Template Version	NHS England FDP National DPIA Template (Identifiable) version 3.0 Final		
Document filename	*NDIT – NHS England FDP DPIA (Identifiable)*		
Directorate / Programme	FDP Programme	Product Name	*National Data Integration Tenant (NDIT) Minimum Viable Product*
Document Reference No	*FDP 129N*	Information Asset Register Number	*N/A*
Information Asset / Product Owner Name	[redacted]	Version	2.0 Final Approved
Author(s)	[redacted]	Version issue date	*23/07/2025*

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

FDP Data Protection Impact Assessment (DPIA) – National Data Integration Tenant (NDIT) Minimum Viable Product

Document Management

Revision History

Version	Date	Summary of Changes
0.1	09/04/2025	Transfer of information onto FDP Templates
0.2	10/04/2025	Programme Team review and update
0.3	11/04/2025	Clean version for review
0.4	17/04/2025	NDG Comments
0.5	25/04/2025	FDP IG Team review and update.
0.6	28/04/2025	Clean version for DGG review and approval
0.7	07/05/2025	DGG Comments
0.8	12/05/2025	FDP IG Team review and update
0.9	13/05/2025	Product Team update
0.10	13/05/2025	ICO Comments transferred and addressed
0.11	13/05/2025	Clean version for approval
0.12	30/05/2025	NHS E DPO Review
0.13	09/06/2025	FDP IG Team review/update
0.14	13/06/2025	Review by NHSE Deputy SIRO
0.15	24/06/2025	Update with additional information, particularly around organisational governance structures.
0.16	16/07/2025	Review by NHSE Deputy SIRO
0.17	17/07/2025	Further updates requested by NHS E Deputy SIRO
1.0	22/07/2025	Final Approved Document
1.1	23/07/2025	Addition of Operational Data (metadata) access and reviewed by NHS England Analysts
2.0	23/07/2025	Final Updated 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 IG - FDP	11/04/2025	V0.2
[redacted]	Head of IG - FDP	13/05/2025	V0.10
FDP Data Governance Group	FDP IG Approval Group	16/05/2025	V0.11
Jon Moore	Deputy Director, Data Protection Officer, Data Protection Office & Trust	30/05/2025	V0.12

Jackie Gray	Director of Privacy and Information Governance as Deputy SIRO	13/06/2025	V0.14
Jackie Gray	Director of Privacy and Information Governance as Deputy SIRO	16/07/2025	V0.16
Jackie Gray	Director of Privacy and Information Governance as Deputy SIRO	17/07/2025	V0.17
[redacted]	Head of IG - FDP	23/07/2025	V1.1

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
FDP Data Governance Group	FDP IG Approval Group	16/05/2025	V0.11
Jackie Gray	Director of Privacy and Information Governance as Deputy SIRO	16/07/2025 18/07/2025	V0.16 V0.17
[redacted]	Deputy Director, Data Collection & Delivery	18/07/2025	V0.16
[redacted]	Head of IG - FDP	23/07/2025	V1.1

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 5
1. Consultation with Stakeholders about the Product 11
2. Data Flow Diagram 12
3. Description of the Processing 12
4. Purpose of Processing Personal Data for this Product 16
5. Identification of risks 20
6. Compliance with the Data Protection Principles - for Processing Personal Data only 22
7. Describe the legal basis for the Processing (collection, analysis or disclosure) of Data? 22
8. Demonstrate the fairness of the Processing 25
9. Automate Decision Making 25
10. What steps have you taken to ensure individuals are informed about the ways in which their Personal Data is being used? 26
11. Is it necessary to collect and process all Data items? 27
12. Provide details of Processors who are Processing Personal Data in relation to this Product 28
13. Describe if Data is to be shared from the Product with other organisations and the arrangements in place for this 29
14. How long will the Data be retained? 29
15. How will you ensure Personal Data is accurate and if necessary, kept up to date 29
16. How are individuals made aware of their rights and what processes do you have in place to manage requests to exercise their rights? 29
17. What technical and organisational controls in relation to information security have been put in place for this Product? 30
18. In which country/territory will Data be stored or processed? 31
19. Do Opt Outs apply to the Processing? 31
20. Risk mitigations and residual risks 32
21. Actions 41
22.Completion and signatories 42
23. Summary of high residual risks 43
Annex 1: Defined terms and meaning 44

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 initiative 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.

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.

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 NHS England and 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.

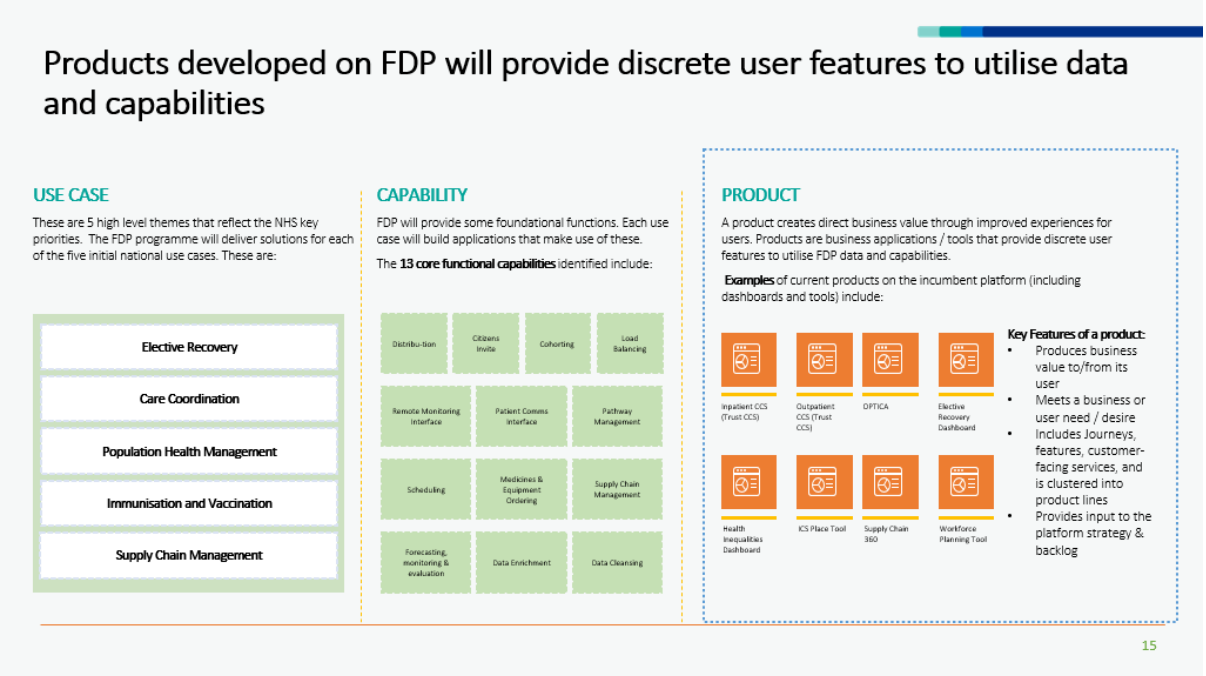
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

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 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 NDIT

Purpose - Overview

Problem statement:

NHS England needs to collect, process and manage national data, including personal identifiable data, in accordance with its statutory duties; currently there are too many platforms and products underpinning these activities.

Navigating and using multiple collection mechanisms increases burden for our users (data providers) and running and maintaining the platforms and products is time consuming and inefficient for our internal teams.

