List Entries and appointments in order to understand the broader context surrounding each RTT Period in order to make an assessment on whether the patient is still waiting and what actions may be needed.

RTT Validation teams have access to all this information already, but the RTT Validation CCS brings it together in one place for holistic review and provides the operational tooling for prioritising and performing the validations and for creating and assigning tasks. The same data will also be used by the services in order to triage tasks assigned to them by the validation team - this provides important context to better enable them to progress the patient pathway and ensured a shared dynamic version of the truth between these different user groups who have typically previously relied on static spreadsheets and/or emails.

Patient Led Validation Module

This Module is configured to enable Trusts to design, conduct, and track Patient Led Validation (PLV) messaging campaigns in a robust and reliable manner. It allows consultants, service managers and pathway coordinators to cohort patients on the Trust waiting list, based on Trust-agreed eligibility criteria, and validate their need for an appointment via third-party patient engagement platform integration. This workflow processes waitlist and appointment data from the Trust's EHR or DWH *[TRUST TO PROVIDE DETIALS]* into the FDP's Canonical Data Model (CDM) so that the Trust's waitlist can be presented to Trust end users within the frontend of the product so that they can begin to configure the PLV campaign. A specification of the CDM entities that underpin the PLV product is embedded in section 10 of this document.

Patient communication is achieved via two mediums, SMS/text messaging and letters (both digital and physical), thereby mitigating the risk of digital inequity affecting care received by patients. PLV campaign details are sent to Trust-procured third-party messaging providers (like DrDoctor for example) *[TRUST TO PROVIDE DETIALS]* using a standard platform Application Programming Interface (API) over HTTPS. The campaign details are used in turn by the messaging provider to actually send the SMS/text messages to patients. Letter sending is mediated by HL7 messages to the Trust Integration Engine (TIE) which in turn is expected to integrate with the letter provider *[TRUST TO PROVIDE DETIALS].* In addition, any failures to send text messages or letters will be flagged as issues in the frontend for users to action.

[Trust to confirm:

The Trust has the appropriate Data Processing Agreements in place with the messaging and letter providers to allow this Data Processing to occur.]

The Trust's third-party messaging provider also sends the patient response data back into the PLV product through a pull-based method over HTTPS. By centralizing this patient response data in the platform, clinicians are able to review the responses with the patient waitlist details in order to make the most informed decisions on the next steps of their pathway and directly make those requests in the platform (i.e. removing them from the waitlist, booking an appointment).

The module also provides a summary overview of past, present and future validation campaigns, thereby providing an overview of all patient communication activity via the CCS.

The addition of the Letter Content Field to the Clinic Letters field to bring up the actual content of clinic letters in the product and perform keyword searches and lookups on the letters to inform them on the next action to take for the patient pathway. By incorporating the letter content and the searching functionality, this module reduces the need for RTT users to switch back to old source systems for this information. This will only be applied to incubator sites

4. Purpose of Processing Personal Data for this Product

The objective of the Referral to Treatment Validation Tool (RTT) of the Federated Data Platform (FDP), is to reduce waiting times and drive elective recovery across participating NHS organisations. With over 5 million patients on waiting lists following the COVID pandemic, reducing these times is considered a priority for NHS England recovery. This programme specifically facilitates NHS Trusts integrating pre-defined datasets to manage and reduce waiting lists for appointments in the acute sector.

This gives Trusts the opportunity to strengthen their elective care programmes even further, building on the excellent work which is already underway, supported by modern technologies.

The programme involves configuring and deploying Care Coordination Solutions (CCSs) which the Referral to Treatment Validation Module (RTT) is part of. The capabilities of this module include:

- The Referral to Treatment (RTT) Validation Portal enables validators and services to manage and validate active RTT periods in a patient tracking list (PTL). The main purpose of the module is to validate next steps for patients whose waiting times are reported nationally as NHSE has a standard that 92% of these patients should be treated within 18 weeks of their referral. Next steps refer to actions that would need to be taken by Trust services to ensure the patient receives treatment in a timely manner. Once a patient has received treatment, their RTT period will end and they will be removed from the active PTL. The RTT module helps orchestrate the timely care of RTT patients to help make sure they receive the treatment they need as soon as possible.
- The RTT module is intended to be used in mixed team structures; where some Trusts may have a centralised validation team; others may have individuals validating in service or division teams. This is facilitated by flexible team management in the module itself. Additionally, the RTT module is a platform that acts as the source-of-truth for validation allowing the following actions to be taken:
    - Organise the RTT PTL by prioritising the longest waiters to ensure they are receiving treatment as soon as possible.

    - Create validation comments and actionable tasks on RTT periods to move patients along in their pathway.
    - View validation history and performance with near-live updates.
- Through this functionality, the RTT module aims to reduce the communication gap and reduce the need to send individual emails to services, by having an audit trail of actions that are present for any permitted user to view.

