

Overarching Data Protection Impact Assessment (DPIA) for the Federated Data Platform (FDP)

Version issue date 5 July 2024

Contents

Purpose of this document	3
0. Scope	3
1. Consultation with Stakeholders	3
2. Data Flow Diagrams	4
3. Purpose of the processing	5
4. Identification of risks	7
5. Approach to Risk	9
6. Description of the Processing	9
7. Compliance with the Data Protection Principles	12
8. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?	12
9. Demonstrate the fairness of the processing	15
10. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?	16
11. Is it necessary to collect and process all data items?	17
12. Describe if personal datasets are to be matched, combined or linked with other datasets? (internally or for external customers)	19
13. Describe if the personal data is to be shared with other organisations and the arrangements you have in place	20
14. How long will the personal data be retained?	20
15. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date	20
16. How are individuals made aware of their rights and what processes do you have in place to manage such requests?	20
17. What technical and organisational controls for “information security” have been put in place?	21
18. In which country/territory will personal data be stored or processed?	22
19. Do Opt Outs apply to the processing?	22
20. Risk mitigation and residual risks	24
21. Actions	32
22. Definitions	34
23. Joint Controller table	39
NHS England and Local FDP User Organisation Joint Controller Table – V1.0 13 March 2024	39
1. Introduction	39
2. Transparent Manner	39
3. Respective Responsibilities for Compliance, in particular with regard to exercise of data subject rights and duties to provide information in Articles 13 and 14	39
4. The arrangement may designate a contact point for data subjects	40
5. The arrangement must reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects	40
6. The essence of the arrangement shall be made available to the data subject	41
24. Appendix – IG Framework	60

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help organisations demonstrate how they 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”*.

Definitions of specific terms used in this DPIA are included at Section 25.

NHS England (also referred to as "NHSE", and in this DPIA "we" and "our" refers to NHSE) has prepared and published this DPIA to describe generally the processing of personal data by the FDP. NHS England reviews and maintains this DPIA regularly, and may update it periodically.

0. Scope

The Federated Data Platform (FDP) is a series of separate data platforms which we call **“Instances”**. There are data platform Instances which are operated by NHS England, called **“National Instances”**. There are separate data platforms Instances which are operated by an NHS Trust or an Integrated Care Board in a local area, which we call **“Local Instances”**. These National and Local Instances of the data platform work alongside Privacy Enhancing Technology, which we call **“NHS-PET”**. NHS-PET records the data which is used in data platform Instances and can de-identify data where this is needed.

Each Instance of the Data Platform uses the same underlying technology and software and has the same basic technical functionality. However, the Data Platform uses the technology, software, and functionality in different ways for different purposes through what we call **“Products”**. Some Products are only designed for the National Instances, some are only designed for the Local Instances, and some are designed to be used in both types of Instance.

Information about the FDP, including high-level deployment plans is made publicly available on the NHS England website [here](#).

1. Consultation with Stakeholders

Seeking and understanding the views of stakeholders and the public and patients is an integral part of the NHS Federated Data Programme. There is a regular programme of engagement supported by a number of formal advisory groups that form part of the programme governance. These include:

- [FDP check and Challenge Group](#). This group provides strategic advice to the FDP Programme on communications, engagement, and transparency. It considers patient, public, professional, and ethical context, and complements the [Health Data Patient and Public Engagement and Communications Advisory Panel \(PPECAP\)](#).
- [Health Data Public and Patient Engagement and Communications Advisory Panel](#). A panel consisting of public and patient members and representatives from national organisations who represent the views of the public. It supports the FDP FDP Programme to develop meaningful and accessible public communications.

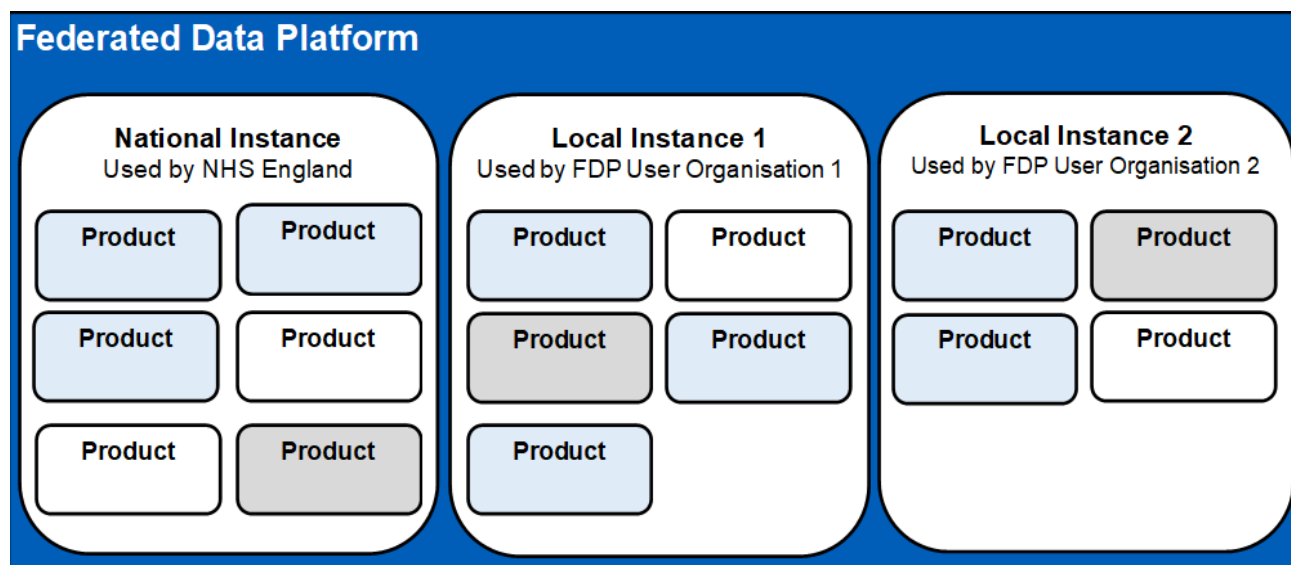
- External IG Advisory Group. A group of external stakeholders with subject matter expertise in data and information governance.
- The Data Governance Group. A national group established by NHS England to provide oversight to the approach to data processing and sharing across all Instances of the Data Platform and NHS-PET which will include membership from across FDP User Organisations

Additionally, the [FDP engagement portal](#), which is hosted on NHS England's website, is a live tool to support the public to seek answers to their questions, provide feedback on the FDP Programme and to register their interest in future engagement activity.

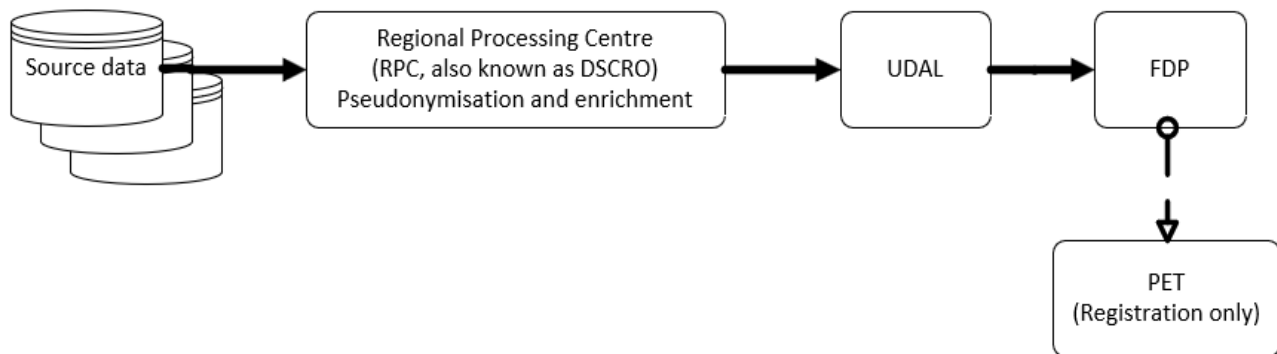
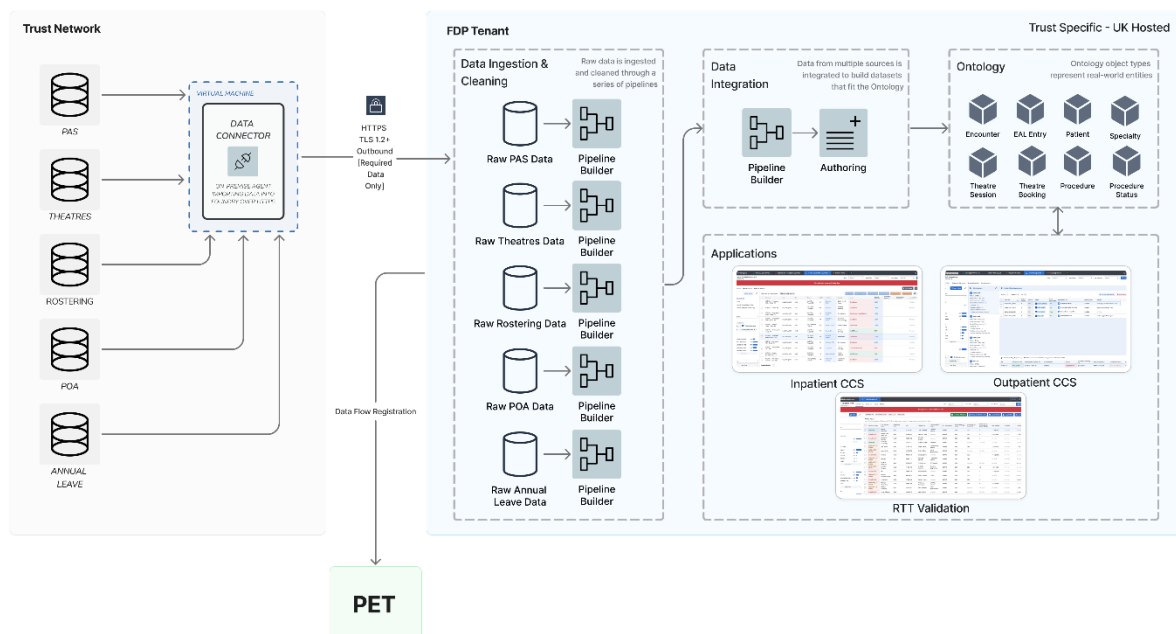
NHS England is committed to communicate and engaging with key stakeholders, the public, and patients in a meaningful way throughout the life of the FDP Programme.

