Template Version	FDP National DPIA Template (Pseudo) version 1.1 240424		
Document filename	*DPIA FDP Ambulance Data Services (ADS) Dashboard*		
Directorate / Programme	FDP Programme	Product Name	*Ambulance Data Services (ADS) Dashboard*
Document Reference No	*IG2023161*	Information Asset Register Number	FDP070N
Information Asset / Product Owner Name	[redacted]	Version	4.0
Author(s)	[redacted]	Version issue date	*05/02/2025*

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

FDP Product Data Protection Impact Assessment – Ambulance Data Services (ADS) Dashboard

Document Management

Revision History

Version	Date	Summary of Changes
0.1	18/03/2024	Minor updates for clarity.
0.2	18/03/2024	Addition of use case table
0.3	18/03/2024	Minor updates for clarity
0.4	20/03/2024	Final Version Created for approval
0.5	20/03/2024	Minor updates with approval
0.6	21/03/24	Minor updates with approval
1.0	21/03/2024	Final
1.5	21/03/2024	Further update and finalised
1.6	21/10/2024	Further update to document
1.7	30/10/2024	Clean version
2.0	30/10/2024	Final approved version
2.1	05/11/2024	Update to the use of information
3.0	05/11/2024	Finalised document
4.0	05/02/2025	Updated to reflect additional datasets to the Product

Reviewers

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

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[redacted]	[redacted]	0.4 0.5	20/03/24 20/03/24
[redacted]	[redacted]	0.4	20/03/24
[redacted]	[redacted]	0.6	21/03/24
[redacted]	[redacted]	1.7/ 4.0	05/02/2025

Approved by

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

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version

[redacted]	[redacted]	20/03/24	0.5
Jackie Gray	Director of Privacy, and Information Governance (Deputy SIRO)	20/3/24	0.5
[redacted]	[redacted]	05/02/2025	4.0

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of this document

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

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

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

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

Defined Terms used in this DPIA

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

Standard wording in this DPIA

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

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

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

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

The aims of the Federated Data Platform (FDP)

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

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

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

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

The Federated Data Platform (FDP)

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

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

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

1. Better outcomes and experience for people

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

2. Better experience for staff

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

3. Connecting the NHS

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

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

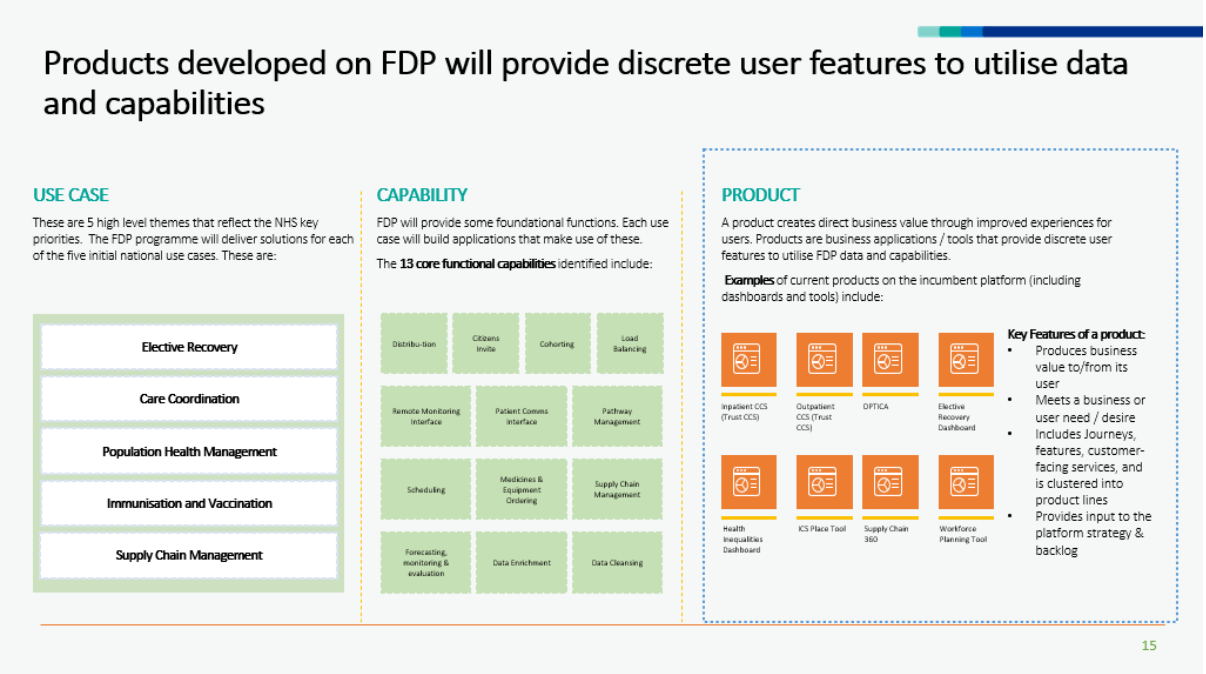
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

