Template Version	NHS FDP National DPIA Template (Pseudo) version 1.1 240424		
Document filename	**NHS FDP Data Protection Impact Assessment – NHS FDP National Ontology**		
Directorate / Programme	NHS FDP Programme	Name	NHS FDP National Ontology
Document Reference No	**IG2023182**	Information Asset Register Number	*FDP 011N*
Information Asset / Product Owner Name	[redacted]	Version	11.0 Final Approved
Author(s)	[redacted]	Version issue date	*13/06/2025*

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.*

NHS FDP Data Protection Impact Assessment – NHS FDP National Ontology

Document Management

Revision History

Version	Date	Summary of Changes
0.1	04/04/2024	Creation of final document for DGG approval
0.2	03/05/2024	Moved onto new template
0.3	09/05/2024	Updated and amended to reflect comments from DGG and NHSE IG
0.4	09/05/2024	Updated and amended to reflect additional comments
0.5	15/05/2024	Final approval review updates and actions added
1.0	16/05/2024	Final approved, signed version
2.0	15/11/2024	Updated to reflect the inclusion of additional data sets
3.0	18/12/2024	Updated to reflect the provision of the Places Ontology Dataset to UHL
3.1	08/01/2025	Updated to include the addition of aggregate data from ambulance service, operational data and pseudonymised pathway data
4.0	08/01/2025	Final Approved
4.1	19/02/2025	Updated to include the PLICS datasets.
5.0	19/02/2025	Final updated approved
6.0	19/03/2025	Updated to include the ability to egress metrics data
7.0	25/03/2025	Updated to include additional datasets from UDAL for use in the analytical workspaces
8.0	01/04/2025	Updated to include an NCDR – PET Pseudo look up table and to add Bridges to Health anonymised dataset to the ICB area
8.1	09/05/2025	Update to include Community HODF data
9.0	09/05/2025	Final Updated Approved DPIA
10.0	21/05/2025	Update to include NMTR data
10.1	06/06/2025	Update to include the remaining UDAL datasets
10.2	10/06/2025	Review from NHS E IG
10.3	13/06/2025	Clean version for final approval
11.0	13/06/2025	Final Approved

Reviewers

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

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[redacted]	Deputy Director for IG Delivery Data & Analytics	04/04/2024	V0.1
[redacted]	Deputy Director for IG Delivery Data & Analytics	03/05/2024	V0.2

[redacted]	Head of IG – FDP	15/11/2024	V0.3/0.4/2.0/3.0/4.0
[redacted]	Head of IG – FDP	19/02/2025	V4.1
[redacted]	Head of IG – FDP	19/03/2025	V5.0
[redacted]	Head of IG -FDP	25/03/2025	V7.0
[redacted]	Head of IG -FDP	09/05/2025	V8.1
[redacted]	Head of IG – FDP	21/05/2025	V10.0
[redacted]	Deputy Director for IG Delivery Data & Analytics	10/06/2025	V10.1
[redacted]	Deputy Director for IG Delivery Data & Analytics	13/06/2025	10.3

Approved by

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

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
[redacted]	Information Asset Owners		0.5
[redacted]	FDP Programme Delivery Director		0.5
[redacted]	Director of Privacy and Information Governance (Deputy SIRO)	15/05/24	0.5
[redacted]	Head of IG - FDP	08/01/2025	4.0
[redacted]	Head of IG - FDP	19/02/2025	4.1
[redacted]	Head of IG-FDP	19/03/2025	5.0/6.0
[redacted]	Head of IG - FDP	25/03/2025	7.0
[redacted]	Head of IG – FDP	01/04/2025	8.0
[redacted]	Head of IG – FDP	09/05/2025	9.0
[redacted]	Head of IG – FDP	21/05/2025	10.5
[redacted]	Deputy Director for IG Delivery Data & Analytics	13/06/2025	11.0

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 Ontology 11
2. Data Flow Diagram 11
3. Description of the Processing 14
4. Purpose of Processing Personal Data for this Product 15
5. Identification of risks 16
6. Compliance with the Data Protection Principles - for Processing Personal Data only 18
7. Describe the legal basis for the Processing (collection, analysis or disclosure) of Data? 18
8. Demonstrate the fairness of the Processing 21
9. What steps have you taken to ensure individuals are informed about the ways in which their Personal Data is being used? 22
10. Is it necessary to collect and process all Data items? 23
11. Provide details of Processors who are Processing Personal Data in relation to this Product 24
12. Describe if Data is to be shared from the Product with other organisations and the arrangements in place for this 25
13. How long will the Data be retained? 25
14. How you will ensure Personal Data is accurate and if necessary, kept up to date 25
15. How are individuals made aware of their rights and what processes do you have in place to manage requests to exercise their rights? 25
16. What technical and organisational controls in relation to information security have been put in place for this Product? 25
17. In which country/territory will Data be stored or processed? 26
18. Do Opt Outs apply to the Processing? 26
19. Risk mitigations and residual risks 27
20. Actions 35
21.Completion and signatories 35
22. Summary of high residual risks 36
Annex 1: Defined terms and meaning 37

Purpose of this document

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

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

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

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

Defined Terms used in this DPIA

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

Standard wording in this DPIA

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

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

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

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

The aims of the Federated Data Platform (FDP)

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

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

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

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

The Federated Data Platform (FDP)