We need to move to a fewer number of platforms and products that are performant, scalable, stable, secure and meet accessibility requirements.

Background/context:

- As part of its statutory duties, NHS England is the '**national safe haven for data**' and currently collects, protects, processes and manages over 400 national data collections, including Directly Identifiable Personal Data.
- This data is then used, in accordance with the relevant legal basis, for analytics, insights and research within NHS England and within the wider system.
- The technical landscape currently underpinning these collection, processing and management activities is a combination of platforms and products from a range of previous organisations (former NHS England and Improvement, NHS Digital, Health Education England).

- There are over 25 separate collection mechanisms and over 6 different processing and management platforms which is a burden for providers to use and navigate and for NHS England to run and maintain.

The National Data Integration Tenant (NDIT) is designed to provide a single, consistent route for Pseudonymised Data, Aggregated Data,Operational Data and Directly Identifiable Personal Data to be collected and curated by NHS England. NHS England currently has multiple routes for Providers to flow data into various technical platforms and systems, and NDIT is the strategic platform to replace the other systems currently in place.

NDIT is considered to be part of the NHS England's "Safe Haven for Data", separated from De-Identified Data analytical environments in line with statutory guidance.

Once data is collected and curated, the primary purpose of NDIT is to safely store and protect data and make it available for downstream uses (e.g. share De-identified Data with national analytical platforms (including the National FDP tenant, and the National Secure Data Environment (SDE), etc.). NDIT will be integrated with both NHS-PET and the National Data Opt-Out Service, to ensure that any flow of data from NDIT to another environment will be treated appropriately (e.g. Pseudonymisation of the Data).

NDIT may develop additional uses, particularly where access to Directly Identifiable Personal Data is required, such as identifying cohorts for vaccination/screening. NDIT will also be a key system for supporting NHS England with individuals' Subject Access Requests.

The use of NDIT to collect and collate data will enable NHS England to:

- Reduce burden on data providers through providing a consistent approach to integration, e.g. a common approach to data quality and validation feedback.
- Reduce the number of systems in the estate, each of which has a burden (e.g. security maintenance, user management, technical debt/upgrades, etc.).

The curation of data within NDIT will allow data to:

- Be quality-checked consistently
- Be matched with key demographics such as NHS Number (to improve linkage rates with other data, dependant on an approved purpose)
- Be enhanced, such as linking to reference data (e.g. matching a postcode to a Local Authority) or by deriving commonly-used information (e.g. calculation of length of stay in a hospital, based on admission and discharge rates)

NDIT is a separate Instance of FDP that will provide core data products at NHS England. These enabling services (e.g. Subject of Care Index) may require their own Data Protection Impact Assessments (DPIAs).

Uses of data beyond core functionality/capabilities will be subject to separate governance.

This includes flows of data out to other systems, e.g. flows of data (including via NHS-PET) for the purpose of FDP Products. **Update July 2025** There is a requirement for NHS England to receive the metadata relating to the data collection routes, the dedicated team uses this intelligence to support the other functions of DCI; Data Collections, Data Coverage and Data Improvement who support data submitters in sending data to NHS England.

Local or National			
Local	☐	National	☒

NDIT 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 within NDIT		**How the different Categories of Data are used in relation to NDIT**
Directly Identifiable Personal Data *Personal Data that can directly identify an individual.*	☒	For Data ingested into the NDIT For Data displayed to, or shared with, users of the NDIT For data being sent to other systems, including flows to be treated by NHS-PET.
Pseudonymised Data *Personal Data that has undergone*	☒	For Data ingested into the NDIT For Data displayed to, or shared with, users of the NDIT For data being sent to other systems, including flows to be treated by NHS-PET.

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 ingested into the NDIT For Data displayed to, or shared with, users of the NDIT For data being sent to other systems, including flows to be treated by NHS-PET.
Operational Data *Items of operational Data that do not relate to individuals e.g.eg stocks of medical supplies.*	☒	For Data ingested into the NDIT For Data displayed to, or shared with, users of the NDIT
Type of Data used in NDIT		
No Personal Data	☐	
Personal Data	☒	For Data ingested into the NDIT For Data displayed to, or shared with, users of the NDIT For data being sent to other systems, including flows to be treated by NHS-PET.
Special Category Personal Data	☒	For Data ingested into the NDIT For Data displayed to, or shared with, users of the NDIT For data being sent to other systems, including flows to be treated by NHS-PET.

1. Consultation with Stakeholders

We have consulted with various key stakeholders whilst determining the key functions of NDIT. This is an existing function and use of Data has previously been carried out by NHS England, which is now being transitioned to FDP.

These Stakeholders include:

- IG and Business Leads across NHS England
- AGEM CSU
- FDP Data Governance Group
- Data submitters
- Data consumers

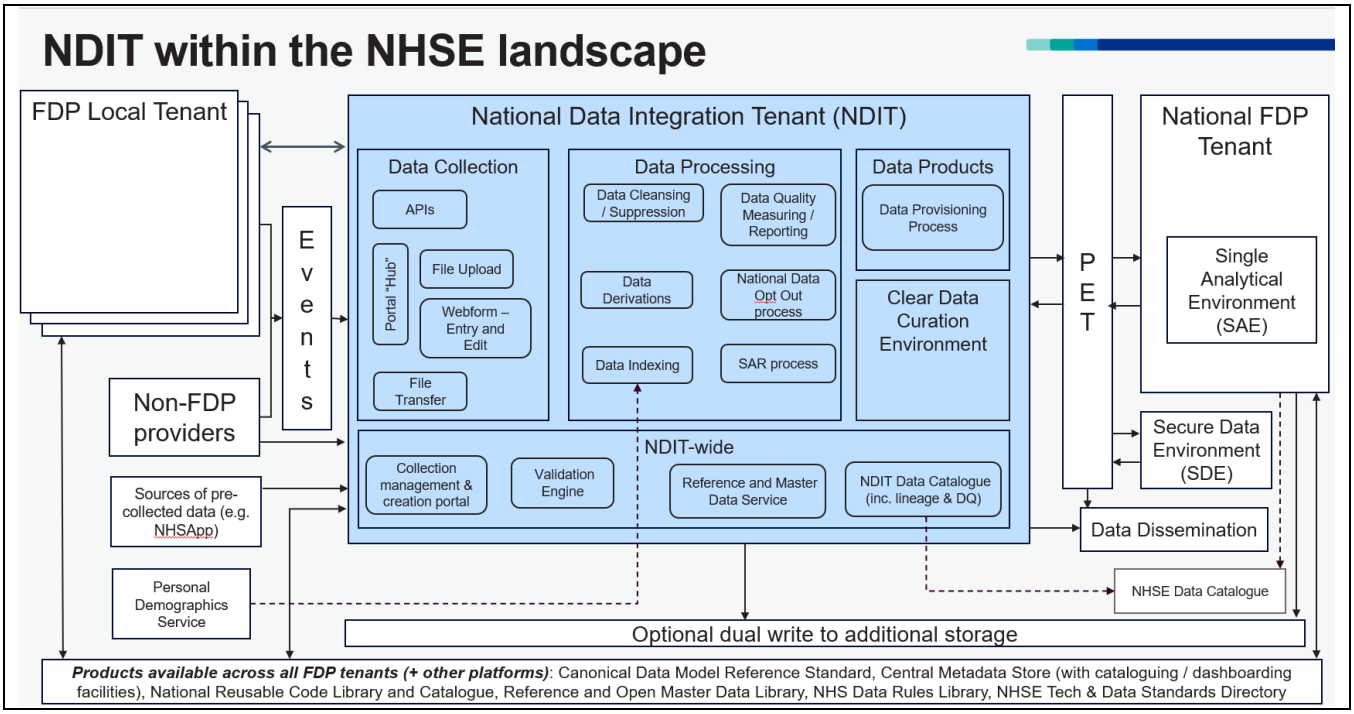
There have also been discussions with the National Data Guardian and Information Commissioners Office regarding this work and review of this document.