2. Data Flow Diagrams

The FDP allows organisations to hold and process data separately, while using common functionality, as shown below:



The flows of data into the FDP are shown below, with separate diagrams for National Instances (NHS England) and Local Instances:

A. National Instances**B. Local Instances**

Detailed data flow diagrams at each Product level are contained within the separate Product DPIAs.

All FDP Instances are hosted in the UK and all dataflows in and out of the FDP start and finish in the UK.

3. Purpose of the processing

The Federated Data Platform (FDP) is a technology solution to support a variety of NHS organisations in the efficient delivery of their statutory functions, including delivering and supporting Direct Care. The FDP is made available for NHS organisations to use if they choose to do so. This is the purpose for which FDP User Organisations process Personal Data in FDP (and for which Commissioned Health Service Organisations may use FDP, if permitted).

The FDP is designed to be a common system that can be used by many different organisations. Each organisation has a separate space (called an “Instance”), where their data is held securely, and separate from data belonging to other organisations. The separate organisations are referred to as “FDP User Organisations”, with each of those FDP User Organisations retaining autonomy (and control over the identification of purpose) over the use of any data they choose to put in their Instance.

As set out in Section **Error! Reference source not found.**, where NHS England is the FDP User Organisation, this may be referred to as the “National Instance” of FDP. For all other FDP User Organisations, the Instances may be referred to as “Local Instances” of FDP. The FDP enables FDP User Organisations with an Instance to process data for the following five use cases:

1. **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.
2. **Care coordination** (Joining up care) – 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.
3. **Vaccination and immunisation** – to ensure that there is fair and equal access, and uptake of vaccinations across different communities.
4. **Population health management** (Planning NHS services) - to help local trusts, Integrated Care Boards (on behalf of the integrated care systems) and NHS England proactively plan services that meet the needs of their population.
5. **Supply chain management** (Getting the best value for the NHS) – to help the NHS put resources where they are needed most and buy smarter so that we get the best value for money.

FDP User Organisations will use the Data Platform initially through Products, each Product being linked to one or more of the Use Cases .FDP will help provide NHS staff (frontline clinicians, operational staff, and planners) with timely information and insight, promoting the efficient use of resources to support the delivery and planning of patient care.

FDP functionality is classified as 13 Core Capabilities which are:

- Distribution
- Citizens Invite
- Cohorting
- Load Balancing
- Remote Monitoring Interface
- Patient Comms Interface
- Pathway Management
- Scheduling
- Medicines and Equipment Ordering
- Supply Chain Management
- Forecasting, Monitoring, and Evaluation
- Data Enrichment
- Data Cleansing

Where these capabilities are used in a Product, this will be described in the relevant Product DPIA.

For Trusts, the ambition is that the FDP will enable users to undertake data analysis and access applications designed to support and enable planning, pathway management and Direct Care.

At ICB level, the FDP will support population health management, tackling health inequalities and care coordination, enabling Integrated Care Systems (ICSs) to respond to a more comprehensive and detailed understanding of their populations, supporting a targeted, more effective use of resources and planning services around the needs of their population.

The National Instance of FDP will improve the flow and analysis of reporting data. As a consequence, there will be a reduction in burden through the change from multiple systems using aged technology (e.g. Excel), and enhanced security and transparency. This will give NHS England teams more accurate and near-real-time data to undertake strategic and operational planning.

The FDP IG Framework has been created to enable the management of the information governance (IG) workflow for FDP.

The FDP IG Framework sets out minimum IG requirements to be applied in the implementation and operation of FDP, with the aim of ensuring a consistent approach and high standard of IG and transparency across the FDP User Organisation community. This framework includes:

1. working within the contractual documentation associated with the FDP Programme. The FDP IG Framework identifies these and sets out how they work together.
2. clearly identifying the various parties involved in delivering the FDP Programme, explaining their data protection roles and setting out their IG responsibilities.
3. laying out the core IG principles of the FDP Programme.
4. identifying the IG documentation that will be required to be put in place and who is responsible for producing and supporting the production of the documentation.
5. setting out the procedure for reporting Security Breaches and Personal Data Breaches relating to data processed in the FDP.
6. setting out how requests under the Freedom of Information Act 2000 will be handled.
7. setting out the governance arrangements relating to how the parties will work together and the various governance groups to be established to facilitate those arrangements. This includes the Data Governance Group and the NHS FDP System IG Group referred to above. More details about the group can be found within the FDP IG Framework
8. identifying the supporting IG documentation for the FDP Programme and where it can be accessed.
9. explaining how the framework will be reviewed, changed and published to provide transparency over the FDP IG Framework.

4. Identification of risks

NHS England has in this section identified inherent risks of FDP 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 then set out steps taken 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
1	There is a risk that personal data may be misused by those with access
2	There is a risk that data will be processed beyond the appropriate retention period.
3	There is a risk that insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls)
4	There is a risk that insufficient technical measures are in place to ensure appropriate security of the personal data (e.g. encryption, access controls)
5	There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures
6	There is a risk that data that has had identifiers removed could be manipulated in some way to re-identify individual people
7	We could lose public trust if our transparency materials are insufficient. This could then lead to a lack of engagement with the NHS and impair health research and planning via an increase in opt-outs.
8	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.
9	With data being shared across different organisations and systems, there is an increased risk of data leakage, where sensitive information is inadvertently exposed or shared with unauthorised parties.
10	There is a risk that inadequate data quality process result in errors, inconsistencies and missing information that could compromise the integrity and reliability of the data.
11	There is a risk that there are inadequate Business Continuity Plans in place to respond effectively to unexpected disruptions such as cyber attacks or downtime.
12	There is a risk that users will attempt to access the system from outside the UK, increasing the data security risk.

5. Approach to Risk

Documentation:

Where data is processed in FDP, the data will be processed in Products, inside an Instance of the Data Platform. The data protection risks associated with processing data are considered through a suite of risk assessments (DPIAs).

This DPIA is the overarching DPIA for the FDP, including an overview of the generic system functionality required for integrating, managing, and operationalising data, describing the risks and mitigations associated with the Data Platform which are relevant across any FDP Instances. This approach should mean that common elements do not have to be described in the Ontology DPIA and separate Product DPIAs to be carried out.

The FDP uses a data model, referred to as an Ontology. This model defines the tables, schemas and definitions of various NHS concepts such as "patient" and "encounter". When the model is deployed in an Instance, an Ontology DPIA or Product DPIA will assess the particular data processing to populate the model, as further described in section 6.

Each FDP User Organisation should also consider risks through the use of Products. Product DPIAs assess the risk in relation to specific processing activities. Each Product will have its own DPIA, and when a Product is deployed to an Instance the FDP User Organisation should consider the associated risks as they relate to their use of the Product in their own Instance.

DPIAs will evolve over time to reflect the enhancements and development in core functionality, development of Products and additional FDP User Organisations. They are not static. This DPIA will therefore also evolve over time.

6. Description of the Processing

The processing of data within FDP will be described in seven broad categories:

- Data Ingress (data arriving into the FDP)
- Data Transfer (data flowing between FDP Instances)
- Data Egress (data leaving the FDP)
- Data Platform Services (tools provided to enable data processing within the FDP)
- Data linkage and analysis (data used within the FDP)
- Auditing
- Detailed Processing

Data Ingress (data landing into the FDP)

Personal Data (including Confidential Patient Information) can arrive in FDP Instances via direct connection to source systems via REST APIs, HL7 streams, ODBC/JDBC connections, S3/ABFS sources, connections made to data warehouses, Secure FTP (SFTP) or MESH. FDP User Organisations as Controllers approve data ingress to FDP further to the FDP IG Framework All Instances are hosted within cloud infrastructure. This aligns to the 'cloud first' policy for public sector IT introduced in 2013, endorsed by the National Information Board's Personalised Health and Care 2020 framework.

All Personal Data brought into the FDP will be registered through NHS-PET (there is a separate DPIA assessing risks in relation to NHS-PET). This registration process is documented elsewhere, but in summary the purpose is to provide transparency of what data is held within FDP. In future (but not in the initial deployment of FDP and NHS-PET), the NHS-PET will also “treat” data, de-identifying it as required (this DPIA will be updated before this occurs).

Any data landing in the FDP is limited to a specific Instance until such time as it is transferred to another Instance (which in all cases is only with the approval of the relevant Controller). Subject to the limitations of data use in the FDP (set out in the FDP IG Framework). FDP User Organisations are responsible for the data entering and leaving their Instance.

Data Transfer (data flowing between FDP Instances)

Data, including Personal Data (including Confidential Patient Information) can transfer between FDP Instances without leaving the secure platform boundaries when authorised by the FDP User Organisation (a copy of the data is created, this is not multi-user access to a single copy of data).

Authorisation by the FDP User Organisation is also subject to the appropriate governance arrangements being put in place for the transfer of any Personal Data (including Confidential Patient Information), which includes data sharing agreements required under the FDP IG Framework and any transfer being lawful under UK GDPR and the Common Law Duty of Confidentiality. Any transfer is subject to registration through NHS-PET, for transparency.

Data Egress (data leaving the FDP)

Personal Data (including Confidential Patient Information) may leave an FDP Instance via the same protocols and mechanism as ingress, subject to the FDP User Organisation's authorisation. In addition, industry standard APIs exist in FDP Instances to allow for egress of data by external systems when authorised. When authorised, external analytics tools used by FDP User Organisations or with their permission can integrate with data in FDP, such as Tableau, Power BI, Excel and more. Any such use of data held within FDP but accessed from outside the Data Platform must occur only where that processing is described by a Product DPIA.