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

The ‘Product’ Data Protection Impact Assessment (DPIA)

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

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



Key information about the Product
Purpose of the Product - Overview
The Product will provide oversight of the operational activity of Ambulance Services to support delivery challenges and improvement/efficiencies to patient care and safety and operational delivery. This ensures that organisations accessing the Data can all view the same Data to support care co-ordination for patients across the NHS. **Update 25/10/2024** There has been an update to the Product to include Emergency Care Dataset (ECDS) to allow the development of metrics and visualisation of the ECDS with Ambulance Data Sets. **Update 05/11/2024** There has been a further update to the metrics being created through the dashboard. The below has been updated: - Tableau for rolling 30 day positions - ED and non-ED split - Monthly, weekly, year to date breakdowns - Comparison periods and change e.g. this week vs last week + difference **Update 05/02/2025:** There has been a further update to the datasets, there will be additional data items from the ECDS dataset, these data items are in the FDP Ontology as well as UDAL and fall within the appropriate directions and the directed use.

Local or National Product			
Local	☐	National	☒

Product falls under the following Use Case(s)		
Care co-ordination	☒	To ensure that health and care organisations all have access to the information they need to support the patient, enabling care to be coordinated across NHS services.
Elective Recovery	☐	To get patients treated as quickly as possible, reducing the backlog of people waiting for appointments or treatments, including maximising capacity, supporting patient readiness and using innovation to streamline care.
Vaccination and Immunisation:	☐	To ensure that there is fair and equal access, and uptake of vaccinations across different communities.
Population Health Management	☐	To help local trusts, Integrated Care Boards (on behalf of the integrated care systems) and NHS England proactively plan services that meet the needs of their population.
Supply Chain	☐	To help the NHS put resources where they are needed most and buy smarter so that we get the best value for money.
Categorisation of the Data used to create the Product		**How the different Categories of Data are used in relation to the Product**
Directly Identifiable Personal Data	☐	
Pseudonymised Data	☒	For Data ingested into the FDP to create the Product
Anonymised Data	☐	
Aggregated Data	☒	For Data displayed or shared with users of the Product
Operational Data	☒	For Data displayed or shared with users of the Product
Type of Data used in the Product		
No Personal Data	☐	
Personal Data	☒	For Data displayed or shared with users of the Product

Special Category Personal Data	☒	For Data displayed or shared with users of the Product

The Product DPIAs describe:

- the purpose for the creation of the Product;
- the Data which has been processed to create the Product. Where Aggregated Data is ingested into FDP, a DPIA is still carried out to provide assurance that the Aggregated Data is not Personal Data;
- the supporting legal basis for the collection, analysis and sharing of that Data;
- the Data flows which support the creation of the Product, and;
- the risks associated with the Processing of the Data and how they have been mitigated.

National Product DPIAs

The Products described in the national Product DPIAs relate to NHS England's use of the Product and related Data in the national Instance of the platform, and therefore all risks and mitigations of those risks contained within the DPIA are only applicable to NHS England.

Local Product DPIAs

The Products described in the template local Product DPIAs relate to an NHS Trust or ICB use of the Product and related Data in a local Instance of the platform, and therefore all risks, and mitigations of those risks, contained within the DPIA are only applicable to Trusts and ICBs.

NHS Trusts and ICBs who use the Products made available to them are responsible for adopting and updating the template local Product DPIA or producing their own DPIA to reflect their specific use of the Product and to assess any specific risks relating to their organisation's use of the Product.

1. Consultation with Stakeholders about the Product

Ambulance Services, regional and national Urgent and Emergency Care (UEC) Leads and commissioners have been involved in the development of the overarching Ambulance Data Set (ADS) Specification.