The use of the Data collected via NDIT has had further consultation which has been covered in the following FDP Product DPIAs (N.B. some of these are in progress, not yet approved at the time of writing):

- HODF Community
- HODF Acute
- Patient Level Information and Costing Systems (PLICS) Local Costing Collection
- Virtual Wards
- Cancer Waiting Times
- NHS App
- National Digital Channels (NDC)
- Diagnostic Imaging Dataset DIDS v2.0

Note: this is a point-in-time list, and should not be taken as exhaustive.

2. Data Flow Diagram



3. Description of the Processing

The descriptions below are broken into sections to match the diagram (blue box) above.

NOTE: Any specific flow of data (including purpose, use, linkage, destination, lawful basis and transparency) is outside of the scope of this DPIA and is covered by the documentation to support each data flow. Examples (not an exhaustive list) of where separate DPIAs exist are NHS-PET, Products in the National FDP Tenant, Personal Demographic Service, etc.

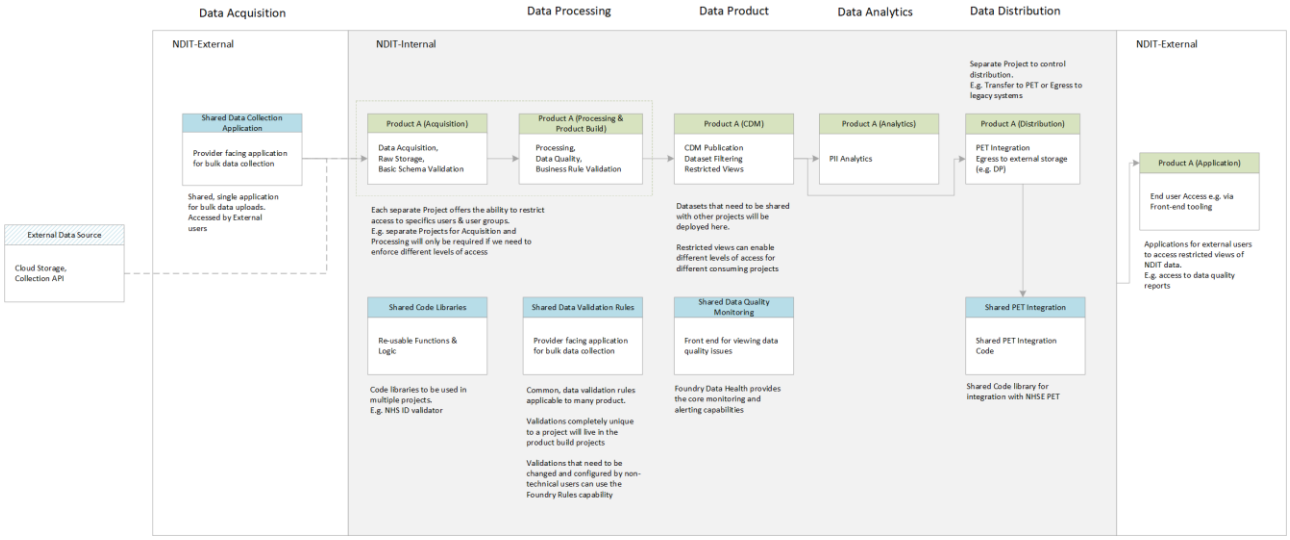
Data Submission (Data Ingress):

Organisations providing Data (e.g. Trusts) to NHS England will send their data to the data Submission area within "NDIT- External". Data can be transferred through the following methods according to Provider need:

- APIs
- File upload
- Webform
- Secure file transfer

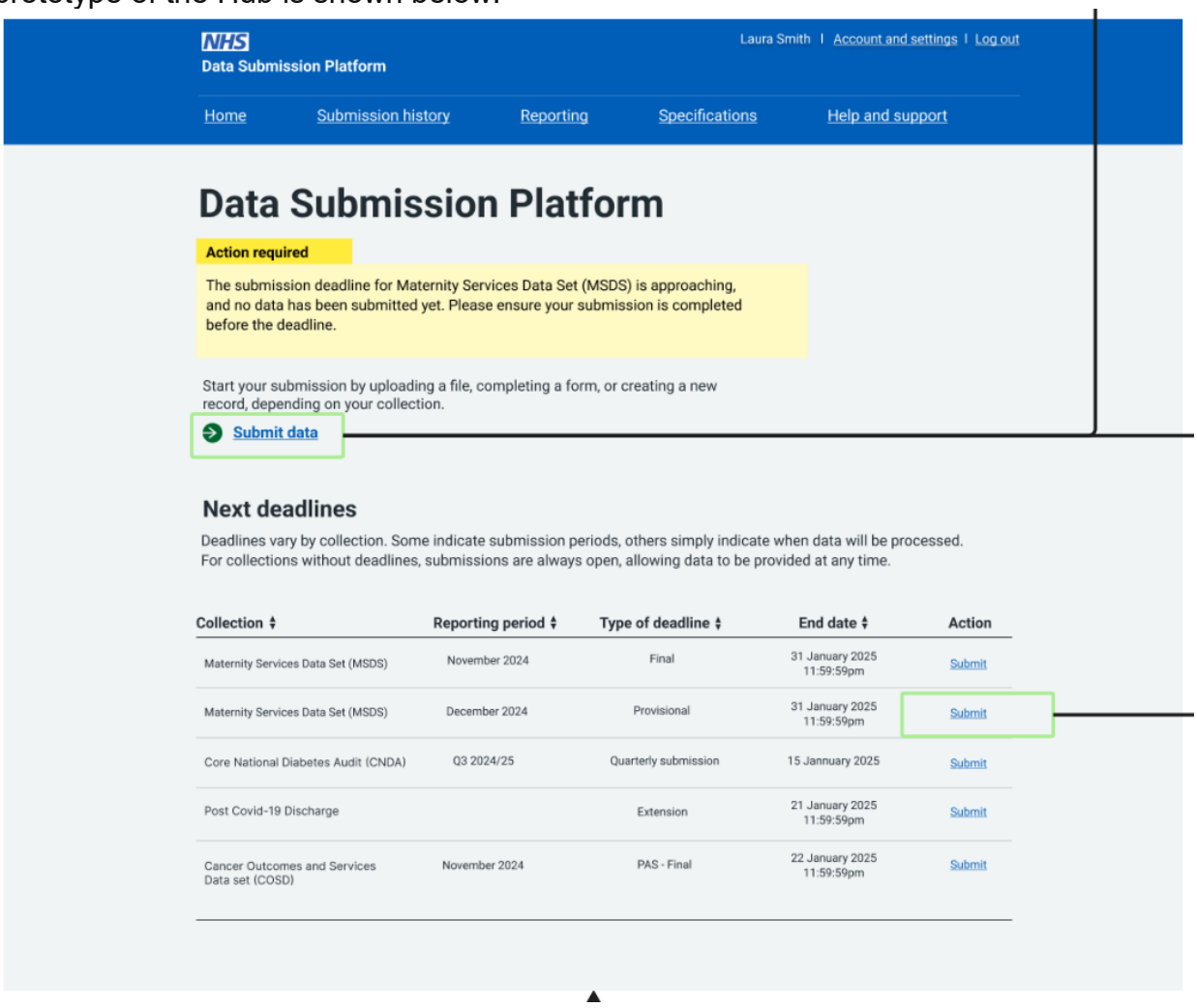
This will become an automated process once locally configured and will enable data to flow routinely from the nominated Provider source systems, as required according to the data set and corresponding specifications. The automated process will accept the correct file format or produce an error report requesting the Provider to correct and resubmit. Different levels of validation will exist as part of the Processing of data from submission through to data distribution.