As described above, authorisation by the FDP User Organisation is also subject to the appropriate governance arrangements being put in place for the transfer of any Personal Data (including Confidential Patient Information), which includes data sharing agreements required under the FDP IG Framework and any transfer being lawful under UK GDPR and the Common Law Duty of Confidentiality.

Data Platform Services (tools provided to enable data processing within the FDP)

The FDP provides tools to enable FDP User Organisations to have access to their own individual Instance, and specific canonical data model (“CDM”), through the use of the Data Platform Services (which include pipeline management; modelling and branching; and data and code versioning) to customise the data model via extensions appropriate to their deployment profile to enable the integration, management and operationalising of data.

A canonical model is a design pattern used to communicate between different data formats. Essentially: create a data model which is a superset of all the others (“canonical”),

and create a "translator" module or layer to/from which all existing modules exchange data with other modules.

The FDP Instance has a CDM, also referred to as the shared healthcare ontology, this model defines the tables, schemas and definitions of a various NHS concepts such as patient and encounter. When the model is deployed in the National Instance, an Ontology DPIA which will be published, will assess the particular data processing to populate the model. Local Product DPIAs will describe the processing to populate local Ontologies.

When the Instance is configured, FDP User Organisations can leverage the Data Platform Services together with object layer services (including ontology manager, object monitoring, scenarios, actions and functions) to integrate data from third-party sources to a CDM which enables the systematic mapping of data to intuitive, operational NHS or FDP User Organisation specific concepts.

Additionally, different types of data may be visible to individual users of the FDP, who may view that data, subject to Role Based Access Controls and Purpose Based Access Controls put in place by the FDP User Organisation, for a specific purpose under one of the five use cases as detailed within a Product DPIA.

In line with the strict access controls in place, the information being displayed may be Personal Data which is Directly Identifiable Data, Pseudonymised Data, Anonymised Data, Aggregated Data or Operational Data.

Data linkage and analysis (data used within the FDP)

Directly Identifiable Personal Data may be linked with other Directly Identifiable Personal Data through the use of patient identifiers such as the NHS number, date of birth and postcode.

Pseudonymised Data may be linked based on common pseudonyms, i.e. the direct identifiers have been replaced in a consistent manner across datasets, to allow linkage.

Specific analysis (including ad hoc analysis and reporting) will be detailed within Product DPIAs, and must adhere to data protection principles, including using the minimum data necessary.

Auditing

Use of all FDP Instances will be audited, and logs will be held within the system. The logs will enable troubleshooting activities and may be used to detect unusual activity within the system, or in the event of a suspected cyber incident or unlawful activity.

Audit logs containing details about user activities and data in the platform can be shared with the NHS Cyber Security Operations Centre (CSOC) operated by NHS England to enable monitoring and responses to unusual activity in the platform.

Users have access to their respective audit logs to enable monitoring of activities.

Detailed Processing

The Canonical Data Model (CDM) is deployed to each FDP Instance. As this is purely a model, there is no data at this point.

Products are developed using this model (to ensure consistency and 'deployability' between products). Where a Product requires data, the data must be present in the Ontology. These Products provide a wide range of capabilities ranging from dashboards

and command centres for staff, alerting, data analysis tools, operational scheduling and data cleaning tools.

Any data ingested into FDP can be fully traced back from the Product and Canonical Data Model back to the original ingestion via the data lineage tool. Purpose Based Access Control enforces that data ingested for a particular purpose, such as Direct Care, is only used for this approved purpose.

7. Compliance with the Data Protection Principles

Compliance with the Data Protection Principles, 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
1. Lawfulness, fairness and transparency	Section 9 (Lawfulness); Section 10 (Fairness); Section 11 (Transparency)
2. Purpose limitation	Section 4
3. Data minimisation	Section 12
4. Accuracy	Section 16
5. Storage limitation	Section 15
6. Integrity and confidentiality (security)	Section 18
7. Accountability	Accountability is addressed throughout the DPIA. In particular, section 23 includes approval of the residual risks by the Information Asset Owner.

8. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?

The FDP is designed to be a common system that can be used by many different organisations, with each of those organisations retaining autonomy over the use of any data they choose to put there. Each organisation has a separate space (called an “Instance”), where their data is held securely, and separate from data belonging to other organisations. The separate organisations are referred to as “FDP User Organisations”.

Data Controllership in relation to Local and National Instances

- NHS England is the sole Controller of the Personal Data which flows into and is Processed within any approved Products it chooses to use in the National Instance of FDP.
- Local FDP User Organisations are the sole Controllers of the Personal Data which flows into and is Processed within any approved Products they chose to use in their own Local Instance of the FDP, subject to what is said below regarding joint controllership.

- NHS England and each Local FDP User Organisation are Joint Controllers for design, governance, and service management of the Local FDP User Organisation's Local Instances of FDP. This is because:
 - NHS England has procured, funds, broadly determines the parameters for use, and manages the security, of the Data Platform.
 - Local FDP User Organisations decide whether to use FDP, what Products to use, what data to commit to FDP and how to use it within these parameters.

NHS England and each Local FDP User Organisation are therefore Controllers for different aspects of how FDP operates at a national and local level, including in relation to their own FDP Instances.

Controllorship responsibilities between NHS England and FDP User Organisations are set out clearly in a Joint Controller table (at the end of this DPIA, and in the FDP IG Framework) and are agreed between NHS England and each Local FDP User Organisation further to the terms of the MoU through the contractual documentation they enter into. The essence of this arrangement will also be made publicly available in privacy material relating to the FDP so that this is readily and easily apparent to the public in line with Article 26 of UK GDPR.

The following explains firstly NHS England's legal basis to procure and provide the FDP system, and then explains the likely legal basis for the processing of Personal Data within an Instance. In each case this will be specifically documented in the separate Product DPIAs and reflect the Processing of Personal Data within a Product.

NHS England's legal basis to procure and provide the FDP

1. Statutory Authority

NHS England has various statutory functions that enable it to procure and provide FDP for itself and for other FDP User Organisations. These include:

- Section 270 of the Health and Social Care Act 2012 (**2012 Act**), to establish and provide FDP for 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 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

1.2 Legal Basis – NHS England

In relation to the procurement and provision of FDP for itself and for 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.

Legal Basis for Processing Personal Data in each Instance of FDP

Where NHS England or an FDP User Organisation is Processing Personal Data and Special Categories of Personal Data, they will each separately as Controllers identify:

- a relevant condition for Processing under Articles 6 and 9 of UK GDPR and Schedule 1 of the DPA, and
- in relation to Confidential Patient Data, a legal basis under the Common Law Duty of Confidentiality.

This will be determined at a Product level for the Personal Data being processed through FDP and reflected in the relevant national or local Product DPIA and Product Privacy Notice. The likely legal basis are set out below:

1.3 Legal Basis – FDP User Organisation

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

- Article 6(1)(c) Legal Obligation, for example where NHS England collects and analyses data under a Direction.
- Article 6(1)(e) Public Task, for example where an FDP User Organisations Processes Personal Data for the purposes of providing an individual with care and treatment. Also where NHS England shares data with NHS Trusts or ICBs through the Platform 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 FDP would include:

- Article 9(2)(g) Public Interest,
- 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 would include:

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

1.4 Common Law Duty of Confidentiality

Under the Common Law Duty of Confidentiality where confidential data, including Confidential Patient Information (Confidential Patient Data) is Processed within FDP, it is expected it would be lawful because of:

- implied consent where the Processing of Confidential Patient Data in any particular circumstances is carried out for the purpose of the Direct Care of a patient.
- legal obligation, including:
 - o 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 Health and Social Care (Direction) that may be processed in the national Instances for purposes covered by a Direction.
 - o 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 to a national Instance.
- statutory authority which expressly sets aside the Common Law Duty of Confidentiality including:
 - o Regulation 3 of the National Health Services (Control of Patient Information) Regulations 2002 (“COPI Regulations”)
 - o 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.

It is not expected that any Processing of Confidential Data within the FDP would rely on a public interest justification.

9. Demonstrate the fairness of the processing

Each FDP User Organisation is responsible for ensuring that the patient information in their FDP Instance is used fairly and transparently. Because the specific uses of the data are determined by the FDP User Organisation, it is not possible for this DPIA to demonstrate the fairness of each specific use/ Product, this will be detailed within the specific Product DPIA's

The high-level uses of the FDP (repeated below) have been developed through consultation with stakeholders:

1. Elective recovery (reducing waiting times) – to get patients treated as quickly as possible, reducing the backlog of people waiting for appointments or treatments which has resulted from the COVID-19 pandemic alongside winter pressures on the NHS.

2. Vaccination and immunisation – to ensure that there is fair and equal access, and uptake of vaccinations across different communities.
3. Population health management (Planning NHS services) – to help local NHS organisations to plan the right services, in the right places, for their local communities.
4. Care coordination (Joining up care) – to ensure that health and care organisations all have access to the information they need to support the patient, reducing the number of long stays in hospital and ensuring that everyone is cared for in the right place for them at the right time.
5. Supply chain management (Getting the best value for the NHS) – to help the NHS put resources where they are needed most and buy smarter so that we get the best value for money.

Where Directly Identifiable Personal Data, including Confidential Patient Information is used within the FDP (until such time as new activity is developed, and this DPIA is updated), it is for Direct Care only.

Where possible, Personal Data will be protected through the use of Pseudonymisation.

In all cases, where Personal Data is used within the FDP, it is the responsibility of the FDP User Organisation to ensure that there is sufficient transparency for the public, and that processing is both fair and lawful.

To assist FDP User Organisations with fulfilling their transparency obligations, NHS England publishes some information about the FDP, including information about the Use Cases. Until further Use Cases are developed and approved, processing of Personal Data within the FDP must only be carried out for the purposes of the initial five Use Cases.