Patient Led Validation

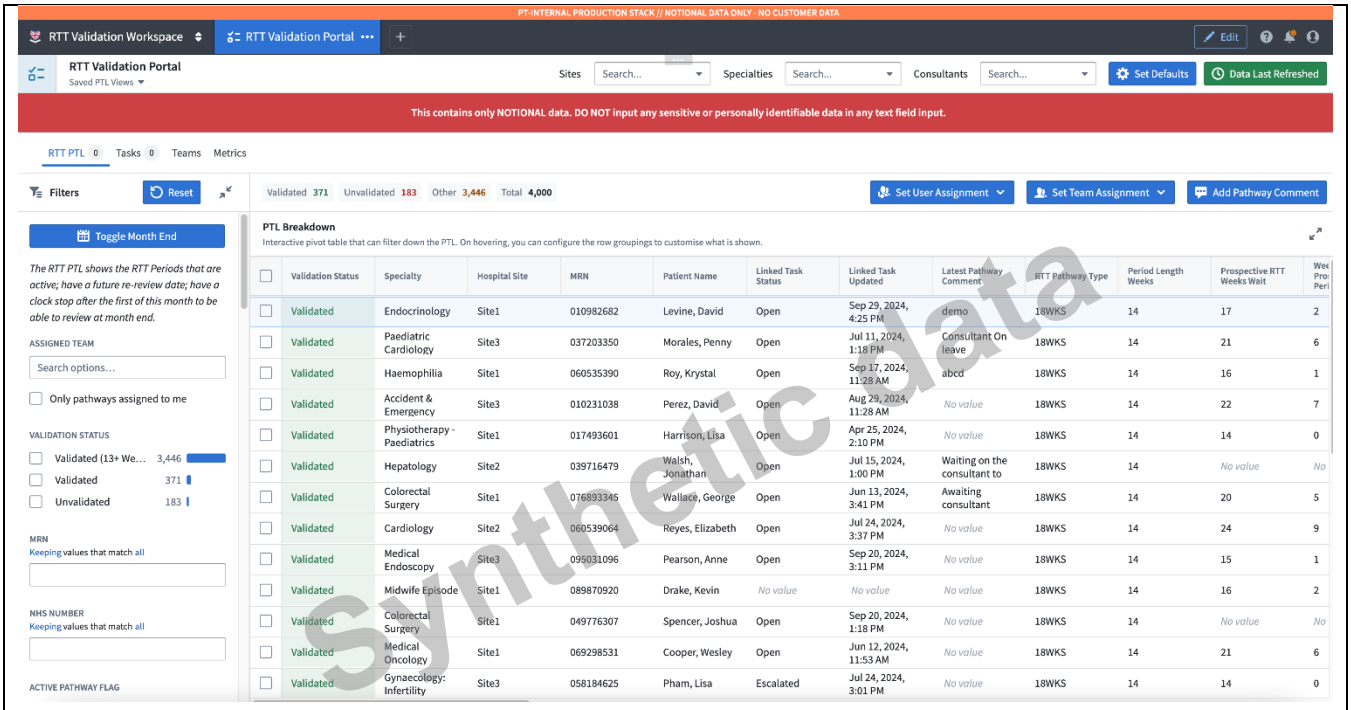
- Enabling Trust PLV teams to identify patients on the Trust's waiting list suitable to be contacted for messaging campaigns asking if they wish to remain on the waitlist for their procedure.
- Creating the campaign itself and enabling Trust users to craft the message that will be sent to patients and managing the approvals of the campaign by appropriate Trust administrators.
- Providing a central platform where the messaging campaign can be triggered and sent to the Trust's messaging or letter providers through simple actions by users.
- Providing a single location where patient responses are automatically collected back from the messaging provider for review by clinicians.
- Enabling clinical reviewers to request actions against waitlist entries based on patient responses (i.e. requesting to remove a patient from the waitlist who has said they do not want their procedure anymore). These requests can then be executed, tracked, and audited by the pathway management team.

The addition of the Letter Content Field to the Clinic Letters field to bring up the actual content of clinic letters in the product and perform keyword searches and lookups on the letters to inform them on the next action to take for the patient pathway. By incorporating the letter content and the searching functionality, this module reduces the need for RTT users to switch back to old source systems for this information. This will only be applied to incubator sites

Out-of-scope of this DPIA

It is anticipated that a minimised, redacted and pseudonymised feed if data will be provided from the Trust to their ICB to enable the CCSs to operate at those levels.

The Trust will be able to carefully calibrate who has access to their own instance of their FDP and which data flows that instance supports.