The data within NDIT-External area (Shared Data Collection Area) will enable bulk uploads of data from multiple Providers and ensure that those with the correct Purpose-Based Access (PBAC) in place to upload data into NDIT-External cannot access any of the areas within “NDIT-Internal”. Providers will only be able to access their own data, not data uploaded by other Providers.
Data will then be pipelined from the Data Submission area in NDIT-External into NDIT-Internal and the designated Project workspaces according to the Data set.



The diagram above demonstrates how Project Workspaces can be utilised to ensure that access to data can be finely controlled, to ensure that engineers, analysts and data submitters only have access to the minimum data required to perform their functions. Some steps may not be required, for example few Projects will require analysis within NDIT as the majority of analytics takes place on Pseudonymised Data after the data leaves NDIT and passes through NHS-PET.

Data submitters will be able to view and manage their submissions via the Portal Hub. A prototype of the Hub is shown below:



The detail of how Controllership will be managed in the Hub will follow - see Action #4. There are expected to be a few standardised patterns that are followed for Collections.

Data Processing:

Each Project workspace is separate and as the Processing function within each Project workspace is completed, the data moves through NDIT-Internal. Each Project workspace has bespoke Purpose Based Access Controls to be in place to govern access to the CPI data within it. The Project workspaces enable the following activity:

- Data acquisition (raw storage and basic schema validation)
- Data processing (Data quality and business rule validation)
- Data product (Common Data Model publication, dataset filtering and generation of restricted views)

The Identifiable layer of NDIT (NDIT-Internal) is siloed from the Non-Identifiable (External) layer of NDIT. NDIT uses a platform capability called "Organisations". Users of the Non-Identifiable (External) layer of NDIT will be added to a separate External Organisation. Only NHSE Staff with genuine need to access Directly Identifiable Personal Data will be

added to the separate Internal Organisation. Data access rights are applied to organisations as well as users and groups, so the use of this concept is a strong mitigation against users being inadvertently granted inappropriate levels of access.

Ingress of Personal Demographic Services (PDS) Data for Cancer Waiting Times
PDS data will be ingested into NDIT-Internal from the legacy NHS Digital Data Processing Service platform (DPS) using a secure S3 connector under this DPIA: the PDS data will be placed in a dedicated S3 location within DPS, which NDIT will access. PDS will be updated daily: DPS receives PDS updates each day, these will be accessed daily by NDIT to populate the Subject of Care (SoC) Index. Updates will be processed as deltas, with the SoC Index retaining history of closed records or previous entries (e.g. address history).

PDS data will be linked with Cancer Waiting Times Data and shared as part of that dataset in accordance with the Cancer Waiting Times Product DPIA.

Data will be linked to reference tables which will be used to apply coding and derivations. As part of routine processing, datasets will be indexed using the 'Subject of Care' index (SoC Index – this is a dataset derived from the Personal Demographic Services dataset, which will be hosted on NDIT). Indexing against SoC will support the consistent identification of patients within processed data, and for the addition of demographic attributes to the data as required. This consistent identification is fundamental to the ability to link patient data across datasets. Linking data in this way will most usually be undertaken on Pseudonymised Data in the FDP National Instance, with pseudonymised identifiers. Linking Confidential Patient Data in NDIT may be expected to support 3rd party cohort linkage and dissemination of Directly Identifiable Personal Data. The initial datasets using NDIT do not require additional data linkage as part of the Processing undertaken within NDIT.

If at any point in the Processing of data within NDIT, the data needs to be subject to National Data Opt Out (as must be identified in the DPIA for the dataset or the specific Processing), then the National Data Opt Out Service must be used.

If the NHSE Data Protection and Trust (DPOT) team request assistance in complying with any Subject Access Requests, then the NHSE SARS process should be followed.

NDIT-wide services:

- **Collection Management and Creation Portal** - where NHSE collection managers and owners can create, amend and manage their data collections e.g. opening and closing collection windows, viewing management information and amending validations.
- **Validation Engine** – a single validation engine will validate all submitted data – regardless of mode of data submission – consistently against a common library of validation rules.
- **Reference and Master Data Service** - provides access to the approved standard reference and master data products (including standard codes for clinical vocabularies or other standard indices) needed for data production Processing, including for data validation checking and for standard data cross-references and transformations (e.g. genericising post codes to geographic areas).
- **NDIT Data Catalogue** (including lineage and Data Quality) – the names and descriptions of data, data policies, data Processing rules, pipelines and data stores implemented within the NDIT environment, including their purpose,

ownership, planned lifecycle, quality scores and inter-relationships, published and managed as part of the NHS England data catalogue service

Clear Data Curation Environment (N.B. "Clear Data" is an engineering term meaning Confidential Patient Data):

Within NDIT, typical processing on Confidential Patient Data will entail:

- Validation of attributes (this may be all or specific attributes)
- Rejection/acceptance of records according to validation rules
- Archiving of raw submission
- Curation of submissions into collated batch for Processing
- Patient indexing to validate patient identity using Confidential Patient Data and retrieval (when available) of any required attributes from Subject of Care Index data
- Data quality reporting – as required by business to flag completion rates and other quality measures with the data (e.g. a null entry in a field may be valid but may indicate poor quality)
- Addition of derivations – these may be sourced from reference data, such as organisational lookups, or may be calculations based on submitted items (e.g. length of stay)
- Any other data cleaning required on the data so that values can conform to the required schema/model of the asset
- Linkage to other dataset – if the required asset is a composite of multiple datasets then linkage to another dataset may occur (if possible, within the requirements of the dataset, this step could be carried out on other platforms/system)

Data Provisioning (Data Egress):

Once Processing and curation according to the individual dataset specifications is complete, and subject to a DPIA (for internal flows) or DSA (for external flows) being in place, the data will be distributed in accordance with the dataset requirement including specifying any required treatment by NHS-PET.

Note that some Processing may require stored data to be linked to a cohort of patients – this cohort could be from another internal business area, generated from a specific dataset within NDIT, or provided by an external organisation (such as a research body).

NOTE: The flow of data including purpose, use, linkage, destination, lawful basis and transparency is outside of the scope of this DPIA and is covered by the documentation to support each data flow.

4. Purpose of Processing Personal Data

The key objectives of the NDIT are to:

- Provide a standard data collection and management portal for Confidential Patient Data and Pseudonymised, Aggregate and Operational Data.
- Standardise the data collected (including data quality and readiness for linkage) and ensure data is handled consistently and efficiently.

- Reduce duplication of data, easing the burden on Providers, improving the timeliness and quality of data, improving access, removing cost and burden of legacy platforms.
- Enable simplified core business processes such as data submission, validation, and collection management alongside a defined range of submission methods including use of APIs, SFTPs and from data entry through a user interface.
- Support individual rights requests, such as Subject Access Requests.