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

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

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

1. Better outcomes and experience for people

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

2. Better experience for staff

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

3. Connecting the NHS

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

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

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

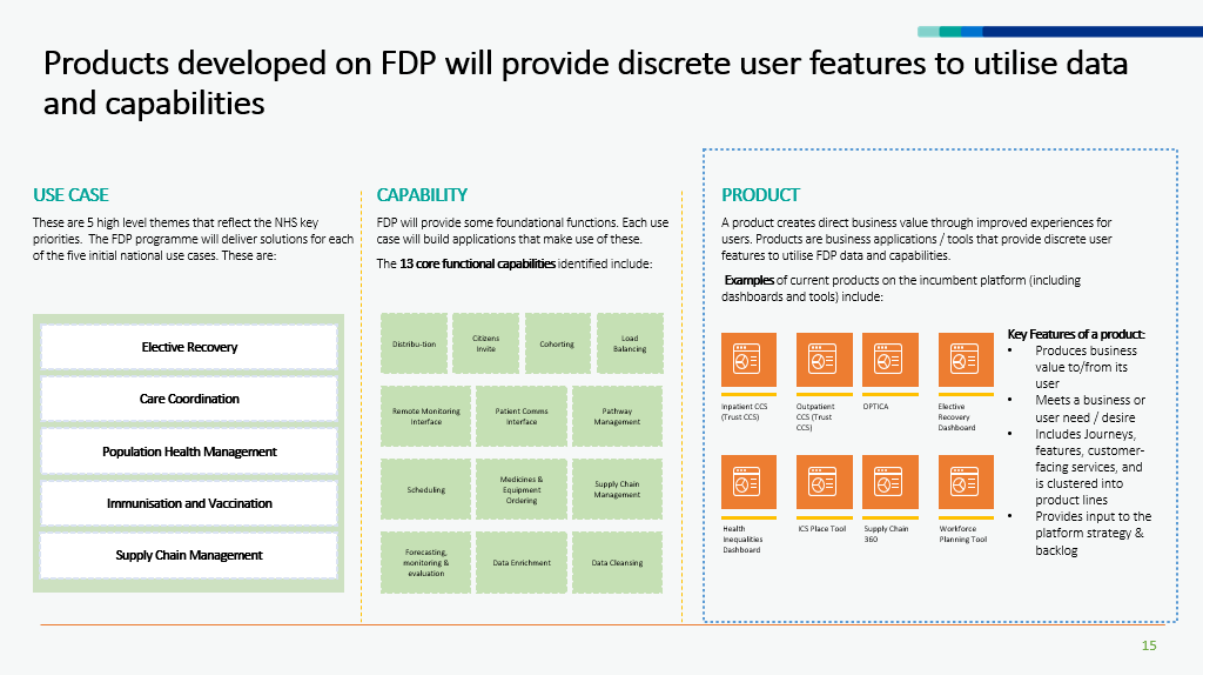
The FDP will not only provide the cutting-edge software to Trusts and ICBs to continue to innovate but the connectivity will enable NHS England (NHSE) to rapidly scale and share innovative solutions that directly addresses the challenges most pressing for the NHS. This will transform the way the NHS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

The ‘Product’ Data Protection Impact Assessment (DPIA)

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

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

This DPIA, which is based on a Product DPIA, is a stand alone DPIA for the FDP Ontology which contains the data used to support the creation of other Products. This DPIA has therefore been amended to reflect that it is assessing the risks relating to the Ontology and not a Product, for which there are separate DPIAs and Screening Questionnaires.



Key information about the Ontology

Purpose of the Ontology - Overview

The FDP National Ontology (Ontology) is a collection of curated and transformed Pseudonymised datasets and place and metric datasets which use Aggregated Data and Operational Data, which together provide the data sources in FDP for many of the national Products.

The purpose of the Ontology is to provide NHS England with a single consistent data source to support Products in the national Instance. This ensures that when different Products are developed, the data being used is consistent, quality assured and in the agreed format.

The Ontology is an essential tool for NHSE and is central to the operation of the FDP. It enables NHSE to manage and exchange data between disparate systems and applications. It provides a standardised format for data exchange, facilitates data governance, and reduces data integration costs. Implementation of the Ontology, will streamline data management processes, improve decision-making, and enhance NHSE's overall performance.

The Ontology as a whole is never made available to external organisations and access to it within NHS England is limited to a small number of developers only who have

responsibilities for maintaining the Ontology. When creating Products which are rolled out to the National FDP Instances, data from the Ontology may be used. Each Product DPIA using data from the Ontology will detail exactly what data has been used in the development of the Product in the form of a Data Specification which detail the datasets from the Ontology and either the data items or a description of the relevant data items.

The Ontology is not a Product in its own right but provides a core capability in enabling developers to draw down specific data and metrics from the datasets within it to support the development of Products. The Ontology does not fall within a specific use case but each Product using data/metrics from the Ontology will set out the specific use case relating to the purpose of their Product in the relevant Product DPIA or Screening Questionnaire.

As part of this DPIA, there is an Annex that details all of the Data that is being collected within the Ontologies and the legal basis that is attributed to the Datasets.

Update November 2024:

The following additional datasets are now being processed within the Ontology, these data sets are currently collected by NHSE in line with the lawful basis described in section 7 of this DPIA:

- Master Patient Index
- NHS Places (this is published data)
- Bridges to Health
- Mortality dataset

Update December 2024

University Hospital Leicester will be provided with the Places Ontology Dataset, which is a fully aggregate or Operational Data set, within their Data Warehouse on their FDP Instance

Update January 2025:

There is a request to ingest further data sets which are held within UDAL to provide a full data set which is required within the Ontologies Product and will allow for better analysis and functionality.

As there are a number of different datasets to ingest, the data flow diagram spreadsheet also lists each of the tables and the column names required to be ingested.

A summary of the tables required is listed below:

Pathways,

IUC Telephony,

999 BT Call Data

Pseudonymised Data

Ambulance AQI,

Monthly IUC ADC, Ambulance Scorecard data

Aggregated Data

NHS Model and dictionary reference Data,

Operational Data

ECDS Technical Output Specification

Update February 2025

There is a request to ingest the PLICS datasets which are held within UDAL to provide a full data set which is required within the Ontologies Product and will allow for better analysis and functionality.

Update March 2025:

There is a requirement for a limited number of approved users to be able to egress metrics data from this product to enable updates to SRO's and pillar leads on the use of this Product.

Update March 2025:

There is a request to ingest further datasets from UDAL to FDP for analysis within the Analytical Workspaces. This includes pseudonymised and aggregate data.

Update April 2025:

There is a request to create a pseudonymised look up table between NCDR and PET within this Product, there is no new data sets being ingested as a result of this update.

Update May 2025

The Community HODF Data is being added to the Ontologies Data specification.

Update May 21st 2025:

National Major Trauma Registry Data is being added to the Ontologies Data specification.