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

FDP Benefit Metrics Data

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

5. Identification of risks

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

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

Risk No	**Describe source of the risk and nature of potential impact on individuals** *The highlighted text are the most identified risks in the programme. Please amend and delete as appropriate and add Product specific risks.*
1	There is a risk that Personal Data may be accidently misused by those with access.

2	There is a risk that Personal Data will be processed beyond the appropriate retention period.
3	There is a risk that insufficient organisational measures are in place to ensure appropriate security of the Personal Data (e.g. policies, procedures, disciplinary controls).
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*][Where there is Aggregated Data used to create the Product or made available to users through a Dashboard]*
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 the connections with the Trust's messaging and letter providers go down due to integration errors and the PLV product is unable to properly coordinate PLV campaigns while the errors persist.
15	There is a risk that the patient data shared to messaging or letter providers is not protected to the same extent as it is on FDP.
	[*Other Product specific risks*]

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 members of the Care Team outside of our organisation with access to the Product for the purposes of providing Direct Care to patients].

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 review the placements on waiting lists ensuring that patients are appropriately place, which falls within Elective Recovery use case. The Processing this Data enables care teams in a hospital to identify the actions they can take to improve and speed up your care pathway.

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

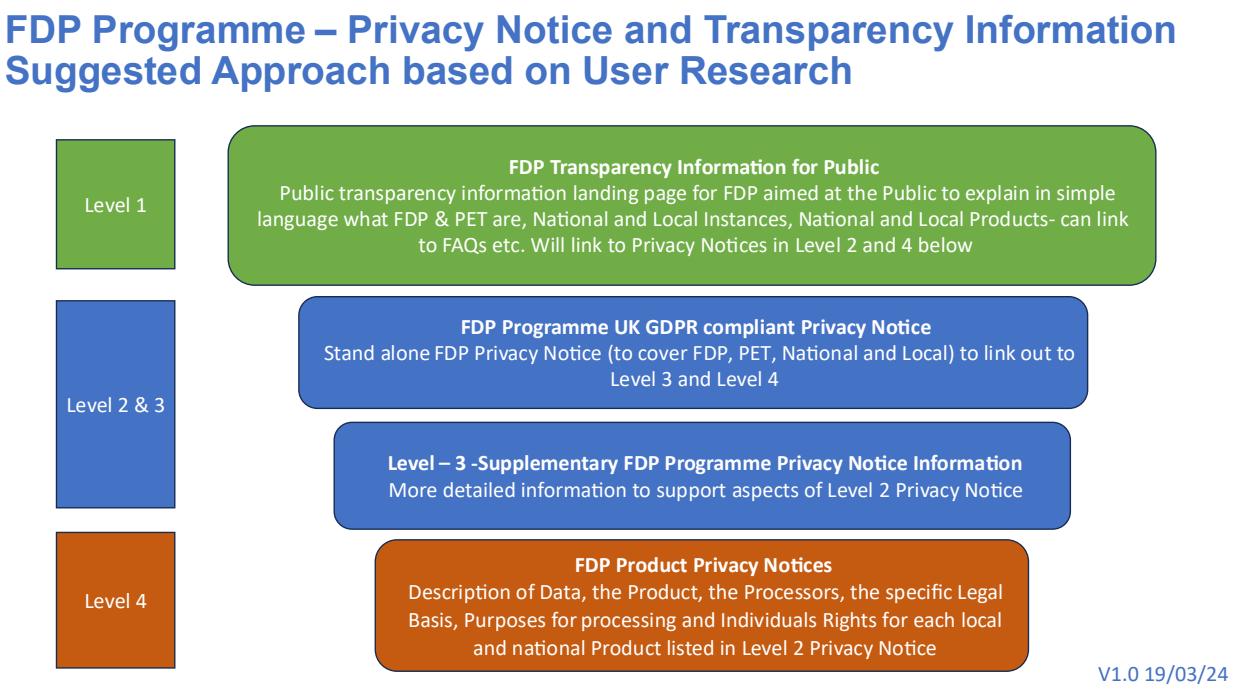
There is a range of information available on the NHS England website about FDP and how it works. This is Level 1 Transparency information.

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.