Once the necessary Processing has been undertaken, data will flow out of NDIT to a variety of systems within NHSE as well as potentially to other organisations. Where required, data will be transferred to NHS-PET for treatment prior to onward flow to their destination, the justification for this Processing will be covered in the specific DPIAs.

This enhanced capability and functionality is being developed out of the existing National Identifiable Data Collection Instance (NIDCI) which is an instance of the Federated Data Platform, currently hosted by Arden and GEM Commissioning Support Unit on behalf of NHS England. This Instance is now renamed as NDIT and will migrate to NHS England's direct (i.e. non-CSU) control under an agreed mechanism which is outside of the scope of this DPIA.

NDIT will, over time, grow to process and accommodate most data flows which currently pass through the legacy NHS Digital Data Processing Service platform (DPS) and replace the many different current collection mechanisms. Any data that is currently outside of scope for this DPIA will require an update to this document.

This DPIA covers the NDIT technical structure and includes both the technical and Information Governance for NDIT as a separate Instance of FDP. This will be iterated with the development of NDIT in terms of technical functionality.

Examples of data planned for processing within NDIT include

- HODF Community
- HODF Acute
- Patient Level Information and Costing Systems (PLICS) Local Cost Collection
- Virtual Wards
- Cancer Waiting Times
- NHS App
- National Digital Channels (NDC)
- Diagnostic Imaging Data Set (DIDS) v2.0
- Personal Demographic Services (PDS) data to support Cancer Waiting Times and the Subject of Care (SoC dataset)

Note: this is a point-in-time list and should not be taken as exhaustive.

These data flows have existing, approved Data Protection Impact Assessments which are referenced within this documentation in the Annex for information only. Data flowing through NDIT will have its own separate approved DPIA and appropriate documentation which will reference this DPIA but will not be included in the NDIT DPIA going forwards.

This mirrors the approach taken in the Overarching DPIA for FDP.

5. NDIT Governance

NDIT will use a modular approach to developing the technical architecture to support integration into the NHSE data ecosystem. This will be governed through the usual NHS England processes, such as the Technical Design Authority (TDA) for the Transformation Directorate and the Technical Review and Governance Group (TRG).

Overview of the governance of NDIT:

NDIT Leadership Group:

Purpose: Provides strategic oversight and accountability for the development and governance of NDIT.

Structure and Contribution:

1. Bring experience in our business and industry to shape and steer the design of the National Data Integration Tenant.
2. Approve governance policies and strategic decisions.
3. Ensure compliance with legislation, NHS England policies and standards.
4. Each member is accountable for their team's delivery for NDIT
5. Resolve escalated disputes.
6. Oversee platform performance and effectiveness.

Decision-making and escalations:

1. Accountable for agreeing onboarding plan and roadmap (including dataset prioritisation)
2. Escalation items from NDIT Design & Governance Group
3. Endorses NDIT SOPs and processes.
4. Escalations will be to FDP programme or Data Services management groups.
5. Decisions required outside of this meeting will be escalated to the SRO.

NDIT Design and Governance Group:

Purpose: The NDIT DGG is responsible for day-to-day decision making

Structure and Contribution:

1. Escalation point for core platform, product, and capabilities team and collection-specific delivery teams.
2. Ownership of collection onboarding plan.
3. Ownership of NDIT-wide roadmap.
4. Coordinating work between core team and collection specific delivery teams.

5. Technical direction-setting: defining design standards and configuration/ development patterns for submission, pipeline and process build on NDIT.
6. Operational approval of collection-specific delivery teams' designs.
7. Formally approve elements of the design and send them for implementation consideration via the NDIT Platform, Product, and Capabilities Team.
8. Support the design work within the core team and across the collection specific delivery teams.
9. Surface other design work underway. This enables the benefit of a consistent oversight and approach across NDIT
10. Developing guidelines for data ingress, access control, egress and data sharing with support from the IG Delivery (Data & Analytics) Team in the Privacy, Transparency & Trust Sub-Directorate (PTT).

Decision-making and escalations:

1. Updates to NDIT plans/ processes and technical design decisions are reviewed within the team.
2. Recommendations are submitted to the NDIT Leadership Group for approval.
3. Escalates to the Technical Design Authority if NDIT plans impact high level architectural designs.

<u>NDIT Core Platform, Product, and Capabilities Team:</u>

Purpose: Develops and supports common, re-useable products and capabilities and advises and supports delivery teams on specific components that they may need to deliver and provides core platform capabilities such as technical set up and maintenance and engineer onboarding.

Structure and Contribution:

1. Develop and maintain design and development patterns and templates for NDIT.
2. Ensure alignment with NHS England and NDIT principles, standards, and policies.
3. Provide recommendations to the NDIT Design and Governance Group.
4. Collaborate with collection-specific delivery teams on their designs to advise and assure.
5. Develop and run a National Data Opt-Out process for NDIT.
6. Develop and run SAR process for NDIT to support the DPO team.
7. Security group creation & maintenance.
8. Technical project set up.
9. Engineer onboarding (in accordance with access management process).
10. Assurance/Testing (end-to-end testing and integration testing).
11. Build & deployment governance.
12. Performance monitoring.
13. Identifying and managing risks, including: duplication and re-work; divergence; poor user experience and burden on submitters and our internal support teams.

Decision-making and escalations:

1. NDIT Core Platform, Product, and Capabilities Team makes day-to-day operational decisions, such as sprint planning, backlog refinement, prioritisation etc.

2. Decisions and recommendations are escalated to the NDIT Design and Governance Group.

Data flows – in and out:

Data flows in (ingress):

Where new data flows into NDIT are to be established, a DPIA must be completed and approved for that data to be ingested (this must include the processing required to test the new dataflow). The programme area responsible for the delivery of the new data flow (e.g. Data Delivery) is accountable for the new/updated DPIA. The NDIT Design and Governance Group, and the NDIT Leadership Group is responsible for ensuring an approved DPIA is in place for the data prior to the new data flow in commencing as per the published DPIA Procedure.

Data flows out (egress):

Where new data flows out of NDIT are to be established. The programme area responsible for the delivery of the new data flow will be accountable, for the following:

- DPIA to be completed/updated and approved (e.g. FDP Product DPIA, internal NHS England dataset, system or service DPIA)
- Confirmation of any NHS-PET treatment required
- Confirmation of whether the National Data Opt-Out is needed
- Confirmation of whether the flow is to a new system/environment for a new purpose;
    - If so, does the flow trigger the De-identified Data for Analytics Process (e.g. if the flow is for a purpose other than the Direction under which the data was collected by NHSE)?

The NDIT Design and Governance Group has operational responsibilities including offering advice to programme areas, and the NDIT Leadership Group is responsible for ensuring an approved DPIA is in place and that confirmations are in place prior to the commencement of the new data flow out.

6. 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 Confidential Patient Information (CPI) may be accidently misused by those with access.
2	There is a risk that Confidential Patient Information (CPI) 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 Confidential Patient Information (CPI) (e.g. policies, procedures, disciplinary controls).
4	There is a risk that insufficient technical measures are in place to ensure appropriate security of the Confidential Patient Information (CPI) (e.g. encryption, access controls).
5	There is a risk that Confidential Patient Information could be deliberately accessed by an internal bad actor in some way to identify individual people.
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 NDIT, preventing individuals from having access to relevant Personal Data held about them by NHS England.
8	There is a risk of failure to provide appropriate transparency information to the data subject by NHS England.
9	There is a risk that increased access to Special Category Personal Data is given to NHS England 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.
12	There is a risk that users will attempt to access NDIT 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 those with access to De-Identified Data within NDIT will inadvertently be provided within access to the Directly Identifiable Personal Data within NDIT.