Updated June 2025

There is an update to the Ontologies to include further Datasets within UDAL to be migrated into FDP. The CVDPrevent Dataset cannot be utilised within the Analytical Workspaces within NHS England FDP at this time. NHS England are moving the majority Datasets from UDAL into FDP in order to provide a consistent Data source, this is due to the FDP by default and FDP first programmes which require NHS England to utilise the functionality within FDP when processing Data that NHS England collects.

Additionally, the Engineering Catalogue and the RC Benchmarking Data Schema have been included in this update to support with the curation of data within the Ontologies. The Engineering Catalogue and RC Benchmarking and the Datasets within these can only be utilised within Ontologies for NHS England FDP at this time.

Local or National Instance			
Local	☐	National	☒

Categorisation of the Data used to create the Ontology		**How the different Categories of Data are used in relation to the Ontology**
Directly Identifiable Personal Data	☐	
Pseudonymised Data	☒	For Data ingested into the FDP to create the Ontology
Anonymised Data	☒	For Data ingested into the FDP to create the Ontology
Aggregated Data	☒	For Data ingested into the FDP to create the Ontology
Operational Data	☒	For Data ingested into the FDP to create the Ontology
Type of Data used in the Ontology		
No Personal Data	☒	Aggregated Data and/or Operational Data is ingested into FDP to create the Ontology.
Pseudonymised Personal Data	☒	For Data ingested into the FDP to create the Ontology

Pseudonymised Special Category Personal Data	☒	For Data ingested into the FDP to create the Ontology

The Ontology DPIA describes:

- the purpose for the creation of the Ontology;
- the Data which has been processed to create the Ontology;
- the supporting legal basis for the collection, analysis of that Data;
- the Data flows which support the creation of the Ontology, and
- the risks associated with the Processing of the Data and how they have been mitigated.

1. Consultation with Stakeholders about the Ontology

The Ontology is essentially a reference library of datasets which NHSE developers can draw upon to support NHS England teams in developing products which at present is only used to create national products. In the future, there is an ambition for Ontologies to used when creating local products, before this takes place, this DPIA will need to be updated. It provides a standardised format for data exchange, facilitates data governance, and reduces data integration costs. Implementation of the Ontology will streamline data management processes.

The subject matter experts (SME's) responsible for the NHS England National Commissioning Data Repository (NCDR) Data and the Unified Data Access Layer (UDAL) were consulted to ensure the data was processed and transformed according to their expectations and data quality was checked and signed off by the relevant SME. The SME's sit within the NHSE PAT team, along with the NHSE Data and Analytics Team who provide best practices to avoid data duplication and to assist in the quality assurance process to ensure that products are created correctly.

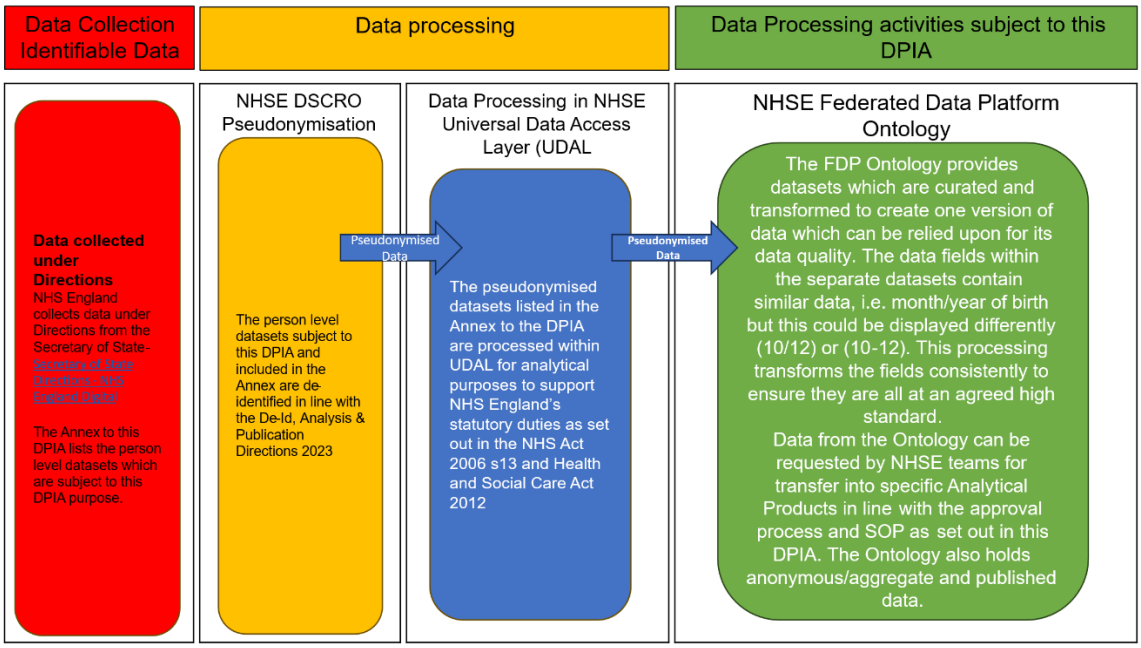
The process of accessing to the Data will be determined in the individual Product DPIAs, in consultation with the Information Asset Owners (IAO).

2. Data Flow Diagram

Pseudonymised datasets are used in the Person Ontology

All Pseudonymised Data ingested into the Federated Data Platform (FDP) flows through the Person Ontology before being made available to Products. This enables the Data to be conformed in terms of data quality standards and assigned to specific events. Processing includes using the Pseudonymised Data sourced from NCDR/UDAL to create cleaned and enhanced data in the Person Ontology that can be further used to calculate metrics in Metrics Ontology.

Person Ontology is a store of person level datasets e.g Emergency Care Dataset patient level data.



Update February 2025

In addition to the Data collections listed above PLICS will also be included.