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]*
Address	Yes	This Data is required to contact patients
Postcode	Yes	This Data is required to contact patients
Date of Birth	Yes	This Data is required to provide Direct Care to patients, as well as Data verification.
Age	Yes	This Data is required to provide Direct Care to patients.
Sex	Yes	This Data is required to provide Direct Care to patients.
Marital Status	No	
Gender	Yes	
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 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	
Spare – add Data item (as necessary)	Yes/No	
Spare – add Data item (as necessary)	Yes/No	
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	This Data is required to provide Direct Care to patients.
Sexual Life / Orientation	No	
Religion or Other Beliefs	No	
Racial / Ethnic Origin	Yes	This Data is required to provide Direct Care to patients.
Biometric Data (Fingerprints / Facial Recognition)	No	
Genetic Data	No	
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences	No	

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

- Data Specification RTT

Update February 2025:

Column	Type	Notes	Description

appointment_id	string	Foreign Key	Appointment the letter relates to
clinic_letter_date	timestamp		Timestamp of the clinic letter
clinic_letter_id	string	Primary Key	Unique identifier of the clinic letter
consultant_id	string		Consultant who wrote the letter
patient_id	string		Patient that the letter relates to
clinic_letter_type	string	Optional	Type of clinic letter
letter_content	string	Optional	Textual content of the letter

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 Annex here once agreed]

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

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

[Insert details of the internal and external users of the Product and how they are provided access eg through the dashboard or if Data is exported out of the Product. Explain what category of Data they get access to eg Aggregated Data and Operational Data only. Explain how user access is kept up to date when there are changes to roles/leavers]

Users of the dashboard may include:

- [ ] who have access to [*insert category of data*] and who use the dashboard for [*describe]*
- [ ] who have access to [*insert category of data*] and who use the dashboard for [*describe]*

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.

To fulfil its purpose, the PLV product shares patient data to the Trust's messaging provider and letter provider through means described in sections 2 and 3.

[Trust to provide their data sharing/processing details with their messaging and letter providers]

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

[*Provide details of how data accuracy is maintained. When inaccuracies are identified, what is the process for updating Data in the Product and reporting inaccuracies in source systems? Is there a need for a clinical safety assessment re the Data being shared into FDP for a different purpose than it was originally used for? If for the same purpose, then what will be the protocol for ensuring that data corrections and updates are implemented in FDP and the Product?]*

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

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

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

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

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

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

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

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

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

Business Continuity Plans
[If 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
- 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 Confidential Patient Information Processed in this Product is used and shared for the Purposes of the Direct Care of patients.

19. Risk mitigations and residual risks

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

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

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

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

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
2	Personal Data may be processed beyond the appropriate retention period.	1.Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place. 2. [*Explain what steps are taken as per section 13 to review and delete information that is no longer required].*	Section 13	Tolerate	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the Personal Data (e.g. policies, procedures, disciplinary controls)	[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	[Pseudonymised Data could be deliberately manipulated by an internal bad actor in some way to re-identify individual people]	[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. Staff are trained and fully aware of their responsibilities when accessing and using Data to only use the minimum required for their purpose and that it is a criminal offence under the DPA 2018 to knowingly re-identify an individual 3. Contracts of employment and other organisational policies provide further safeguards against Data misuse 4. Specific Data Processing instructions are provided to the Platform Contractor which limits their Processing of the Personal Data to this Product for the purposes required 5. The download functionality of Data from the FDP is disabled by default, and access to this is controlled by the	Set out in the Overarching FDP DPIA and Section 11, 12 & 16 above	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
		Product Owner which ensures appropriate governance in in place.]					
6	[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
7.	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
8	There is a risk that Subject Access Requests will not include a search of FDP preventing individuals from having access to all data held about them by the Trust	[1. IG and Medical Records teams responsible for coordinating SAR responses need appropriate levels of access through the Role Based and Purpose Based Access Controls/Permissions Matrix]; [2. Existing SOPs relating to clinical system searches in response to SARs have been revised to include FDP and the Products sitting within the Trust's local Instance of the platform.]	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
		[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].					
9	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
10	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
11	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
12	[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
13	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
14	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
15	There is a risk that the connections with the Trust's messaging and letter providers go down due to integration errors and the PLV product is unable to properly coordinate PLV campaigns while the errors persist.	Integrations with participating messaging and letter providers are conducted through standard FDP APIs via established connection mechanisms like HTTPS and in common industry standards like HL7. Extensive testing is carried out by the supplier for each integration using notional data before moving to production.	Section 2 & 3	Tolerate	Remote	Significant	Low
16	There is a risk that the patient data shared to messaging or letter providers is not protected to the same extent as it is on FDP	[Trust to provide references to their DPIAs covering the participating messaging and letter providers for their organisation]	Section 12	Tolerate	Remote	Significant	Low

20. Actions

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

Action No	**Actions required.** (Date and responsibility for completion)	**Risk No impacted by action**	**Action owner** (Name and role)	**Date to be completed**
1	[Ongoing review of unsuppressed Data to ensure it remains Anonymous Aggregated Data or Operational Data when any new Data items are added to the Product, or when any changes are made the dashboard visualisations].	[6]	*[Insert name of IAO/Product owner]*	*[*Ongoing at each change of the Product and update to this DPIA]
2	[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], 5, 10 & 14	[*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]	[14]	[*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]*

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