15	There is a risk that NDIT enables requests to collect and Process data, and egress data (this is the extraction or onward sharing of data from NDIT) without the appropriate approvals.

7. 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 8 (Lawfulness); Section 9 (Fairness); Section 10 (Transparency) and 12 (Processors)
Purpose limitation	Section 4
Data minimisation	Section 11
Accuracy	Section 15
Storage limitation	Section 14
Integrity and confidentiality (security)	Section 13 & 17
Accountability	Accountability is addressed throughout the DPIA. In particular, section 23 includes approval of the residual risks by the Information Asset Owner and on behalf of the SIRO.

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

NHS England's legal basis to operate NDIT:

1.1 Statutory Authority

NHS England has various statutory functions that enable it to operate NDIT for itself and for use by other FDP User Organisations. These include:

- Section 270 of the Health and Social Care Act 2012 (**2012 Act**), to establish and provide FDP and NDIT as a service to NHS Trusts and ICBs pursuant to NHS England's power to supply services to any person and provide new services. The supply of FDP and NDIT involves, and is connected with, the collection, analysis, publication or other dissemination of information.
- Section 13D of the National Health Service Act 2006 (**NHS Act**), as part of its duty as to effectiveness, efficiency.
- Section 13K of the NHS Act, as part of its duty to promote innovation.
- Section 1H(2) of the NHS Act as part of its duty under Section 1(1) to promote a comprehensive health service.

- Section 2(2) to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of its functions. Under Section 13Y of the NHS Act this expressly includes the power to enter into agreements.
- The duty under Section 253(1)(ca) to have regard, in the exercise of its functions, to the need to respect and promote the privacy of recipients of health services and of adult social care in England
- The duty under a Direction issued by the Secretary of State under Regulation 32 of the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013 (**NICE Regs**) requiring NHS England to exercise such systems delivery functions of the Secretary of State as may be specified in the Direction.

Note that the statutory authority for the collection of data through NDIT is set out in the relevant DPIA for the data collection. Where this is Directly Identifiable Personal Data, the legal basis will most often be a legal direction issued to NHS England by the Secretary of State under section 254 of the 2012 Act and/or Regulation 32 of the NICE Regs or a request made and accepted by NHS England under section 255 of the 2012 Act.

In relation to the ingestion of PDS Data to support the Cancer Waiting Times Product, the legal basis for ingestion of the PDS Data is set out in the Cancer Waiting Times Product DPIA.

1.2 UK GDPR Legal Basis

In relation to the procurement and provision of FDP for itself and for use by other FDP User Organisations, NHS England relies on the following legal basis:

Article 6 – Personal Data

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

Article 9(2)(g): processing is necessary for reasons of substantial public interest (**Public Interest**). Under section 10(3) of the Data Protection Act 2018 (**DPA**), this requires a condition in Part 2 of Schedule 1 of the DPA. NHS England relies on paragraph 6 (**Statutory Purpose**), as the processing—

- is necessary for the exercise of a function conferred on a person by an enactment or rule of law. Processing is necessary to discharge NHS England's statutory functions set out above, and
- is necessary for reasons of substantial public interest. This is to enable the safe, secure, efficient processing of patient data to deliver more effective and efficient healthcare services.

Note that the legal basis under UK GDPR and the Common Law Duty of Confidentiality for the collection of data through NDIT, including PDS for the Cancer Waiting Times Product, is also set out in the relevant DPIA for the dataset collection. Where this is Directly Identifiable Personal Data:

(a) UK GDPR Legal Basis

- **Under Article 6,** it is expected that the legal basis for Processing Personal Data in NDIT would include:

    - Article 6(1)(c) Legal Obligation, for example where NHS England collects and analyses data under a Direction and FDP User Organisations upload data into NDIT in response to a requirement issued under section 259 of the 2012 Act in a Data Provision Notice. Also where NHS England is complying with a Subject Access Request.
    - Article 6(1)(e) Public Task, for example where NHS England shares data with NHS Trusts through NDIT relying on its powers to disseminate data under Section 261 of the 2012 Act.

- **Under Article 9,** it is expected that the legal basis for Processing Special Categories of Personal Data in NDIT would include:

    - Article 9(2)(g) Substantial Public Interest, on the basis of the statutory authority set out in the relevant DPIA
    - Article 9(2)(h) for medical diagnosis, the provision of health care, or the treatment or management of health care services and system (**Health Care**),
    - Article 9(2)(i) for public health purposes (**Public Health**)
    - Article 9(2)(j) for statistical purposes (**Statistical Purposes**)

- **Under Schedule 1 of the DPA** it is expected the additional conditions of Processing Special Categories of Personal Data in NDIT would include:

    - paragraph 2 (Health Care),
    - paragraph 3 (Public Health),
    - paragraph 4 (Statistical Purposes), and
    - paragraph 6 (Statutory Purpose).

(b) Common Law Duty of Confidentiality

Under the Common Law Duty of Confidentiality Confidential Patient Data is Processed within NDIT, it is expected it would be lawful because of:

- legal obligation, including:
    - under section 254 of the 2012 Act in relation to data that NHS England has been directed to collect and/or analyse pursuant to a Direction issued by the Secretary of State for purposes covered by a Direction.
    - Under section 259 of the 2012 Act in relation to data that NHS England has required is supplied to it by an FDP User Organisation in response to a Data Provision Notice so that it can comply with its duty to collect and analyse data under a Direction. This may apply to data shared from a local Instance into NDIT.
- statutory authority which expressly sets aside the Common Law Duty of Confidentiality including:
    - Regulation 3 of the National Health Services (Control of Patient Information) Regulations 2002 (“COPI Regulations”)
    - Regulation 5 of the COPI Regulations in relation to medical purposes approved by the Secretary of State with support from the Confidentiality

Advisory Group, also known as an approval under Section 251 of the NHS Act 2006.

The specific legal bases for each dataset flowing through NDIT are covered by the corresponding DPIA for those datasets and are outside of the scope of this DPIA.

9. 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 NDIT 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 11 below.

Regarding the impact on individuals, the purpose of the NDIT is to provide a stable environment for the management of Confidential Patient Data which Providers are required to submit to NHS England and/or which NHS England is required to Process, which is a Core Capability. NHS England is Processing data to enable the NHS to operate more effectively, utilising resources in the best possible way to benefit patient care.

Fairness in relation to any specific dataset collected and processed through NDIT is set out in the relevant DPIA for the dataset.