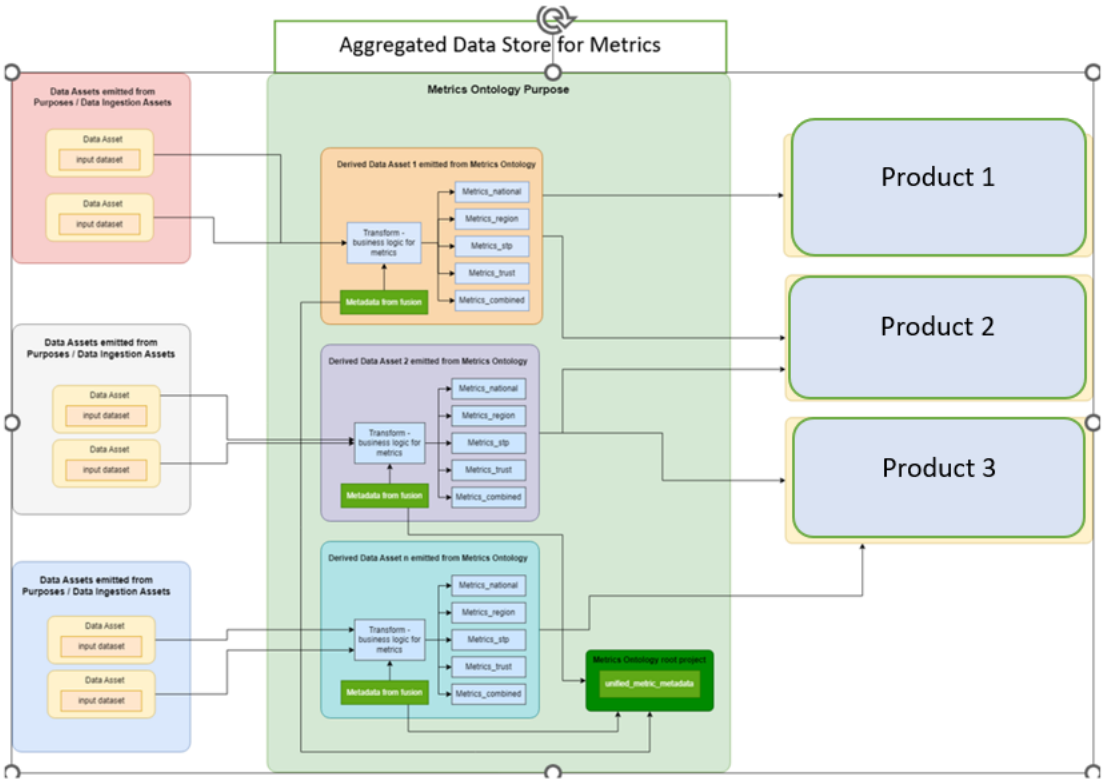
Update April 2025:

The inclusion of an NCDR-PET pseudonymised look up table within the Product.

Metrics Ontology

Aggregated Data or Operational Data is used in the Metrics Ontology.

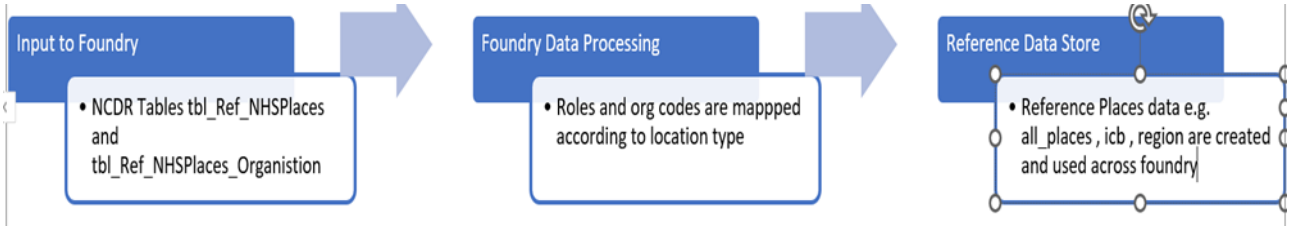
The Metrics Ontology is a central store of aggregated Metrics, some of which are Aggregated Data derived from Pseudoymised Data and some of which are Operational Data. For example, A&E Metrics has metrics / calculations like number of total admissions etc. This is described in the data flow diagram below:



Place Ontology

Operational Data is used in the Place Ontology.

The Place Ontology is the reference data store for all organisation codes for example metadata information of all ICBs, Trusts, Regions.



National Ontology

National Ontology uses data from Metrics ontology and Person Ontology to calculate application specific aggregated metrics that are shown on front end dashboards in Products.

Canonical Data Model (CDM)

CDM is the ontology currently used in the local FDP instances (Trusts) to support operational applications and will be transitioned into FDP. There is a demo version of CDM in National FDP instance which uses synthetic data. This application is not used by business users. The CDM only uses notional/synthetic data.

3. Description of the Processing

The Person Ontology is part of a centralised reference library which allows the NHSE platform developers to bring together different datasets in the way analysts require for use in approved Products for the approved purpose.

The processing in FDP is as follows:

1) Data is cleaned up and converted to standardised format. For example Dates are consistently kept in a format 'YYYY-MM-DD'. Dataset and Column Naming conventions are followed.
2) Duplicate records are removed.
3) Datasets are joined to reference datasets to enhance the codes to meaningful values.

For example: Emergency dataset has department codes but they are not meaningful to users. Hence we join with other datasets to bring in department names instead of codes. Such as department code '01' is changed to department name 'Acute'.

All patient-level Pseudonymised Data ingested into the Federated Data Platform (FDP) flows through the Person Ontology before being made available to Products. This enables the data to be validated and transformed in terms of data quality standards and assigned to specific events. Processing includes using the Pseudonymised Data sourced from NCDR/UDAL to create cleaned and enhanced data in the Person and National Ontology that can be further used to calculate metrics in Metrics Ontology and calculate forecasts in forecasting tools. Data can be derived from the Pseudonymised Person Ontology to be enhanced for specific product requirements.