Transparency needs to be achieved through a layered approach, describing various topics at a high level (such as FDP, NHS-PET, National and Local Instances, National and Local Products, etc.), alongside a more detailed FDP Privacy Notice, and more specific Product Privacy Notices. NHS England will be publishing this information on its website and Local FDP User Organisations will also need to publish appropriate transparency information on their websites.

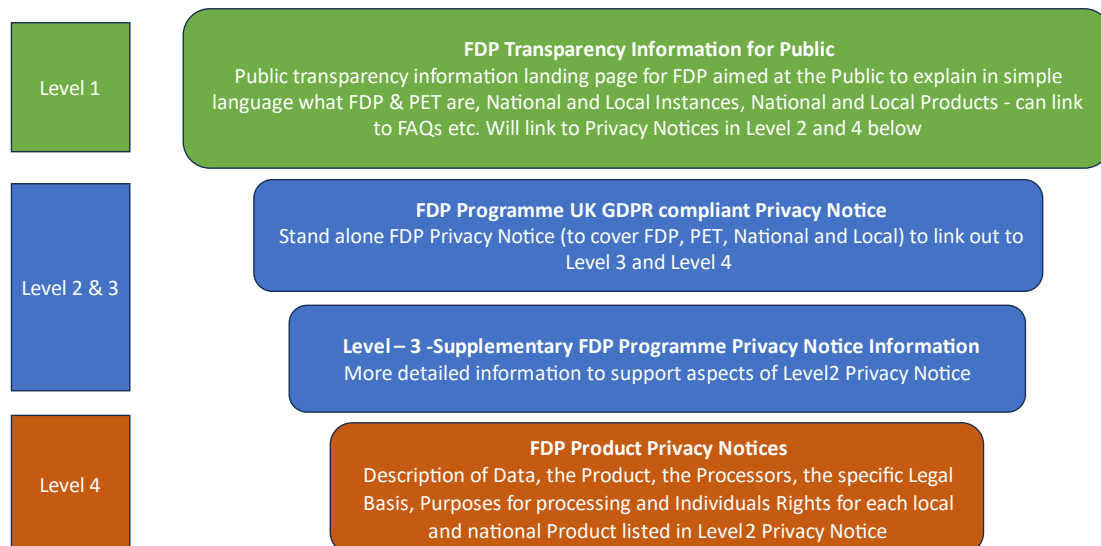
10. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

In establishing the way in which the FDP will be delivered and operate for the NHS, there has been on-going engagement with several stakeholder groups (see “Consultation with Stakeholders” section) to co-design the approach to transparency. This has ensured that FDP has taken a privacy-by-design approach, ensuring that the views of the data subjects have been included in the design of the FDP IG Framework and associated documentation.

NHS England will publish overarching generic information about the use cases, and about the FDP, as mentioned in the previous section. In addition, NHS England is an FDP User Organisation in its own right, and has a responsibility to be transparent about processing within the NHS England Instance of FDP. NHS England is also therefore publishing a General FDP Privacy Notice, and separate Product Privacy Notices for every national and local Product on its website.

NHS England has taken a layered approach to providing the public with transparency information and UK GDPR required privacy notice information. The diagram below describes the approach that has been taken:

FDP Programme – Privacy Notice and Transparency Information Suggested Approach based on User Research



V1.0 19/03/24

Additionally, each Product will be approved by the Data Governance Group (with membership from across FDP User Organisations) and template approved IG documentation will be made available to any FDP User Organisation who wants to use the Product. This Product template documentation will include a DPIA and Level 4 Product Privacy Notice.

Each FDP User Organisation is responsible for its own data protection obligations, and any generic templates (provided to improve consistency, transparency, and understanding) may be altered or the information presented in other formats by an FDP User Organisation.

NHSE FDP Programme will be issuing regular FDP communications to be clear to the public about the approach to the roll out of the FDP Programme, what data is being processed for what purposes as products evolve, how FDP works and how privacy is protected, including how NHS-PET works, particularly when PET starts treating data later in 2024.

11. Is it necessary to collect and process all data items?

Data Categories [Information relating to the individual's]	Yes	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 products, please refer to the product specific DPIA for details

Data Categories [Information relating to the individual's]	Yes	Justify [there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]
Address	Yes	For some products, please refer to the product specific DPIA for details
Postcode	Yes	For some products, please refer to the product specific DPIA for details
DOB	Yes	For some products, please refer to the product specific DPIA for details
Age	Yes	For some products, please refer to the product specific DPIA for details
Sex	Yes	For some products, please refer to the product specific DPIA for details
Marital Status	Yes	For some products, please refer to the product specific DPIA for details
Gender	Yes	For some products, please refer to the product specific DPIA for details
Living Habits	Yes	For some products, please refer to the product specific DPIA for details
Professional Training / Awards / Education	Yes	For some products, please refer to the product specific DPIA for details
Income / Financial / Tax situation / Financial affairs	No	
Email Address	Yes	For some products, please refer to the product specific DPIA for details
Physical Description	Yes	For some products, please refer to the product specific DPIA for details
General Identifier e.g. NHS No	Yes	For some products, please refer to the product specific DPIA for details
Home Phone Number	Yes	For some products, please refer to the product specific DPIA for details
Online Identifier e.g. IP Address/Event Logs	Yes	This may be processed in relation to FDP User staff accessing FDP and is required for help desk functionality and audit
Website Cookies	No	
Mobile Phone / Device No / IMEI No	No	
Location Data (Travel / GPS / GSM Data)	No	
Device MAC Address (Wireless Network Interface)	Yes	This may be processed in relation to FDP User staff accessing FDP and is required for help desk functionality and audit
Banking information e.g. account number, sort code, card information	No	
Criminal convictions / alleged offences / outcomes / proceedings / sentences	No	

Data Categories [Information relating to the individual's]	Yes	Justify [there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]
Spare – add data item (as necessary)		
Spare – add data item (as necessary)		
Special Category Data		
Physical / Mental Health or Condition	Yes	For some products, please refer to the product specific DPIA for details
Sexual Life / Orientation	Yes	For some products, please refer to the product specific DPIA for details
Religion or Other Beliefs	Yes	For some products, please refer to the product specific DPIA for details
Trade Union membership	No	
Racial / Ethnic Origin	Yes	For some products, please refer to the product specific DPIA for details
Biometric Data (Fingerprints / Facial Recognition)	No	
Genetic Data	Yes	For some products, please refer to the product specific DPIA for details

12. Describe if personal datasets are to be matched, combined or linked with other datasets? (internally or for external customers)

Datasets will be matched/combined/linked within FDP. Any such use of data will be described in Product DPIAs.

In general:

- Linkage may occur through data which is not directly Personal Data, but relates to other factors (e.g. linkage of data relating to a common location).
- Directly Identifiable Personal Data may be linked with other Directly Identifiable Personal Data through the use of direct patient identifiers, e.g. NHS Number.
- Pseudonymised Data may be linked based on common pseudonyms, i.e. the direct patient identifiers have been replaced in a consistent manner across datasets, to allow linkage but to protect Personal Data by preventing re-identification of individuals without additional information/resources.
- Specific analysis will be detailed within Product DPIAs, and must adhere to data protection principles, including using the minimum data necessary.

13. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

The FDP functionality allows for data to be transferred between Instances, or to be taken away from the FDP (Egress).

Any such transfer/flow will be subject to the FDP User Organisation's approval, its governance processes, there being a legal basis, audit within FDP, and registration by the NHS-PET.

14. How long will the personal data be retained?

Retention of Personal Data within an Instance is subject to the FDP User Organisation's policies. Each Product may have a unique data retention period, this will be set by the FDP User Organisation and articulated within the Product DPIA.

Each FDP User Organisation must abide by their own Records Management Policies and Retention Schedules, in compliance with the NHS Records Management Code of Practice 2021.

15. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

The FDP will not be directly collecting data from patients.

All FDP User Organisations are responsible for adhering to data protection law requirements such as transparency and maintaining accurate records. There may be additional requirements around clinical record-keeping.

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

Awareness:

All FDP User Organisations must:

- i) have the relevant policies and procedures to ensure that data subjects understand their rights in relation to their data.
- ii) have the policies and procedures in place to be able to answer any subject rights requests.

Process:

All individual rights requests should be considered by the relevant Controller, i.e. NHS England do not have a central co-ordinating role. If a request is received by the FDP Platform Contractor, it will be passed to the relevant FDP User Organisation(s).

FDP User Organisations will follow their own internal processes for determining how to progress with any rights request. If this results in action being required within the FDP, then the FDP User Organisation will inform the FDP Platform Contractor to take the appropriate action (such as provision, amendment or deletion of information).

The general (Level 2) FDP Privacy Notice provides general information about an individual's rights under UK GDPR and the specific (Level 4) Product Privacy Notices identify which rights apply to the data processed in the Product.

17. What technical and organisational controls for “information security” have been put in place?

Encryption and security:

All data stored in the FDP will be protected via industry good practice layers of protection including encryption at rest and transit, regular penetration testing, firewall, anti-virus and intrusion protection.

The central data platforms are penetration tested to provide assurance and confirmation that all data is secure in accordance with an agreed schedule.

Both the FDP Platform Contractor and the national Cyber Security team will monitor technical systems for signs of suspicious activity.

All access to the FDP must be authenticated using Multi-Factor Authentication (MFA). Each FDP Instance can integrate with the FDP User Organisation's chosen Single Sign-On (SSO) provider, commonly NHSmail. MFA must be enforced by the SSO provider via either smartcard, application based, hardware token, or phone based.

FDP utilises Role Based Access Controls and Purpose-Based Access Control to ensure all access to data for users is approved and with justification. Access of individual users and groups of users can be audited at any time by the FDP User Organisation to view when, why and how access was approved. The FDP User Organisation remains fully in control of data access and must approve any requests for access to data to enable the relevant processing or support.