10. 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.	NDIT is a Data collection environment in which datasets are submitted for validation and preparation prior to flowing into other areas of NHSE's technical infrastructure such as the National FDP Instance.
If yes, is the decision: • 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?	Not Applicable
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	Not Applicable

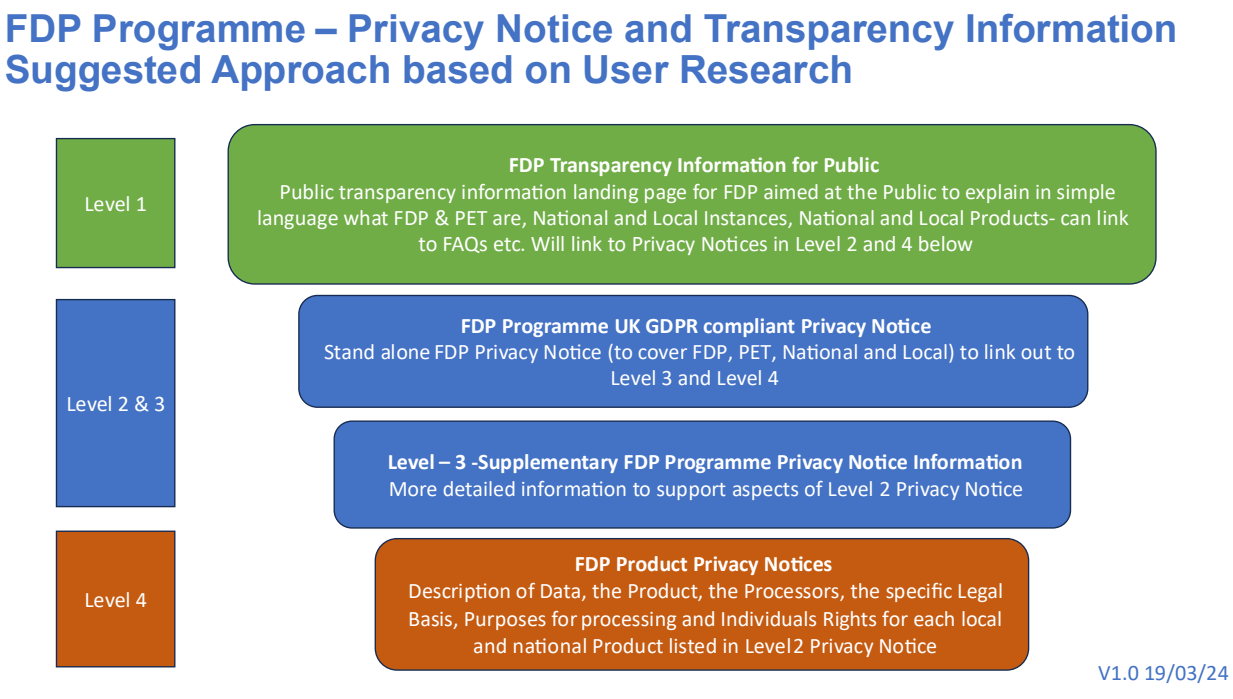
GDPR when using Automated Decision Making	
If Automated Decision Making has been identified, please describe your approach to opt outs for this matter.	Not Applicable
Please describe your approach to be able to process the Data without Automated Decision Making, if the Data Subjects upholds their right to withdraw their Data from Automated Decision Making?	Not Applicable

11. 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. See Action 6 in relation to updates required to Level 1 Transparency information about NDIT

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. See Action 7 in relation to updates required to Level 2 and 3 Privacy Notice about NDIT

NHS England » NHS Federated Data Platform privacy notice



We have consulted with various key stakeholders whilst determining the key functions of NDIT. This is an existing function and use of Data has previously been carried out by NHS England, which is now being transitioned to FDP.

These Stakeholders include:

- IG and Business Leads across NHSE
- AGEM CSU
- FDP Data Governance Group
- Data submitters
- Data consumers

The use of the data collected via NDIT has had further consultation which has been covered in the below Product DPIAs:

- HODF Community
- HODF Acute
- Patient Level Information and Costing Systems (PLICS) Local Cost Collection
- Virtual Wards
- Cancer Waiting Times
- NHS App
- NDC
- Diagnostic Imaging Data Set DIDS v2.0

Each dataset collected and Processed in NDIT also has its own Privacy Notice published on the NHS England website as explained in the relevant DPIA for the dataset.

12. 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	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Address	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Postcode	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Date of Birth	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Age	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Sex	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Marital Status	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Gender	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Living Habits	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Professional Training / Awards / Education	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Email Address - Patient	No	
Email Address - Staff	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Physical Description	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.

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]*
General Identifier e.g. NHS No	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Home Phone Number	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Online Identifier e.g. IP Address/Event Logs	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Mobile Phone No – Patient	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Mobile Phone / Device No / IMEI No - Staff	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Location Data (Travel / GPS / GSM Data)	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Device MAC Address (Wireless Network Interface)	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Sexual Life / Orientation	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Religion or Other Beliefs	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Racial / Ethnic Origin	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Biometric Data (Fingerprints / Facial Recognition)	No	
Genetic Data	Yes	For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences	Yes	Not directly intended, but in some circumstances, data processed on the platform may relate to the health and justice system. This data would likely be limited to the location of a patient at a particular time (e.g. if serving a prison sentence or being treated in a particular health and justice setting). For some Datasets; please refer to the specific DPIA relating to the Product or Dataflow.

13. 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 NHS England as a Controller in relation to Processing Personal Data held in NDIT. 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 NDIT will be issued. A copy of this Data Processing Annex is attached here:

  FDP Product Annex NDIT – V1.0 Final Approved

14. Describe if data is to be shared from NDIT with other organisations and the arrangements in place for this

No sharing of Personal Data from NDIT is authorised under this DPIA. Any planned sharing should follow the procedure for establishing data flows out of NDIT including completion/update of a DPIA where required.

15. How long will the data be retained?

The data will be kept in line with business requirements as described in the DPIA for each dataset.

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

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

The Processing of Personal Data within NDIT is continually checked to ensure it is of good quality, accurate and up-to-date. The dashboard visualisations enable action to be taken where data quality is inadequate. Because Processing is completed on a daily basis, errors are quickly rectified.

In the future, the Subject of Care Index is expected to improve the accuracy of Personal Data within NDIT.

DPIAs for each dataset Processed through NDIT contain further details about any dataset specific data quality processes.

17. 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. See Action 7 in relation to updates required to the FDP Privacy Notice to include NDIT

The following rights under UK GDPR may apply to the Processing of Personal Data within NDIT:

- Right to be informed
- Right of access
- Right to rectify
- Right to object (applicable when relying on Article 6 1 (e) legal basis)

Any requests would be handled by the DPO & Trust Team in NHS England in accordance with standard processes.

For Subject Access Requests, the NHSE SARS process should be followed.

18. What technical and organisational controls in relation to information security have been put in place for NDIT?

Specific Access controls for NDIT

The NDIT Design and Governance Group has responsibility for developing NDIT processes, controls and standard operating procedures (SOPs). The Design and Governance Group includes members from Cyber Security and Service Operations to ensure NDIT is secure by design. The SOPs will cover approving access, monitoring access, revoking access, access coverage, audit and authentication.

NDIT will look to utilise existing controls and processes such as NHS Mail or Okta for multi-factor authentication and the NHS England Clear Data Access process for internal users.

Currently the SRO has sole responsibility for approving access to NDIT on the basis that each individual:

- has had their role and its need for access verified by the Assistant Director of Data Engineering
- can evidence the DBS check
- has completed the National Data Opt-Out Training to enable the users to ensure that Data is being used appropriately and within the boundaries of the National Data Opt Out Policy.
- is not working offshore (outside of the UK).

This is an interim position until the NDIT access SOP is in place, after which all access decisions will be reviewed. Access requests are logged and monitored with an audit trail for approval.

NDIT is an isolated Instance of FDP which has a distinct audit log and is only accessible by approved staff within NHS England. These members are reviewed and approved by NDIT Design and Governance Group.