Principles of the Ontology:

- Patient level Pseudonymised Data is organised as entities and events
- A sub folder to be created as per the names of the entities and events
- Patient pseudo id serves as the link between the pseudonymised datasets
- Data will be organised as bronze, silver and gold. The Classification is an approach to organise the data within FDP. These are data quality categories.
    - **Bronze Data** quality means that the datasets are mostly raw and are not enhanced or transformed in any way. This is mainly used in combination with the Person Ontology to produce the silver and gold data sets. The Bronze data set may also be used when a Product requires raw data as it is ingest. The use of this dataset is minimized to where it is absolutely necessary.
    - **Silver Data** quality ensures that the data set have following standards:
        - IG restrictions and requirements are documented on the dataset
        - Metadata of columns will be documented on the dataset
        - Dataset has Health checks and monitoring to ensure that they are timely refreshed and data quality checks are applied to ensure row counts are as expected.
        - The documentation should capture the process on versioning datasets. e.g. deprecation of older versions of datasets.
        - Use reusable functions for standard transformations / business logic.
    - **Gold Data** quality datasets ensure that where there are multiple sources of data, data is combined to have the most reliable and timely data . For example for Inpatients dataset (which land in Person Ontology and is then aggregated in Metrics Ontology and are used to create Products such as ERD Dashboard and POD), where we have data from SUS and SUS sources, SUS Data is more reliable and Faster SUS is more timely and is

used to create national Products such as ERD Dashboard and POD. Hence they are combined to fill in the latest data from Faster SUS and older data from SUS. All silver level standards are also applicable to Gold data category.

- The IG Restrictions are documented in Ingestion forms. IG Restrictions will be implemented using the user access model in FDP.

The datasets are not linked together however they may be linked at the point they are required for a particular Product. This linkage will be detailed in the relevant Product DPIA.

4. Purpose of Processing Personal Data for this Product

The whole Ontology is made up of 5 separate areas – Person, Place, Metrics, National and the Standard Healthcare Ontology.

The **Person Ontology** serves as the single source of the truth for Pseudonymised patient level datasets which will be the source of data that is used within some of the Products.

The **Metrics Ontology** serves as the single source of truth for metrics which are used across Products. This is count data, so typically has counts of activity. This may be Aggregated Data or Operational Data.

The **Place Ontology** is the reference data store for all NHS organisations codes for example metadata information of all ICBs, Trusts, Regions. This Ontology therefore contains Operational Data.

The **National Ontology** National Ontology uses data from Metrics ontology and Person Ontology to calculate application specific aggregated metrics that are shown on front end Product dashboards and provides restricted views on Aggregated Data with metadata information like User Access Scopes and Application specific schema. This means that there are restrictions applied on the Rows of the Data Tables depending on the User groups. For example, a regional user shouldn't be able to see all data and should be a ble to see only records for the region they belong to. These restrictions are applied in the National Ontology

The **Standard Healthcare Ontology (SHO)** is currently only a demonstration version of the SHO which uses synthetic data (Synthetic data is created using a python library FAKER https://faker.readthedocs.io/en/master/ . We don't use actual NHS Data in anyway while creating the synthetic data. It is all fake data) which has been created by Palantir following an agreed methodology.

Purpose

All Products in the National Instance of the Federated Data Platform will use data from the Ontologies. Datasets within the Ontology will only be used to support approved FDP Products

The purpose of the Ontology is to have a curated set of datasets, conformed to provide one version of the truth for teams in NHS England creating Products for the national Instance of FDP which will require the use of some or all of the data in the Ontologies. Previously, each Product ingested datasets of similar kind creating their own data pipelines. We now have created the Ontology where all pseudonymised patient level datasets that are required for all current Products in Foundry (that will move over to FDP)

are onboarded and this will allow users migrating and creating FDP Products to use this library instead of creating their own data pipelines.

The Person Ontology currently holds activity data for citizens in different care settings. The data is Pseudonymised Data and therefore does not identify an individual. It allows Products to be created which can provide a view of care activity associated with an individual across the different datasets. For example, currently this data is required for the A&E Risk Likelihood Dashboard. Developers and analysts are not able to identify the patient even after linking the datasets as they only have access to Pseudonymised information and residence postcodes.

For example, a patient may have received inpatient care, then outpatient care leading on to care being provided in a community setting. For the purposes of use in a Product, the data in the Ontology allows a patient's pathway to be followed to understand their care journey and outcomes, without identifying the individual.

Inpatients datasets are used in various Products such as for example, ERD Dashboard and POD Dashboard, to show the Average Length of Stay for Patients. The Inpatients data lands in Person Ontology, then is aggregated in Metrics Ontology and then used in the Products. Ontology datasets are used in multiple Products after they are aggregated in the Metrics Ontology.

The Ontology enables good data governance. By defining a standard for data structure and meaning, the Ontology can help to ensure data quality, consistency, and accuracy in the data used to support Products. This, in turn, supports better quality information in Products, supports more informed and effective decision-making, more effective collaboration, and is centrally located avoiding duplication of data items and pipelines. It is therefore a more secure way of using the data and upholds the data minimisation principle of not using more data than is necessary.

The Ontology also significantly reduces data integration costs. Instead of having to build and maintain separate data mapping and transformation processes for each Product, the Ontology provides a single source of truth that can be used by all Products. This eliminates the need for custom integration code, which can be costly and time-consuming to develop and maintain.

The Ontology underpins all of the Products in the National Instance of FDP as it contains the data which they need.

The data in the Ontology is only accessible to a restricted number of NHSE developers in order that they can work with the Product owners to draw into the Product the correct data items required for the Product.

5. Identification of risks

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

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

Risk No	Describe source of the risk and nature of potential impact on individuals *The highlighted text are the most identified risks in the programme. Please amend and delete as appropriate and add Product specific risks. If the Data being processed is Directly Identifiable Personal Data, the risks will be different from below and you should refer to this category of Data. If the Data being processed is only Aggregated Data, then most of the risks below, other than small number suppression, may not be relevant.*
1	There is a risk that Pseudonymised Data may be accidentally misused by those with access.
2	There is a risk that Pseudonymised 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 Pseudonymised 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 Pseudonymised Data (e.g. encryption, access controls)
5	There is a risk that Pseudonymised Data could be deliberately manipulated by an internal bad actor in some way to re-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 FDP or the Product, preventing individuals from having access to all Personal Data held about them.
8	There is a risk of failure to provide appropriate transparency information to data subjects.
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 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 Personal Data is processed in the Ontology which is not required for approved Products.