Purpose-Based Access Control enforces that data ingested for a particular purpose, such as Direct Care, is only used for this approved purpose. Information on what data is being ingested, and the associated purpose, can be viewed in FDP and NHS-PET by the FDP User Organisation.

More detail on Purpose-Based Access Controls is available within Part 2 of Schedule 3 of the FDP IG Framework.

Further detailed system and technical level security policies apply, which are not published.

18. In which country/territory will personal data be stored or processed?

All processing of patient information will be within the UK only. This is a contractual requirement and one of the key principles of the FDP IG Framework. This is enforced through technical controls within FDP

19. Do Opt Outs apply to the processing?

There will be a wide range of Products available for use within the FDP by FDP User Organisations.

National Data Opt Out

The National Data Opt-Out provides an individual with a right to opt out of their Confidential Patient Information being used for purposes beyond their Direct Care, unless an exemption applies under the [National Data Opt-Out Operational Policy Guidance](#).

At the start of the Transition Phase of the FDP Programme there are no existing Products where the National Data Opt Out would be applicable because:

- No Confidential Patient Information is being processed by a Product in the National Instances of FDP to which the National Data Opt-Out would apply.
- Confidential Patient Information that is being used in the FDP in a Product in a Local Instance is only being used for the purposes of Direct Care and therefore the National Data Opt-Out does not apply.

Product DPIAs and (Level 4) Product Privacy Notices will explain why the National Data Opt Out does not apply.

Type 1 Opt Outs

A Type 1 opt-outs registered with a GP Practice prevents an individual's confidential patient information from being shared outside of their GP Practice except when it is being used for the purposes of their individual care.

At the start of the Transition Phase of the FDP Programme there are no existing Products where Type 1 Opt Outs would be applicable because:

- No Confidential Patient Information that has come from a GP Practice is being processed by a Product in the National Instances of FDP.
- Any Confidential Patient Information that has come from a GP Practice which is being used in the FDP in a Product in a Local Instance is only being used for the purposes of individual care.

Product DPIAs and (Level 4) Product Privacy Notices will explain why the Type 1 Opt Out does not apply.

Future changes

If this changes in the future because a new Product processes Confidential Patient Information in a way which would mean that one of the above opt-outs would apply, the relevant FDP User Organisation would be responsible for ensuring that the opt-out was applied, the relevant (Level 4) Product Privacy Notice would identify this and the general

(Level 2) FPD Privacy Notice and general (Level 1) transparency information would be updated to make this clear.

It is a core principle of the FDP IG Framework and also a contractual obligation of the suppliers of both FDP and NHS-PET that National Data Opt-Outs and Type 1 Opt Outs are respected and applied where they should be applied.

20. Risk mitigation and residual risks

The “Identification of Risks” section 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 that have been identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

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

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
1	Personal data may be misused by those with access	<p>1. External suppliers are 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.</p> <p>2. All individual users are required to sign security operating procedures that confirm their responsibilities to protect data. Individual Users are also subject to contractual confidentiality requirements.</p>	<p>1 – section 18</p> <p>2 – section 18</p>	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
		3. The download functionality of data from the FDP is disabled by default, and access to this is controlled by the relevant FDP User Organisation which ensures appropriate governance in place. 4. Purpose based access controls are in place to limit access to data.	3 – section 18 4 – section 7				
2	Personal data 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. 2. Product DPIAs include a section on retention of personal data.	1 – section 18 2 – section 15	Treat	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls)	1. Appropriate organisation 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. Any breaches are reported in line with these.	1 – section 18 2 – section 4	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
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 3. System level security policies in place to record services compliance to security policy requirements 4. Cyber Security Consultancy team assess architecture (including things like threat modelling) to ensure the right technical measures are in place. These include Role Based and Purpose Based Access Controls, effective security monitoring, and encryption in transit and at rest.	1 – section 4 2 – section 4 3 – section 18	Treat	Remote	Significant	Low
5	Insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures	1. An AWS platform configuration review by AWS security team has been performed to ensure that first ingest of data is stored securely. 2. Full penetration testing has already been undertaken. 3. Regular PEN testing to be scheduled	1 – sections 4, and 18 2 – sections 4, and 18 3 – sections 4, and 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
6	Data that has had identifiers removed could be manipulated in some way to re-identify individual people	<p>1. Access to NHS Data at pseudonymised record level remains in control of the NHS controller. Role Based and Purpose Based Access Controls control who has access to data</p> <p>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</p> <p>3. Contracts of employment and other organisational policies provide further safeguards against data misuse</p> <p>4. Product level DPIAs assess the risks of re-identification and identify additional controls that apply at Product level</p>	<p>1 – section 4 & 7</p> <p>2 – section 4</p> <p>3 – section 4</p>	Tolerate	Remote	Significant	Low
7	We could lose public trust if our transparency materials are insufficient. This could then lead	1. Transparency achieved through a layered approach, describing various topics at a high level (such as FDP, NHS-PET, National and Local Instances, National and Local Products, etc.), alongside a more detailed FDP Privacy Notices (which	1 – sections 10, and 11	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
	to a lack of engagement with the NHS and impair health research and planning via an increase in opt-outs.	<p>also takes a layered approach), and more specific Product Privacy Notices. The FDP IG Framework and DPIAs will also be published to support full transparency.</p> <p>2. Continued engagement with stakeholder and patient groups to support transparency by design and by default and to inform FDP Programme communications to the public.</p> <p>3. Regular FDP Programme Communications to be clear to the public about the approach to the roll out of the FDP f, how FDP works and how privacy is protected, including how NHS-PET works. Be clear about what is current processing and Product and what is future aspirational processing and Product which are not yet agreed to ensure that public is clear on current processing</p> <p>4. Transparency over application of opt outs in high level FDP communications, the FDP Privacy</p>	<p>2 – section 2</p> <p>3 – section 11</p> <p>4 – section 20</p>				

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
		Notice, Product Privacy Notices and Product DPIAs.					
8	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.	<p>1. The FDP Contractor is required to have Business Continuity Plans in place to mitigate this risk.</p> <p>2. The relevant FDP User Organisation is required to have Business Continuity Plans in place to mitigate this risk.</p>	Section 4	Tolerate	Remote	Significant	Low
9	With data being shared across different organisations and systems, there is an increased risk of data leakage, where sensitive information is inadvertently exposed or shared with	<p>Mitigations are in place for organisational measures (risk #3) and technical measures (risk #4). In addition:</p> <p>1. The FDP IG Framework requires that without the appropriate Data Sharing arrangements in place, data cannot be moved between Instances.</p>	Sections 4 and 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
	unauthorised parties.						
10	There is a risk that inadequate data quality process result in errors, inconsistencies and missing information that could compromise the integrity and reliability of the data.	<p>1. The FDP User Organisation is responsible for the quality of the data being provided to the Data Platform. Where this is Personal Data, there are data protection obligations and DSPT obligations.</p> <p>2. Product DPIAs should consider this risk for individual Products depending on the data sources</p>	Sections 4 and 18	Tolerate	Remote	Significant	Low
11	There is a risk that there are inadequate Business Continuity Plans in place to respond effectively to	<p>1. Under the terms of the contract, the FDP Contractor is obliged to have and maintain Business Continuity Plans.</p> <p>2. FDP User Organisations, as NHS bodies, are obliged to have and maintain Business Continuity Plans. Product DPIAs should consider this</p>	Section 4	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
	unexpected disruptions such as cyber attacks or downtime.	risk for individual Products depending on their criticality.					
12	There is a risk that users will attempt to access the system from outside the UK, increasing the data security risk.	<p>1. It is clearly articulated within the FDP IG Framework that no personal/patient data should leave the UK without the express prior approval from the Data Governance Group.</p> <p>2. It is set out in the contract that no access to Personal Data should take place from outside the UK. There are technical controls in place to this effect to prevent access from IP addresses outside of the UK.</p>	Sections 4, 18, and 19	Treat	Remote	Significant	Low
13.	There is a risk that FDP communications to date may not have fully explained the use of the FDP	1. Updated communications for the NHSE website have been produced to be clearer about national Instance use, with comms plans to provide more information about FDP and how it is used in the local and	<p>1 – Section 11</p> <p>2 – Section 11</p>	Tolerate	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
	by NHSE in the national Instance and that individuals were not previously aware of how NHSE and Trusts were processing data in the previous National Data Platform for Products that are now migrating to FDP	<ol style="list-style-type: none"> national Instances during the Transition Phase The Level 2 FDP Privacy Notice and Level 4 Product Privacy Notices provide full transparency over Processing in Products and will be made available on NHSE website, Local FDP User Organisations have obligations to be transparent and adopt/amend and use these Notices for their local Products Publication in due course of this Overarching DPIA and Product DPIAs will provide more transparency 					

21. Actions

NHS England through FDP Programme governance and management arrangements regularly reviews this DPIA and identifies and manages to completion actions to ensure it is accurate and updated.