Restricting access to Directly Identifiable Personal Data

Each Project workspace is separate and has bespoke Purpose Based Access Controls to be in place to govern access to the CPI data within it.

The Identifiable layer of NDIT (NDIT-Internal) is siloed from the Non-Identifiable (External) layer of NDIT. NDIT uses a platform capability called "Organisations". Users of the Non-Identifiable (External) layer of NDIT will be added to a separate External Organisation. Only NHSE Staff with genuine need to access Directly Identifiable Personal Data will be added to the separate Internal Organisation. Data access rights are applied to organisations as well as users and groups, so the use of this concept is a strong mitigation against users being inadvertently granted inappropriate levels of access.

NDIT System Level Security Policy (SLSP)

NDIT System Level Security Policy (SLSP)

19. 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.

20. Do Opt Outs apply to the Processing?

The National Data Opt Out (NDOO) policy may apply to some data collections or Processing utilising NDIT, in such cases the DPIA for the specific collection/Processing will identify this and the route for managing the NDOO.

Type 1 Opt Outs do not apply to NDIT because the Data Processed within NDIT does not contain Confidential Patient Information that has been collected by NHS England from GP Practices.

21. Risk mitigations and residual risks

Section 5 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 5, 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	There is a risk that Confidential Patient Information (CPI) 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 NHS England 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 reason 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 a response	Section 14 & 18	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	There is a risk that Confidential Patient Information (CPI) will be processed beyond the appropriate retention period.	1.Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place.	Section 15	Tolerate	Remote	Minimal	Low
3	There is a risk that insufficient organisational measures are in place to ensure appropriate security of the Confidential Patient Information (CPI) (e.g. policies, procedures, disciplinary controls).	1.Appropriate technical and 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 13 & 18 above	Tolerate	Remote	Minimal	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
4	There is a risk that insufficient technical measures are in place to ensure appropriate security of the Confidential Patient Information (CPI) (e.g. encryption, access controls).	1. Data is encrypted in storage 2. All Data to and from the platform is encrypted in transit using at least TLS1.2 3. SLSP in place	Set out in the Overarching FDP DPIA and Section 13 & 18 above	Tolerate	Remote	Minimal	Low
5	There is a risk that Confidential Patient Information could be deliberately accessed by an internal bad actor in some way to identify individual people.	1. There is only a limited number of staff who have access to NDIT. 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. 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 NHS England.	Set out in the Overarching FDP DPIA and Sections 5, 12, 13 & 18 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
		4. Contracts of employment and other organisational policies provide further safeguards against Data misuse 5 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 6. The download functionality of Data from the FDP is disabled by default, and any requirement to download from NDIT must be approved by the NDIT Leadership Group (as described in section 5).					
6	There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures.	1. Full details are described in the Overarching FDP DPIA.	Set out in the Overarching FDP DPIA and Section 3, 12 & 17 above	Tolerate	Remote	Minimal	Low
7.	There is a risk that Subject Access Requests will not include a	1. Existing internal NHSE procedures for managing DSARs have been updated to include consideration of any Personal Data held in FDP.	Sections 5, and 16	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
	search of NDIT, preventing individuals from having access to relevant Personal Data held about them by NHS England.	2. The NDIT Core Platform, Product, and Capabilities group are working with the DPO team to review and update the existing process to reflect the latest DSAR process.					
8	There is a risk of failure to provide appropriate transparency information to the data subject by NHS England.	1. The NHSE General FDP Privacy Notice has been published. 2. There are actions (6 and 7) to review and update the Transparency Information in light of NDIT.	Section 9 and 10	Treat	Remote	Minimal	Low
9	There is a risk that increased access to Special Category Personal Data is given to NHS England staff who would not normally access	1. There is a limited number of staff who have access to NDIT, all of whom have 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 13 & 17	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
	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.	1. The FDP Contractor is required to have Business Continuity Plans in place.	Section 17	Treat	Possible	Minimal	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	1. NDIT will only collect the mandated datasets including Personal Data from various NHS source organisations. It does not collect Personal Data directly from individuals. Services carried out through NDIT include data quality checking and validation which will enable errors and data quality issues to be identified and addressed. The DPIA for each dataset will provide more information about how any	Section 3 & 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
	reliability of the data.	specific data quality risks are addressed					
12	There is a risk that users will attempt to access NDIT 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 or be accessible from outside of the UK without the express prior approval from the Data Governance Group. 2. It is within the Platform 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 18	Tolerate	Remote	Significant	Low
13	There is a risk that users will not have their permissions revoked when they leave their role/organisation.	1. There is a limited number of staff who have access to NDIT, all of whom have Role Based and Purpose Based Access Controls are in place. 2.It is the responsibility of the NDIT Leadership Group to ensure the appropriate access is in place at all times, this includes revoking	Section 14 &18	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
		permissions for those staff members who no longer require access.					
14	There is a risk that those with access to Non-Identifiable Data within NDIT will inadvertently be provided within access to the Directly Identifiable Personal Data within NDIT.	1.It is the responsibility of the NDIT Leadership Group to ensure the appropriate access is in place at all times, this includes providing the appropriate permissions for those staff members who require access to NDIT. 2.The Identifiable layer of NDIT (NDIT-Internal) is siloed from the Non-Identifiable (External) layer of NDIT.	Section 2 and 3	Treat	Remote	Significant	Low
15	There is a risk that NDIT enables requests to collect and Process Data, and egress data (this is the extraction or onward sharing of data from NDIT) without	1.For any processing of Data there will be a specific DPIA completed (as per governance described in section 5) outlining the lawful basis both under UK GDPR and Common Law Duty of Confidentiality for that processing to commence, as well as specific access control mechanisms.	Section 3, 4, 5 and 8	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
	the appropriate approvals.						

21. Actions

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

Action No	**Actions required.** (Date and responsibility for completion)	**Risk No impacted by action**	**Action owner** (Name and role)	**Date to be completed**
1	Update DPIA to explain what Business Continuity Plan will be applied for NDIT.	10	[redacted]	November 2025
2	Provide details of the process in place to review access to NDIT and to remove access where users change role or leave the organisation	14	[redacted]	November 2025
3	Review plans for NDIT and seek to establish any new Use Cases required (following the procedure set out in the FDP IG Framework).		[redacted]	November 2025
4	Standardised patterns of Controllership in the NDSP submission hub (where submitters can view and amend their submitted data) to be documented.		[redacted]	November 2025
5	DPIA to be shared (after approval) with ICO/NDG, with DGG, and with NHSE DPO/Caldicott Guardian. For review and comments.		[redacted]	July 2025
6	Review and update Level 1 Transparency Information about NDIT	8	[redacted]	October 2025
7	Review and update Level 2 and 3 Transparency Information about NDIT	8	[redacted]	October 2025
8	High-level description of how new dataflows are tested to be added in section 3 (description of processing) prior to any new datasets being ingested.	15	[redacted]	August 2025

Action No	Actions required. (Date and responsibility for completion)	Risk No impacted by action	Action owner (Name and role)	Date to be completed
9	The NDIT Core Platform, Product, and Capabilities group to complete the review and refresh of the DSAR process, with the DPO team.	7	[redacted]	End of August 2025

22.Completion and signatories

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.*

The completed DPIA should be submitted to the NHSE Privacy Transparency and Trust IG Team (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	[redacted]
Signature	[redacted]
Date	21/07/2025

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 (Data sets 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 Data sets 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