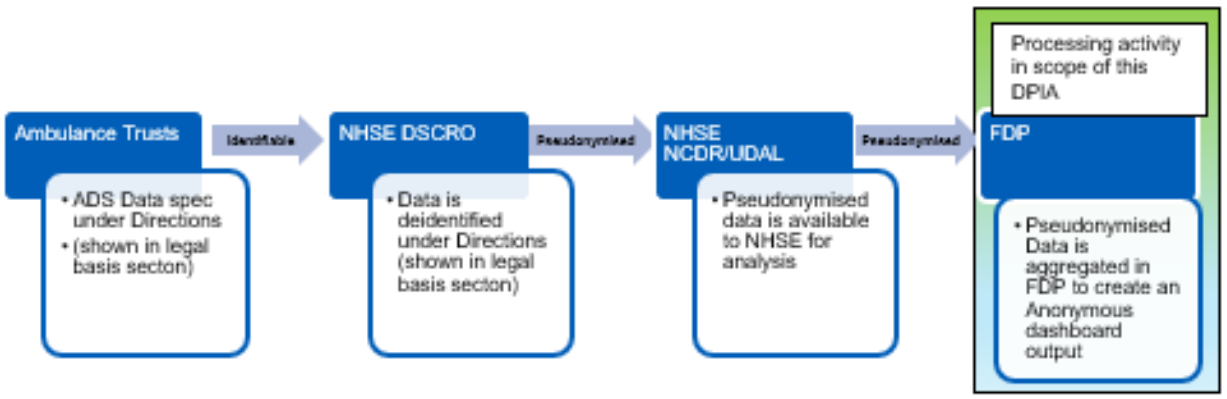
All Ambulance Services have completed updates to their DPIAs and system technologies to capture the information required for ADS in the correct format and Data fields and have updated Organisational Privacy Notices where applicable.

NHS England has also completed a DPIA for receipt and processing of the initial patient identifiable Data through the API route under the Ambulance Data Set (ADS) Directions 2022.

Discovery work has been undertaken with Ambulance Services, regional and national UEC Leads and commissioners to understand the requirements of the Ambulance Dataset Dashboard

Consultation was also undertaken with stakeholders for the initial collection of the Data under the Ambulance Data Set (ADS) Directions 2022 (the Directions).

2. Data Flow Diagram



The ADS Data collected under Directions flows to the NHSE AGEM Data Services for Commissioners Regional Office (DSCRO) to be Pseudonymised before flowing to the National Commissioning Data Repository (NCDR) and the Unified Data Access Layer (UDAL) for NHSE analysis.

For the purposes of creating this Product, the Pseudonymised ADS Data then flows into the FDP to be aggregated so that it can be used to populate the ADS dashboard. The ADS Dashboard only provides users with access to Anonymous Aggregated Data and Operational Data.

3. Description of the Processing

The Ambulance Data set (ADS) which is the underlying Data source used in the Product, has been designed, developed and implemented across all English Ambulance Services to collect standardised patient level information about activity delivered by ambulance services. The Pseudonymised ADS Data is transferred from UDAL into FDP, as explained in the Data Flow Map above.

NHS England uses this Product to support the development of national policy within the Ambulance Team in the Integrated Urgent and Emergency Care Directorate, as well as providing commissioners with information to make a case for change and supporting operational management at an ICS, Regional and National Level.

The information in the ADS Data provides a strong evidence base for change. This includes, but is not limited to:

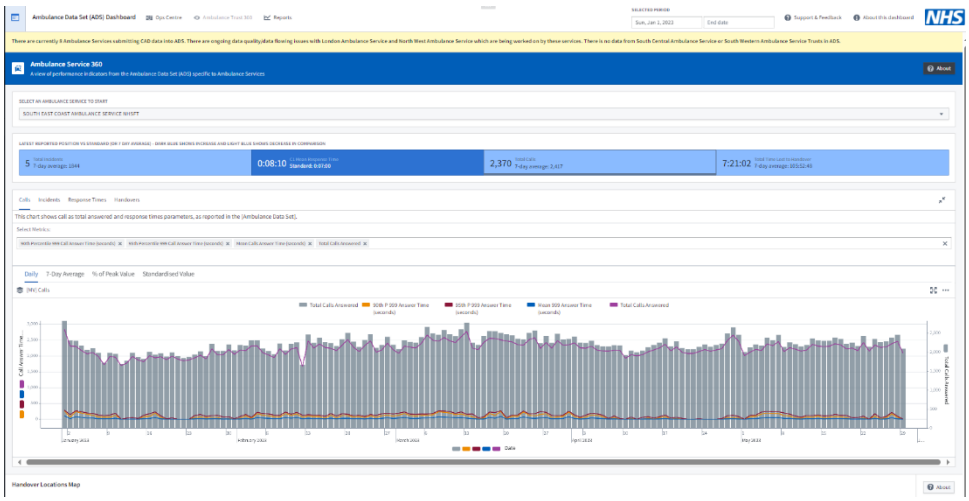
- Identification of patterns of activity to identify unwarranted variation in operational delivery;
- Outcomes of patient incidents to support review of prioritisation of ambulance calls to improve patient safety and ensure all patients, but in particular the most acutely unwell patients receive a timely and appropriate response;
- Identify and benchmark best practice to share with services to facilitate improvement; and

- Monitoring and addressing system challenges using Data to identify particular health conditions and/or patient groups requiring additional support.

4. Purpose of Processing Personal Data for this Product

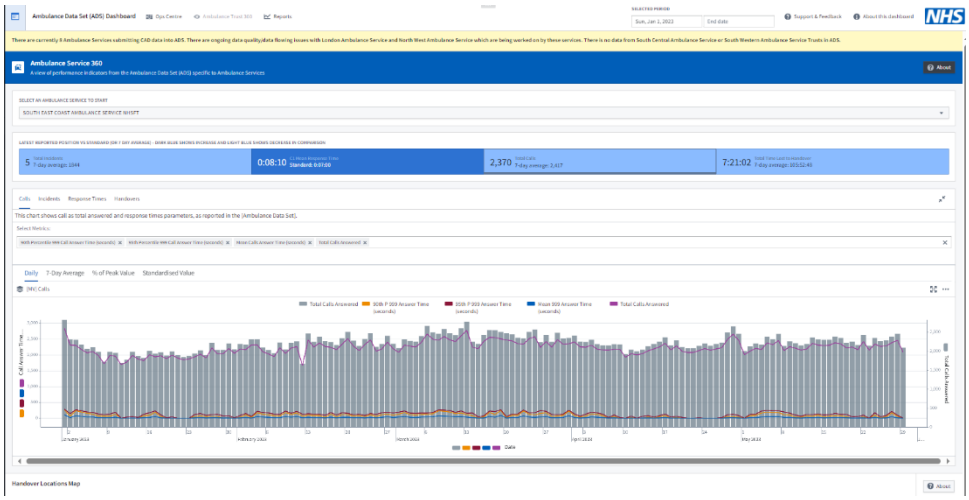
The Product comprises of a number of dashboards:

- The 'Operations Centre' Dashboard provides a summary of key performance indicators across regions and ambulance services. A national view is available for individuals within NHSE who require a national view. For other users, access has been designed so that users will only see the geographical levels within the scope applied. Handover information is available at ICB level (limited to their geographical area).



- The 'Reports' tab offers the user the opportunity to compare activity (this will be within specific geographical levels according to the user's geographic scope. This allows a combination of time series and benchmarking opportunities to understand activity comparisons.

- The 'Ambulance 360 Dashboard' provides users with greater detail for specific service activity, with a timeseries of performance and optional metrics within established measure groups.



- The 'Ambulance 360 Dashboard' also provides a 'map version' of handover activity and allows users to identify the location of handover pressures.

The Product will be used to realise the strategic ambition described at section 1.33 the NHS Long Term Plan 2019: "*Without access to timely and accurate Data we cannot maximise the opportunities to improve care for all patients"*.

The Pseudonymised Data, which has been aggregated in FDP to create the ADS dashboards, will be made available to NHS England, ICBs and NHS Trust users only as Anonymous Aggregated Data and Operational Data. This will provide them with oversight of the operational activity of Ambulance Services to support delivery challenges and improvement / efficiencies to patient care and safety and operational delivery. This ensures that organisations accessing the Data can see the same Data and for the same purpose as NHS England (albeit, limited to that organisation's geographic area).

The Product will deliver the benefits of the ADS Data to support ongoing and new streams of Ambulance Policy development across four key areas on the dashboard:

- management information;
- strategic and programme reporting;
- commissioner support; and
- UEC Pathways.