22. Definitions

Definitions which may be useful in the review of this document:

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 the FDP IG Framework (Part 1 of Schedule 2 (Approved Use Cases and Products)), or any subsequent broad purpose agreed to be a use case through the Data Governance Group
Commissioned Health Service Organisations	Means organisations who provide health services in England pursuant to arrangements made with an NHS Body exercising functions in connection with the provision of such services.
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.
Confidential Patient Information	Has the meaning given in section 251(11) of the National Health Service 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 FDP and NHS-PET which will include membership from across FDP User Organisations
Data Platform	The NHS Federated Data Platform
Data Security and Protection Toolkit (DSPT)	The Data Security and Protection Toolkit is an online self-assessment tool that FDP User Organisations are required to complete annually to demonstrate they are meeting required data protection and security standards
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.
Directly Identifiable Personal Data	Personal Data that can directly identify an individual.
DPIA	Data Protection Impact Assessments in a form that meets the requirements of UK GDPR
FDP	Federated Data Platform
FDP IG Framework	The FDP IG Framework attached at section 24 (as the same may be updated from time to time) has been created to enable the management of the information governance (IG) workflow for FDP.
FDP Programme	The NHS England Programme responsible for the procurement and implementation of the FDP across the NHS
External IG Advisory Group	The advisory group established by NHS England to provide specialist IG advice to the FDP Programme which includes membership from external organisations including the Office of the National Data Guardian and the Information Commissioner's Office
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 FDP
General FDP Privacy Notice	A privacy notice providing information on the Personal Data Processed in the FDP 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
Instance	A separate instance or instances of the FDP deployed into the technology infrastructure of an individual FDP User Organisation
Joint Controller	Has the meaning given in UK GDPR, being where two or more Controllers jointly determine the purposes and means of Processing Personal Data
Joint Controller Arrangement	Has the meaning given in UK GDPR being an arrangement between two or more Joint Controllers who shall in a transparent manner determine their respective responsibilities for compliance with the obligations under UK GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of UK GDPR and reflecting the roles and relationships of the Joint Controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
Local FDP User Organisation	Any organisation which holds an instance of FDP other than NHS England
MoU	The Memorandum of Understanding signed between NHS England and an NHS Trust, ICB or other NHS Body as may be amended from time to time in accordance with its terms
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 ² and Operational Policy Guidance for more information ³
NHS Body	Has the meaning given in the National Health Service Act 2006, which includes ICBs, NHS Trusts, NHS Foundation Trusts and other bodies concerned with NHS service delivery
NHS FDP System IG Group	The user group established by NHS England for local IG leads to discuss and agree IG documentation for the initial and the subsequent deployment of other local Products
NHS-PET	The privacy enhancing technology (PET) solution which records data flows into the FDP and, where required, treats data flows to pseudonymise or anonymise them
NHS-PET Contractor	IQVIA Limited

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 creates a real-life representation of data, linking activity to places and to people.
Operational Data	Items of data that are not about individuals.
Parties	NHS England, the Platform Contractor, the NHS-PET Contractor and FDP User Organisations
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 the 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 FDP 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 FDP. A list of approved Products is maintained in the IG Framework.(set out in the Appendix at section 24).
Product Privacy Notice	A privacy notice providing information on the Personal Data Processed in the FDP 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
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 the IG Framework
Role Based Access Controls	Means user access controls 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 the IG Framework
Security Breach	Is a breach of security, and includes in the case of the Platform Contractor, a Breach of Security as defined in Schedule 2.4 (Security Management) of the Platform Contract
Special Category Personal Data	Refers to 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.
UK GDPR	is as defined and referred to in the Data Protection Act 2018

23. Joint Controller table

NHS England and Local FDP User Organisation Joint Controller Table – V1.0 13 March 2024

1. Introduction

The purpose of this Table is to set out the Joint Controller Arrangement between NHS England and each Local FDP User Organisation (each **a Party** in this Schedule) regarding the Personal Data Processed in the Data Platform and NHS-PET in order to clarify roles and responsibilities for the purposes of Article 26 of the UK GDPR.

Article 26 of the UK GDPR governs the relationship between joint controllers. Article 26(1) of the UK GDPR provides that “*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*”

Under Article 26(2) of the UK GDPR, “*The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.*”

2. Transparent Manner

The Table below can be referred to in relevant Data Protection Impact Assessments (DPIAs). It will also stand as a stand-alone document which can be issued to anyone who requests it. It transparently sets out each Party’s respective obligations and responsibilities as joint Controllers in relation to the Data Platform and NHS-PET.

3. Respective Responsibilities for Compliance, in particular with regard to exercise of data subject rights and duties to provide information in Articles 13 and 14

The Table below sets out each Controller’s responsibilities for:

- compliance with the obligations under UK GDPR which apply to Controllers,
- compliance with duties to provide the information referred to in Article 13 and Article 14, and
- compliance with the obligations under UK GDPR as regards the exercise of data subjects’ rights.

This Table constitutes the arrangement referred to in Article 26.

4. The arrangement may designate a contact point for data subjects

NHS England is designated as a contact point, for data subjects,

- in the Table below for FDP Programme-wide queries and queries concerning the national Instance; and
- in the General FDP Privacy Notice and in the transparency information, for queries concerning each Product in the national Instance.

NHS England's Data Protection Officer is also named in the General FDP Privacy Notice and the transparency information for each Product in the national Instance of FDP as a contact point.

Local FDP User Organisations are designated as a contact point, for data subjects,

- in the Table below for queries concerning their use of the local Instances; and
- in the General FDP Privacy Notice for each Product in their local Instance;
- in the transparency information they provide for each Product in the local Instance which they deploy.

The Local FDP User Organisation's Data Protection Officer should also be named in such transparency information of the Local FDP User Organisation.

5. The arrangement must reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects

In accordance with Article 26 of the of the UK GDPR this Table sets out the roles and responsibilities of the following Parties:

- NHS England (**NHSE**)
- Local FDP User Organisations

(together referred to as the FDP User Organisations), in relation to the Processing of Personal Data in the Data Platform and, when Processing of Personal Data commences, in the NHS-PET.

The FDP is a series of individual platforms referred to as Instances and each of NHS England and the Local FDP User Organisations have their own Instance and they each control the Personal Data held and Processed within their own Instances.

NHS England is the Controller for the Personal Data which flows into, and is processed within, any approved Products it chooses to use within the national Instance.

NHS England is a joint Controller with each Local FDP User Organisation in relation to the local Instances for design, governance, and service management of the Data Platform. This is because NHS England broadly determines the parameters for the use of the Data Platform.

Local FDP User Organisations are Controllers for the Personal Data they flow into and Process in their local Instances. Each Local FDP User Organisation decides whether to use the Data Platform, what data to commit to the Data Platform and how to use it within those parameters.

Where the NHS–PET Contractor Processes Personal Data prior to it entering or leaving the national Instance then NHS England is the Controller of such Personal Data Processing.

Where the NHS-PET Contractor Processes Personal Data prior to it entering or leaving the local Instance then the Local FDP User Organisation is the Controller of such Personal Data Processing.



NHS England are a joint Controller with each Local FDP User Organisation in relation to the Local FDP User Organisation's engagement of the NHS-PET Contractor to Process Personal Data prior to it entering or leaving a local Instance, specifically in relation to the design, governance, and service management of NHS-PET.

6. The essence of the arrangement shall be made available to the data subject

The essence of this arrangement is described in the General FDP Privacy Notice referred to above. This document is publicly available and can also be provided to data subjects on request to NHS England.

Key to Roles and Responsibilities in the Table below

To assist, where a Party:

- has compliance responsibilities this has been identified with a 
- does not have compliance responsibilities, this has been identified with a 

UK GDPR Requirement	NHS England	Local FDP User Organisation
The Controllers	<p>NHS England 7 Wellington Place Whitehall Road Leeds LS14AP ICO Registration No: Z2950066</p> <p>1. The legal basis for NHS England's role as a joint controller in relation to the Local FDP User Organisation's local Instances of the Data Platform and NHS-PET, for the design, governance, and service management of the Data Platform and NHS-PET is based on its statutory functions including:</p> <ul style="list-style-type: none"> (a) the provision of FDP arrangements as a service pursuant to Section 270 of the Health and Social Care Act 2012 (the 2012 Act); (b) the duty as to effectiveness and efficiency under Section 13D of the National Health Service Act 2006 and the duty to promote innovation under Section 13K of the National Health Service Act 2006 (the 2006 Act); (c) The duty to promote a comprehensive health service under Section 1(1) applicable to NHS England by virtue of Section 1H(2) of the 2006 Act; (d) The duty to have regard to the need to respect and promote the privacy of recipients of the health services 	<p>[Add name]</p> <p>Add address</p> <p>ICO Registration No:]</p> <p>The legal basis for the Local FDP User Organisation to be a Controller of the Processing in their local Instance and for the NHS-PET Contractor Processing of Personal Data prior to it entering or on leaving their local Instance shall be determined at a Product level and reflected in the local Product DPIA and in the transparency information for the local Product. This will be dependent on the statutory functions of the Local FDP User Organisation.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>and of adult social care in England under S253(1) ca of the 2012 Act;</p> <p>(e) The powers under Section 2(2) of the 2006 Act to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of its functions.</p> <p>2. The Legal basis under UK GDPR is therefore Art 6(1)l (Public Task) and additionally, for special category data is Art 9(2)(g) (Public Interest) together with paragraph 6 condition (Statutory Purpose) in Part 2 of Schedule 1 of the Data Protection Act 2018.</p> <p>3. In addition to the legal basis for NHS England's role in determining the design, governance and service management arrangements for the Data Platform and NHS-PET, the legal basis for NHS England's role as Controller of the Processing within the national Instance and for the NHS-PET Contractor Processing of Personal Data prior to it entering or on leaving the national Instance shall be determined at a Product level and reflected in the national Product DPIA and in the transparency information for the national Product.</p>	
Data Protection Officers (DPO)	<div data-bbox="327 1187 479 1228" style="background-color: black; width: 68px; height: 26px; margin-bottom: 10px;"></div> <p>Email: england.dpo@nhs.net</p> <p>Address: Data Protection Officer, NHS England, 7 Wellington Place, Whitehall Road, Leeds LS1 4AP</p>	<p><i>[Add name of the Local FDP User DPO]</i></p> <p>Email: []</p> <p>Address: []</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
Accountability Requirements		
Accountability	<p>✓</p> <p>NHS England is a Controller responsible for jointly determining with the Local FDP User Organisation the purposes and means of Processing Personal Data in relation to the local Instance and the Local FDP User Organisation Processing of Personal Data in NHS-PET. In particular NHS England broadly provides the parameters for the use of the Data Platform and NHS-PET and sets the design, governance arrangements and service management of the Data Platform and the NHS PET Solution.</p> <p>Additionally, NHS England is a Controller solely responsible for determining the purposes and means of Processing Personal Data in relation to the national Instance and the Processing of Personal Data in the NHS-PET prior to the data being included in or on leaving the national Instance.</p> <p>NHS England is the Controller responsible for determining the purpose and means of Processing of Personal Data in relation to the NHS-PET Contractor</p>	<p>✓</p> <p>The Local FDP User Organisation is a Controller responsible for jointly determining with NHS England the purposes and means of Processing Personal Data in relation to the local Instance and the Local FDP User Organisation Processing of Personal Data through NHS-PET. In particular the Local FDP User Organisation decides whether to use the Data Platform, what data to commit to the Data Platform and how to use it within the parameters set by NHS England.</p> <p>The Local FDP User Organisation is therefore responsible for complying with the following provisions of UK GDPR in relation to the Processing of Personal Data in their local Instance and Processing of Personal Data in the NHS-PET prior to data being added to or on leaving their local Instance:</p> <ul style="list-style-type: none"> • Article 5(2) (Accountability) • Article 24 (Responsibility of the Controller) • Article 25 (Data protection by design and default) • Article 28 (Processors) • Article 30 (Records of Processing activities) • Article 31 (Co-operation with the supervisory authority) • Article 32 (Security of Processing)