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

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

Data Protection Principle	Section addressed in this DPIA
Lawfulness, fairness and transparency	Section 7 (Lawfulness); Section 8 (Fairness); Section 9 (Transparency) and 11 (Processors)
Purpose limitation	Section 4
Data minimisation	Section 10
Accuracy	Section 14
Storage limitation	Section 13
Integrity and confidentiality (security)	Section 12 & 16
Accountability	Accountability is addressed throughout the DPIA. In particular, Section 21 includes approval of the residual risks by the Information Asset Owner and on behalf of the SIRO.

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

Statutory authority: *This is for national Products only, please remove the Datasets which are not applicable and remove the highlight and/or amend as necessary.*

NHSE's various statutory authorities for collecting, Processing, analysing and sharing Data are set out in the table below.

Source Dataset	Statutory Authority for collection of Data	Statutory Authority for Processing & Analysis of Data	Statutory Authority for sharing of Data
Secondary Use Services+(Admitted Patient Care Episodes)	Spine services (no 2) 2014 Direction	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing
NHS BSA Primary Care Medicines	NHS Business Services Authority (NHSBSA) Medicines Data Directions 2019	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is

Statutory authority: *This is for national Products only, please remove the Datasets which are not applicable and remove the highlight and/or amend as necessary.* NHSE's various statutory authorities for collecting, Processing, analysing and sharing Data are set out in the table below.			
Source Dataset	**Statutory Authority for collection of Data**	**Statutory Authority for Processing & Analysis of Data**	**Statutory Authority for sharing of Data**
			separately considered for sharing
Mental Health Data Set	Mental health services Directions 2020 - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing
COVID-19 Vaccination Status	COVID-19 Public Health Directions 2020 - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Diagnostic Imaging Dataset (DID)	Diagnostic Imaging Dataset (DIDS) - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Community Services Dataset (CSDS)	Community Services Dataset (CSDS) - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Emergency care data set	Emergency care data set collection Directions 2017 - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Civil Registration of Deaths Dataset	The Health and Social Care Act 2012 (HSCA 2012) section 254.	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Patient Level Information and	The Health and Social Care Act	Patient Level Information and	Not applicable as no data is shared from the

Statutory authority: *This is for national Products only, please remove the Datasets which are not applicable and remove the highlight and/or amend as necessary.* NHSE's various statutory authorities for collecting, Processing, analysing and sharing Data are set out in the table below.			
Source Dataset	**Statutory Authority for collection of Data**	**Statutory Authority for Processing & Analysis of Data**	**Statutory Authority for sharing of Data**
Costing Systems (PLICS)	2012 (HSCA 2012) section 254.	Costing Systems (PLICS) Mandatory Collections continued implementation Mandatory Request Information System - NHS England Digital	Ontology, only Products, where legal basis is separately considered for sharing.
Secondary Use Services+(Admitted Patient Care Episodes)	Data services for commissioners Directions 2015 (as amended) until revoked by the Healthcare Operational Data Flow Directions 2024 when issued	Further processing: Healthcare Operational Data Flows Directions 2024 and NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Master Person Index	Primary care registration management Direction 2018	NHS England De-Identified Data Analytics and Publication Directions 2023	Not applicable as no data is shared from the Ontology, only Products, where legal basis is separately considered for sharing.
Ontologies Data Schema Datasets in UEC	Data Schema for each dataset provides more detailed information on the data fields used in each dataset.		
Additional Aggregate Datasets	Additional Aggregate datasets to be ingested from UDAL		

Statutory authority: *This is for national Products only, please remove the Datasets which are not applicable and remove the highlight and/or amend as necessary.*

NHSE's various statutory authorities for collecting, Processing, analysing and sharing Data are set out in the table below.

Source Dataset	Statutory Authority for collection of Data	Statutory Authority for Processing & Analysis of Data	Statutory Authority for sharing of Data
Additional Pseudonymised Datasets	Additional pseudonymised datasets to be ingested from UDAL		
NMTR Data Spec May 2025	Additional pseudonymised NMTR dataset to be ingested into Ontologies		

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

Article 6 – Personal data

- Article 6(1)(c) processing is necessary for compliance with a legal obligation, where NHS England collects and analyses data under the Directions listed above (**Legal Obligation**).

Article 9 – Special category personal data

- Article 9(2)(g) processing is necessary for reasons of substantial public interest, where NHS England is processing under Legal Obligation under Direction **(Substantial public interest),** plus Schedule 1, Part 2, Paragraph 6 '*statutory etc and government purposes'* of DPA 2018

Common Law Duty of Confidentiality

Legal obligation – NHSE is required by law to process Confidential Patient Data it collects and analyses and which is used in the Ontologies to support Products. This is required under legal directions referred to above and issued by the Secretary of State for Health and Social Care to NHSE under section 254 of the Health and Social Care Act 2012.

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.

All Personal Data contained in the Person Ontology has been collected and Pseudonymised under legal direction. Transparency information is provided for each approved Product that uses Personal Data from the Person Ontology. As all Products migrate to FDP, Privacy Notices for them will be provided, increasing the current level of transparency over processing of the Personal Data in products on the existing Foundry platform. Further information is set out in section 9 below.

Regarding the impact on individuals, the purpose of collecting and using the data is to ensure that the NHS can operate and effectively and efficiently to provide and co-ordinate

the care of individuals. The processing of this data will provide a single version of all datasets which will be used within approved Products on FDP. This will ensure that data quality standards are managed appropriately and only the minimal amount of data is used to achieve the aim(s) of the Product.

Any potential adverse impact to individuals is also mitigated by the Personal Data being processed for this Product having been Pseudonymised before it is shared into FDP.