The Data in the dashboard, is also used to inform the calculations displayed within the Data insight tools.

5. Identification of risks

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

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

Risk No	**Describe source of the risk and nature of potential impact on individuals** *The highlighted text are the most identified risks in the programme. Please amend and delete as appropriate and add Product specific risks. If the Data being processed is Directly Identifiable Personal Data, the risks will be different from below and you should refer to this category of Data. If the Data being processed is only Aggregated Data, then most of the risks below, other than small number suppression, may not be relevant.*
1	There is a risk that Pseudonymised Data may be accidentally misused by those with access
2	There is a risk that Pseudonymised Data will be processed beyond the appropriate retention period.
3	There is a risk that insufficient organisational measures are in place to ensure appropriate security of the Pseudonymised Data (e.g. policies, procedures, disciplinary controls)
4	There is a risk that insufficient technical measures are in place to ensure appropriate security of the Pseudonymised Data (e.g. encryption, access controls)
5	There is a risk that Pseudonymised Data could be deliberately manipulated by an internal bad actor in some way to re-identify individual people
6	There is a risk that unsuppressed small numbers in Aggregated Data made available via the Product dashboard could lead to the identification of an individual
7	There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures.
9	There is a risk of failure to provide appropriate transparency information to data subjects.
10	There is a risk that increased access to Special Category Personal Data is given to NHS England staff who would not normally access that Data within their role.
11	There is a risk that the platform becomes inaccessible to users which could cause delays in the management of patient care and availability of Data.

12	There is a risk that inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product.
13	There is a risk that users will attempt to access FDP and the Product from outside the UK, increasing the data security risk.
14	There is a risk that users will not have their permissions revoked when they leave their role/organisation.

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

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

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

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

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

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

Source Dataset	Statutory Authority for collection of Data	Statutory Authority for Processing & Analysis of Data	Statutory Authority for sharing of Data
Ambulance Dataset	Ambulance Data Set Directions	NHS England De-Identified Data Analytics and	Health and Social Care Act 2012 s261(5)(d) and s13Z3 (e) and (f)

	2022 - NHS Digital	Publication Directions 2023	
ECDS	Emergency Care Data Set (ECDS) - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	Health and Social Care Act 2012 s261(5)(d) and s13Z3 (e) and (f)

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

Article 6 – Personal Data

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

Article 9 – Special Category Personal Data

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

Common Law Duty of Confidentiality

- **Legal obligation –** NHSE is required by law to process Confidential Patient Data it collects, Pseudonymises and analyses to create the Pseudonymised Data Aggregated Data input and Aggregated Data output for the Product. This is required under legal directions referred to above and issued by the Secretary of State for Health and Social Care to NHSE under section 254 of the Health and Social Care Act 2012.

- The Anonymous Aggregated Data and Operational Data which is shared with users through the dashboards is not Confidential Data.

8. Demonstrate the fairness of the Processing

Fairness means that we should handle Personal Data in ways that people would reasonably expect and not use it in ways that have an unjustified adverse impact on them.

The Product will have its own transparency information which sets out why the Processing is fair in what it is intended to achieve to improve the care of patients. Further information is set out in section 9 below.

Regarding the impact on individuals, the purpose of collecting and using the Data is to ensure that the NHS can operate and effectively provide and co-ordinate the care of individuals which falls within the Care Co-ordination Use Case. The impact for individuals of NHS England Processing this Data includes, but is not limited to:

- Identification of patterns of activity to identify unwarranted variation in operational delivery;
- Outcomes of patient incidents to support review of prioritisation of ambulance calls to improve patient safety and ensure all patients, but in particular the most acutely unwell patients receive a timely and appropriate response; and

- Identify and benchmark best practice to share with services to facilitate improvement

NHS England is Processing Data in the Product to enable the NHS to operate effectively and to benefit patient care.

Any potential adverse impact to individuals is mitigated by the data being processed for this Product having been Pseudonymised. The information shared in the dashboards to users is Anonymous Aggregated Data and Operational Data.