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>Processing of Personal Data prior to it entering or on leaving the national Instance.</p> <p>NHS England is therefore responsible for complying with the following provisions of UK GDPR in relation to the joint controllership with the Local FDP User Organisation:</p> <ul style="list-style-type: none"> • Article 5(2) (Accountability) • Article 24 (Responsibility of the Controller) • Article 25 (Data protection by design and default) • Article 28 (Processors) • Article 30 (Records of Processing activities) • Article 31 (Co-operation with the supervisory authority) • Article 32 (Security of Processing) • Article 33 (Personal data breach reporting to the ICO) • Article 34 (Personal data breach notification to data subjects) • Article 35 (Data protection impact assessment) • Article 36 (Prior consultation) • Articles 37-39 (DPO) • Articles 44 – 49 (Transfers of Personal Data to third countries or international organisations) 	<ul style="list-style-type: none"> • Article 33 (Personal data breach reporting to the ICO) • Article 34 (Personal data breach notification to data subjects) • Article 35 (Data protection impact assessment) • Article 36 (Prior consultation) • Articles 37-39 (DPO) • Articles 44 – 49 (Transfers of Personal Data to third countries or international organisations)

UK GDPR Requirement	NHS England	Local FDP User Organisation
Compliance with Data Protection Principles		
Article 5 (1)(a) Lawfulness Personal Data is Processed lawfully in relation to the data subject	<div> <div>✓</div> <p>NHS England is responsible for determining the purposes and means of the design, governance and service management of the Data Platform and the NHS-PET (Joint Controller Purposes).</p> <p>The lawful basis for NHS England to Process Personal Data under Article 6 of the UK GDPR for the Joint Controller Purposes is Article 6(1)(e) (public task).</p> <p>NHS England is responsible for ensuring that it has a legal basis under UK GDPR for any FDP Product it uses within the national Instance.</p> <p>NHS England is also responsible for ensuring that it has a legal basis under the Common Law Duty of Confidentiality for the Processing of confidential patient information:</p> <ul style="list-style-type: none"> • in the NHS-PET prior to it entering or on leaving the national Instance; and • in the national Instance. </div>	<div> <div>✓</div> <p>The Local FDP User Organisation is responsible for determining whether to use the Data Platform, what data to commit to it, and how to use it within the parameters set by NHS England.</p> <p>The lawful basis for the Local FDP User Organisation to Process Personal Data is determined by the Local FDP User Organisation.</p> <p>The Local FDP User Organisation is responsible for ensuring that it has a legal basis under UKGDPR for any FDP Product that it selects for use within their local Instance.</p> <p>The Local FDP User Organisation is responsible for ensuring that it has a legal basis under the Common Law Duty of Confidentiality for the Processing of confidential patient information:</p> <ul style="list-style-type: none"> • in the NHS-PET prior to it entering or on leaving their local Instance; and • in their local Instance. </div>

UK GDPR Requirement	NHS England	Local FDP User Organisation
Article 5(1)(a) Lawfulness – special categories of Personal Data¹ are Processed lawfully in relation to the data subject	<input checked="" type="checkbox"/> The lawful basis for NHS England, within the national Instance or in the NHS-PET prior to transfer to or on leaving of the national Instance, to Process special categories of Personal Data for the Joint Controller Purposes is: Article 9(2)(g) (substantial public interest) of UK GDPR, supplemented by paragraph 6(2)(a) of Part 2, Schedule 1 to the Data Protection Act 2018 NHS England is responsible for ensuring that it has a legal basis under UK GDPR to Process any special categories of Personal Data for any FDP Product it uses within the national Instance.	<input checked="" type="checkbox"/> The lawful basis for the Local FDP User Organisation, within the local Instance or in the NHS-PET prior to transfer to or on leaving the local Instance to Process special categories of Personal Data in is determined by the Local FDP User Organisation.
Article 5(1)(a) and Articles 12–4 -	<input checked="" type="checkbox"/> NHS England is responsible for producing: -	<input checked="" type="checkbox"/> The Local FDP User Organisation must provide transparency materials as required by UK GDPR. In doing so, they may use the General FDP Privacy Notice and template

¹ If there is no SCPD then state N/A

UK GDPR Requirement	NHS England	Local FDP User Organisation
Fairness and transparency - Personal Data is Processed fairly and in a transparent manner in relation to the data subject	<ul style="list-style-type: none"> a. The General FDP Privacy Notice about the Data Platform and NHS-PET; b. Transparency Information required by Article 14 for Processing of Personal Data Processed in the national Instance and by NHS-PET prior to Processing in the national Instance or on leaving the national Instance; c. Template transparency information for each Product in the national and local Instance of FDP; <p>Transparency Information in respect of the Personal Data is published on the NHS England website at: [add link]</p>	<p>transparency materials provided by NHS England together with any additional materials as they consider necessary or appropriate.</p> <p>Transparency Information in respect of the Personal Data is published at: [add link to Local FDP Transparency Information]</p>
Article 5(1)- Purpose limitation Personal Data is collected for specified, explicit and	<p>✓</p> <p>NHS England determines the overall purpose(s) for which the Data Platform and NHS-PET could be used.</p> <p>NHS England is responsible for ensuring that it does not use Products in the national Instance of FDP for</p>	<p>✓</p> <p>The Local FDP User Organisation is responsible for ensuring that it does not use the Products in their local Instance of FDP for any purposes not covered within the Approved Use Cases.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
legitimate purposes and is not further Processed in a manner incompatible with those purposes	<p>any purposes not covered within the Approved Use Cases.</p> <p>NHS England is responsible for determining the initial five overarching Use Cases. NHS England and Local FDP User Organisations may submit subsequent Use Cases for approval to the Data Governance Group for any new Use Case or changes to Use Cases, subject to consultation with relevant Stakeholders.</p>	
Article 5(1)(c) – Data minimisation Personal Data must be adequate, relevant, and limited to what is necessary in relation to the	<input checked="" type="checkbox"/> NHS England is responsible for ensuring that Personal Data it Processes in relation to the national Instance are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for ensuring that Personal Data it Processes in relation to its local Instance are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed.

UK GDPR Requirement	NHS England	Local FDP User Organisation
purposes for which they are Processed		
Article 5(1)) Accuracy Personal Data must be accurate and where necessary kept up to date; reasonable steps must be taken to rectify or erase inaccurate Personal Data without delay	<input checked="" type="checkbox"/> NHS England is responsible for ensuring that Personal Data it Processes in relation to the national Instance are accurate and where necessary kept up to date and for taking reasonable steps to rectify or erase inaccurate Personal Data without delay.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for ensuring that Personal Data it Processes in relation to its local Instance are accurate and where necessary kept up to date and for taking reasonable steps to rectify or erase inaccurate Personal Data without delay.
Article 5(1)(-) - Storage limitation	<input checked="" type="checkbox"/> NHS England is responsible for ensuring that Personal Data it Processes in relation to the national Instance are kept in a form which permits identification for no	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for ensuring that Personal Data it Processes in relation to its local Instance are kept in a form which permits identification for no