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

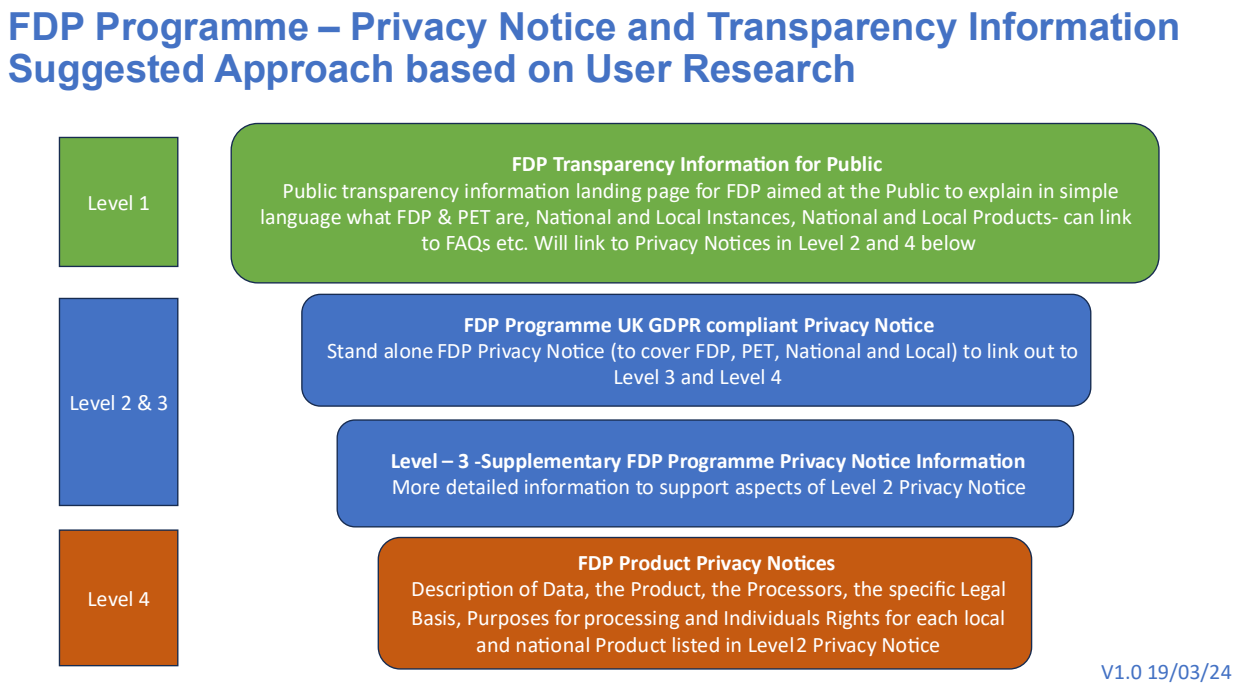
There is a range of information available on the NHS England website about FPD and how it works. This is Level 1 Transparency information.

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

NHS England » NHS Federated Data Platform privacy notice

There is also a privacy notice for each Product at Level 4 available via this link:

NHS England » FDP products and product privacy notices



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

All of the Personal Data items processed for the production of the Ontology is Pseudonymised or has been derived to create Aggregated Data before flowing into FDP. The items listed below are therefore only items which are Pseudonymised Data items flowing into FDP or the Product.

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	No	
Address	No	
Postcode	Yes	Provider postcodes are present for use cases where we need to identify patient care depending on their provider deprivation but patient is not identifiable from the provider postcode. patient postcodes are not available.
Date of Birth		
Age	Yes	To support Products analysing data in different age cohorts.
Sex	Yes	To support Products analysing data in different sex cohorts.
Marital Status		
Gender	Yes	To support Products analysing data in different gender cohorts.
Living Habits	Yes	Smoking / Drinking habits in patient health records but individual patient not identifiable. Used to identify how habits influence some diseases such as Cancer, Heart attacks.
Professional Training / Awards / Education		
Email Address		
Physical Description		
General Identifier e.g. NHS No	Yes	Pseudonymised Patient Id is present, and NHS No is not retrievable from it and patient is not identifiable.
Home Phone Number		
Online Identifier e.g. IP Address/Event Logs		
Mobile Phone / Device No / IMEI No		
Location Data (Travel / GPS / GSM Data)	Yes	Provider location details present as postcode. Used to measure performance of providers.
Device MAC Address (Wireless Network Interface)		
Spare – add Data item (as necessary)		
Spare – add Data item (as necessary)		
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	Not Patient identifiable. Data about symptoms, diagnosis, treatment and outcomes required to support the Product. See the Data Specification
Sexual Life / Orientation		
Religion or Other Beliefs		

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]*
Racial / Ethnic Origin	Yes	Used to support Products analysing data with reference to racial or ethnic origin . But individual patient cannot be identified.
Biometric Data (Fingerprints / Facial Recognition)		
Genetic Data		
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences		

Please see the detailed Data Specification above which identifies the source Datasets and specific Data items.

Dataset with subset in Person Ontologies

Update February 2025 – Inclusion of PLICS datasets.

FoC Specification V5.0 (2)

NCC 2024-25 - Output Specifications - Integrated Collection

Update May 2025

HODF Community Data Specification

Update June 2025 – RESTRICTION – CVD Prevent cannot be utilised within the Analytical Workspaces within NHS England FDP. The Engineering Catalogue and RC Benchmarking and the Datasets within these can only be utilised within Ontologies for NHS England FDP at this time.

Existing UDAL Datasets

RC Benchmarked Data Schema

Engineering Catalogue - Copy of udal_catalogue_datasets

Engineering Catalogue - Copy of udal_objects

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 NHS England as a Controller in relation to Processing Pseudonymised 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:

  Ontologies - FDP Annex v1.0 Approved

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

The Ontology will not be shared with any other organisations and access is restricted to developers within NHSE only.

13. How long will the Data be retained?

The Data will be kept in line with business requirements for the purposes of providing data to support Products. At the point that the Product is decommissioned, an assessment will be undertaken to ascertain whether any of the Data can be destroyed, or a retention period agreed in line with the NHS Records Management Code of Practice 2021.

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

When the data is initially collected under legal Direction the data quality is verified and any anomalies rectified. This is standard practice which ensures that the data is of good quality before it is Pseudonymised for secondary use purposes.

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 each approved FDP Product.

The following rights under UK GDPR apply to the Processing of Personal Data (Pseudonymised Data) to produce the Person Ontology:

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

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

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.