UK GDPR Requirement	NHS England	Local FDP User Organisation
Personal Data must be kept in form which permits identification for no longer than necessary for the purpose for which the Personal Data are Processed	longer than necessary for the purpose for which the Personal Data are Processed.	longer than necessary for the purpose for which the Personal Data are Processed.
Article 5(1)(-) - (Integrity and confidentiality - Personal Data must be Processed in a manner that ensures appropriate	<div data-bbox="322 943 398 997">✓</div> <p>NHS England is responsible for ensuring that Personal Data it Processes in relation to the national Instance is Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage.</p> <p>NHS England is responsible for the security arrangements in place across the FDP and NHS-PET, the contractual arrangements, underpinning such</p>	<div data-bbox="1218 943 1294 997">✓</div> <p>The Local FDP User Organisation is responsible for ensuring that Personal Data it Processes in relation to its local Instance is Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage.</p> <p>The Local FDP User Organisation must report any Incident to NHS England's National Service Desk.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
security including protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage	<p>security arrangements and the oversight of data security arrangements.</p> <p>NHS England must report any Incident to NHS England's National Service Desk.</p> <p>NHS England must demonstrate compliance to the Data Security and Protection Toolkit (DSPT) to standards met.</p> <p>NHS England is responsible for ensuring appropriate technical and organizational measures are in place for the security of Personal Data in transit to and from the NHS-PET and to and from the Data Platform in relation to the national Instance.</p>	<p>The Local FDP User Organisation must demonstrate compliance to the Data Security and Protection Toolkit (DSPT) to standards met.</p> <p>The Local FDP User Organisation is responsible for ensuring appropriate technical and organizational measures are in place for the security of Personal Data in transit to and from the NHS-PET and to and from the Data Platform in relation to its local Instance.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
Data Subjects' Rights and Contact Details		
Article 12 – Transparent information, communication, and modalities for the exercise of the rights of the data subject	<p>✓ NHS England is responsible for compliance with the obligations in Article 12 in relation to the Processing of Personal Data in the national Instance and for the Processing of data by the NHS-PET prior to being Processed in or on leaving from the national Instance.</p> <p>NHS England is responsible for addressing complaints and the exercise of individual data subject rights for Processing of Personal Data in the NHS-PET prior to it being Processed in or leaving from the national Instance and in the national Instance.</p> <p>NHS England is responsible for responding to complaints or enquiries from individuals about Processing of Personal Data in the Data Platform and the NHS-PET except for such complaints and enquiries</p>	<p>✓ The Local FDP User Organisation is responsible for compliance with the obligations in Article 12 in relation to the Processing of Personal Data in its local Instance and for the Processing of data by the NHS-PET prior to being Processed in or on leaving from its local Instance.</p> <p>The Local FDP User Organisation is responsible for addressing complaints and the exercise of individual data subject rights for Processing of Personal Data in the NHS-PET prior to it being Processed in or leaving from its local Instance and in the local Instance.</p> <p>The Local FDP User Organisation is responsible for responding to complaints or enquiries from individuals about Processing of Personal Data in the Data Platform and the NHS-PET where such complaints and enquiries relate to</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>that relate to Processing of Personal Data of an individual in a particular local Instance of FDP.</p> <p>Through its Transparency Information, NHS England is responsible for setting out what rights under UK GDPR are available in relation to its Processing of the Personal Data in the national Instance and in the NHS-PET prior to or on leaving the national Instance and how data subjects may exercise those rights. [insert link]</p>	<p>Processing of Personal Data of an individual in its local Instance of FDP.</p> <p>Through its Transparency Information, the Local FDP User Organisation is responsible for setting out what rights under UK GDPR are available in relation to its Processing of the Personal Data in its local Instance and in the NHS-PET prior to or on leaving its local Instance and how data subjects may exercise those rights. [insert link]</p>
Article 13 – Information to be provided where Personal Data are collected from the data subject	<p>X</p> <p>Not applicable as NHS England will not collect Personal Data directly from data subjects in connection with the Data Platform or NHS-PET.</p>	<p>✓</p> <p>The Local FDP User Organisation is responsible for providing information about Processing of its Personal Data that may take place within the NHS-PET or their local Instance when the Personal Data is collected from data subjects, in accordance with Article 13.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
Article 14 – Information to be provided where Personal Data have not been obtained from the data subject	<input checked="" type="checkbox"/> NHS England is responsible for providing data subjects with the information required in Article 14 in relation to its Processing of Personal Data in the national Instance and Processing in the NHS-PET prior to Processing in or on leaving the national Instance.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for providing data subjects with the information required in Article 14 in relation to its Processing of Personal Data in its local Instance and Processing in the NHS-PET prior to Processing in or on leaving its local Instance.
Article –5 - Data subject access request	<input checked="" type="checkbox"/> NHS England is responsible for complying with data subject access requests regarding its Processing of Personal Data in relation to the national Instance and Processing in the NHS-PET prior to or on leaving the national Instance.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for complying with data subject access requests regarding its Processing of Personal Data in relation to its local Instance and Processing in the NHS-PET prior to or on leaving its local Instance.
Articles 16 – – 2 - Other applicable data subject rights	<input checked="" type="checkbox"/> NHS England is responsible for complying with the exercise of any other data subject rights regarding its Processing of Personal Data in relation to the national Instance and Processing in the NHS PET prior to or leaving the national Instance.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for complying with the exercise of any other data subject rights regarding its Processing of Personal Data in relation to its local Instance and Processing in the NHS PET prior to or on leaving its local Instance.

UK GDPR Requirement	NHS England	Local FDP User Organisation
Complaints	<input checked="" type="checkbox"/> NHS England is responsible for investigating any complaints regarding its Processing of Personal Data in relation to the national Instance and Processing in the NHS PET prior to or on leaving the national Instance.	<input checked="" type="checkbox"/> The Local FDP User Organisation is responsible for investigating any complaints regarding its Processing of Personal Data in relation to the local Instance and Processing in the NHS PET prior to or on leaving its local Instance
Contact Point for Data Subjects	<input checked="" type="checkbox"/> NHS England is a contact point for Data Subjects referred to in its Transparency Information regarding its Processing of Personal Data in relation to the national Instance or Processing in the NHS-PET prior to or on leaving the national Instance. NHS England is a contact point for Data Subjects with queries about the Data Platform and NHS-PET that are not concerned with Processing in a particular Instance.	<input checked="" type="checkbox"/> The Local FDP User Organisation is a contact point for Data Subjects referred to in its Transparency Information regarding its Processing of Personal Data in relation to their local Instance or Processing in the NHS-PET prior to or on leaving its local Instance.
Article 28 Processors	NHS England is responsible for engaging the FDP Contractors on Article 28 UK GDPR-compliant terms which govern the design, governance and service management elements of the Products which may be made available to Local FDP User Organisations.	The Local FDP User Organisation is responsible for engaging the FDP Contractors on Article 28 UK GDPR-complaint terms which specifically reflect the manner in which the Local FDP User Organisation intends to instruct the FDP Contractors, by particular reference to the Use Cases, Approved Products

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>NHS England is also responsible for engaging the FDP Contractors on Article 28 UK GDPR compliant terms which specifically reflect the manner in which it intends to instruct the FDP Contractors by particular reference to the Use Cases, Approved Products and Personal Data to be Processed on behalf of NHS England in relation to the national Instance.</p>	<p>and Personal Data to be Processed on behalf of the relevant Local FDP User Organisation in relation to the local Instance.</p>
Personal Data Breach and notifications		
Articles 33 and 34 – Notification of Personal Data breach to supervisory authority / data subject	<p>✓ NHS England is responsible for putting in place appropriate policies for detecting, preventing, and reporting actual and potential Personal Data Breaches where those breaches result in (or could result in) a risk to the rights and freedoms of natural persons in relation to the NHS-PET and the Data Platform.</p> <p>NHS England has internal operational Processes in place for dealing with Personal Data Breaches, with support from its internal Data Protection Office Team and Cyber Security Operations Centre, which will be invoked in the event of a Personal Data Breach.</p>	<p>✓ The Local FDP User Organisation, on becoming aware of an Incident concerning the NHS-PET or the Data Platform shall immediately notify NHS England's National Service Desk and provide as much information as they can at the time of notification.</p> <p>The Local FDP User Organisation will notify the ICO and Data Subjects affected where required in accordance with Articles 33 and 34 of UK GDPR in relation to Personal Data Breaches affecting its local Instance or Processing of Personal Data in the NHS-PET prior to Processing in or on leaving its local Instance except where the Personal Data</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>NHS England will notify the Local FDP User Organisation on behalf of the FDP Contractor in relation to any Incidents reported to NHS England which impact on its local Instance.</p> <p>NHS England will notify the ICO and Data Subjects affected where required in accordance with Articles 33 and 34 of UK GDPR in relation to Personal Data Breaches affecting the national Instance or Processing of Personal Data in the NHS-PET prior to Processing in or on leaving the national Instance.</p> <p>NHS England will notify the ICO and Data Subjects affected where required in accordance with Article 33 and 34 of UK GDPR in relation to Personal Data Breaches affecting local Instances or Processing in the NHS-PET prior to Processing in or leaving local Instances where the Personal Data Breach is considered to have arisen due to the design, governance or service management of the Data Platform or NHS-PET.</p> <p>Where there is a Personal Data Breach in one or more local Instance that may be reportable to the ICO or to</p>	<p>Breach arose due to the design, governance or service management of the Data Platform or NHS-PET.</p> <p>Where there is a Personal Data Breach in one or more local Instance that may be reportable to the ICO or to Data Subjects under Articles 33 and 34 then NHS England and the Local FDP User Organisations whose local Instances are affected will liaise with each other to determine whether the Personal Data Breach arose as a consequence of the design, governance and service management of the Data Platform and NHS-PET or as a result of the use of the local Instance or NHS PET by the Local FDP User Organisations.</p>

UK GDPR Requirement	NHS England	Local FDP User Organisation
	<p>Data Subjects under Articles 33 and 34 then NHS England and the Local FDP User Organisations whose local Instances are affected will liaise with each other to determine whether the incident arose as a consequence of the design, governance and service management of the Data Platform or NHS-PET or as a result of the use of the local Instance or NHS PET by the Local FDP User Organisations.</p>	
Data Protection Impact Assessment		
Articles 35-36 – Data Protection Impact Assessment and prior consultation.	<p>✓ NHS England is responsible for producing an overarching DPIA for each of the Data Platform and NHS-PET and for consulting, as appropriate regarding Processing of Personal Data in relation to the Data Platform and NHS-PET. These overarching DPIAs will be made available to the Local FDP User Organisations.</p> <p>NHS England is responsible for producing an Ontology DPIA for the use of Personal Data within the Products in the national Instances of the Data Platform and for</p>	<p>✓ Making use of the templates provided by NHS England, the Local FDP User Organisation shall adopt, adapt, or create an overarching DPIA for each of the Data Platform and NHS-PET and a DPIA for each Product that is deployed in their local Instance.</p>

UK GDPR Requirement	NHS England		Local FDP User Organisation	
		<p>consulting, as appropriate regarding Processing of Personal Data in relation to the national Instance.</p> <p>NHS England will produce National Product DPIAs for Products in the national Instance and DPIA Templates for Products to be deployed in local Instances. The template DPIAs will be made available to Local FDP User Organisations to help create their own Product DPIAs relating to their use in their local Instances.</p>		

24. Appendix – IG Framework

- [NHS England » Federated Data Platform: information governance framework](#)