Specific Access controls for Ontology

Access to the Ontology is restricted by role based access controls to a limited number of NHSE developers (currently 4). The developers are responsible for supporting Products which migrate to FDP and support product development which has been approved through the FDP governance process.

The process of accessing to the Data will be determined in the individual Product DPIAs, in consultation with the Information Asset Owners (IAO).

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 the Person Ontology as:

- the collection and analysis of Data by NHS England to create the Person Ontology that supports Products has been carried out under a legal obligation (the Legal Directions) and therefore the National Data Opt out does not apply.
- No Confidential Patient Information will be processed within the Person Ontology, therefore the National Data Opt out does not apply.

Type 1 Opt Outs do not apply because the Datasets used in the Person Ontology do not contain Confidential Patient Information that has been collected by NHS England from GP Practices.

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	Pseudonymised 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 NHS England. 2. No external users have access to Pseudonymised Data in the Person Ontology. All internal users are required to sign security operating procedures that confirm their responsibilities to protect Data. Internal users are also subject to contractual confidentiality requirements. 3. The download functionality of Data from the FDP is disabled by default, and access to this is controlled by the	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
		Product Owner which ensures appropriate governance in in place. 4. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Pseudonymised Data to only those with a legitimate need eg developers of a Product. 5. The FDP access audit logs ensure that all access is logged and can be fully audited.					
2	Pseudonymised 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.The data is being regularly refreshed to ensure that it is up-to-date and is therefore will be required as long as the Person Ontology is in place. 3. A Records Management Information Co-ordinator will provide advice on how long Data should be retained at the point a Product is decommissioned.	Section 13	Tolerate	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the Personal Data	1.Appropriate organisational measures in relation to Data controls and governance are in place to ensure the security of the Data. 2. Organisational measures are adhered to across the Data platform.	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
	(e.g. policies, procedures, disciplinary controls)	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 to only 4 NHSE developers.					
4	Insufficient technical measures are in place to ensure appropriate security of the Personal Data (e.g. encryption, access controls)	1. Data is encrypted in storage 2. All Data to and from the platform is encrypted in transit using at least TLS1.2 3. SLSP in place 4. A standard operating procedure will be developed to manage access requests.	Set out in the Overarching FDP DPIA and Section 12 & 16 above	Tolerate	Remote	Minimal	Low
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 NHS England. 2. Staff are trained and fully aware of their responsibilities when analysing 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	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
		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 Pseudonymised Data in any Products, and which prohibits any reidentification 5. The download functionality of Data from the FDP is disabled by default, and access to this is controlled by the IAO which ensures appropriate governance in in place.					
6	Insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures supporting the Product.	1. Full details are described in the Overarching FDP DPIA. 2.For national Products migrating from Foundry to FDP, there is no change in the Products, their operation or the technical measures supporting them. The Ontology currently exists in Foundry and is migrating to FDP as part of the overall product migration work. New governance processes for migrating existing Products have been put in place, including approval of relevant DPIAs by the DGG and the Deputy SIRO. This DPIA has also been put in place to assess the risks in	Set out in the Overarching FDP DPIA and Section 3, 12 & 16 above	Tolerate	Remote	Minimal	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
		relation to the Ontology consistently across all national Products.					
7	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	1. Existing internal NHSE procedures for managing DSARs have been updated to include consideration of any Personal Data held in FDP.	Section 15	Treat	Remote	Minimal	Low
8	Failure to provide appropriate transparency information to data subjects.	1. The NHSE General FDP Privacy Notice has been published and a separate Product Privacy Notices have been produced and will be published on NHS England's website with a link to them from the General FDP Privacy Notice.	Sections 8 and 9	Tolerate	Remote	Significant	Low
9	Increased access to Special Category Personal Data is given to staff	1. Role Based and Purpose Based Access Controls are in place. 2. The Data Processed to create the Ontology has been Pseudonymised before being ingested into FDP.	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
	who would not normally access that Data within their role.	3. Only the developers have access to this Data, who review and approve/deny access requests.					
10	The platform becomes inaccessible to users which could cause availability of Data.	1. The FDP Contractor is required to have Business Continuity Plans in place. 2. The IAO has Business Continuity Plans in place which cover the inaccessibility/unavailability of the data required to populate the Ontology	Section 16	Tolerate	Remote	Significant	Low
11	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 Person Ontology will only collect a sub-set of Personal Data from existing NHSE datasets that are required to support national Products. 2. It is our responsibility to ensure that all Data that is ingested into FDP for use in the Person Ontology is up to date and accurate for the purposes for which it is Processed within the Products. We will use our existing processes relating to the source datasets for maintaining accuracy.	Section 14	Tolerate	Remote	Significant	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
12	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 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 17	Treat	Remote	Minimal	Low
13	Users will not have their permissions revoked when they leave their role/ organisation and may continue to have access to Data they are no longer entitled to access	1. As access to the Ontology is only available to 4 NHSE Developers, the IAO is fully aware of who has access and will revoke access where it is no longer required.	Section 12 & 16	Treat	Remote	Significant	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
14	There is a risk that Personal Data is processed in the Ontology which is not required for approved Products.	1. The Ontology is currently being used to support national Products in Foundry which are migrating across to FDP. Following completion of Product migration work, a review will be undertaken to identify if there are any data items in the Person Ontology which are no longer required. 2. All data ingested into FDP is approved through the data Ingestion Process which involves IG advice to ensure the data is necessary for a Product on FDP.					

20. 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	Section 3 refers to IG Restrictions on datasets being identified at ingestion and captured in ingestion forms. Risk 14 also refers to the ingestion process to manage necessity for data flowing into Ontology. Please can the ingestion process be explained further, including what the criteria is for ingesting data into the Ontology, the source of the IG restrictions on any data (who determines them), what type of restrictions, who completes the forms, where are they stored, who is responsible for reviewing and updating them etc. This will be written into a Standard Operating Procedure (SOP) to be utilised by the developers who have access to the Ontologies.	2 and 14	[redacted]	July 2025

21.Completion and signatories

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	
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