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

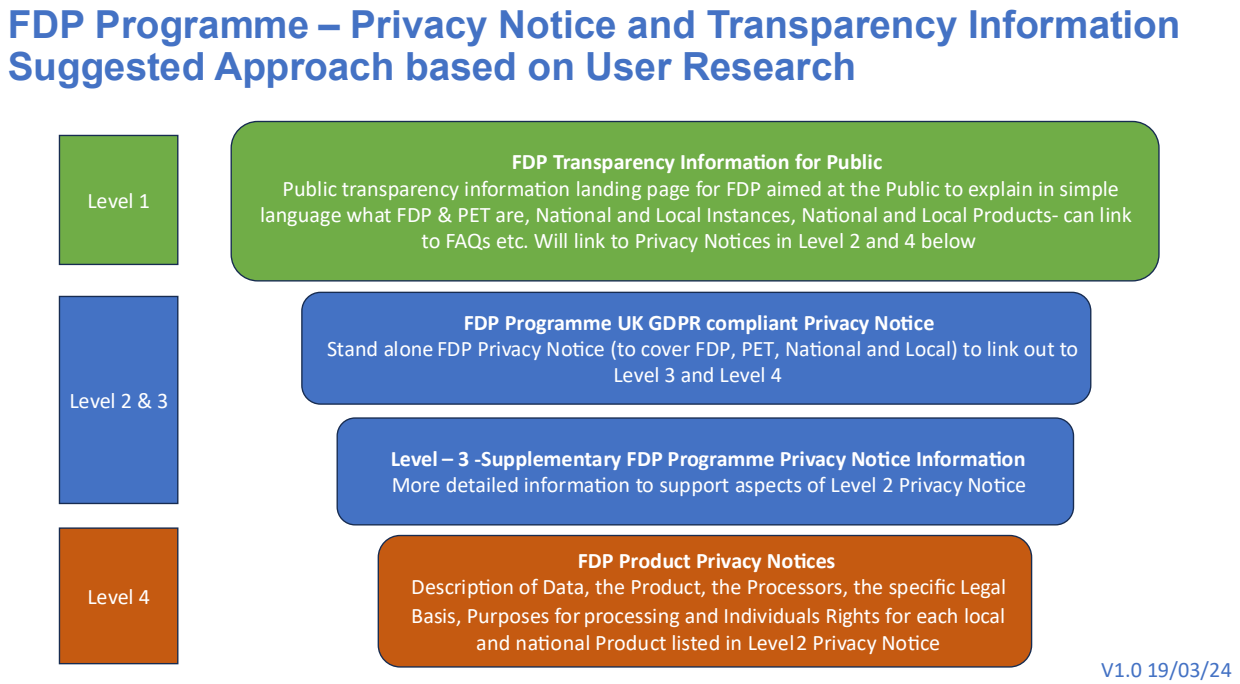
There is a range of information available on the NHS England website about FPD and how it works. This is Level 1 Transparency information.

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

NHS England » NHS Federated Data Platform privacy notice

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

NHS England » FDP products and product privacy notices



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

Data Categories [*Information relating to the individual's*]	**Yes/No**	**Justify** *[there must be justification for Processing the Data items. Consider which items you could remove, without compromising the purpose for Processing]*
Personal Data		
Name	No	
Address	No	
Postcode	Yes	The Postcode is derived to Lower Super Output which means that postcodes are aggregated to an average population of 1500 people or 650 households
Date of Birth	Yes	DOB is derived to month and year of birth in the Pseudonymised Data which is used to create this Product.
Age	Yes	To show demographic differences in metrics
Sex	Yes	To show demographic differences in metrics
Marital Status	No	
Gender	No	
Living Habits	No	
Professional Training / Awards / Education	No	
Email Address	No	
Physical Description	No	
General Identifier e.g. NHS No	Yes	A Pseudonymised Identifier is used
Home Phone Number	No	
Online Identifier e.g. IP Address/Event Logs	No	
Mobile Phone / Device No / IMEI No	No	
Location Data (Travel / GPS / GSM Data)	Yes	To understand distances travelled by ambulances.
Device MAC Address (Wireless Network Interface)	No	
Special Category Data	es/No	
Physical / Mental Health or Condition, Diagnosis/Treatment	Yes	To understand and reduce inequalities impacting patient care.
Sexual Life / Orientation	No	
Religion or Other Beliefs	No	
Racial / Ethnic Origin	Yes	To understand and reduce inequalities impacting patient care.
Biometric Data (Fingerprints / Facial Recognition)	/No	
Genetic Data	No	
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences	No	

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

Updated 02/05/2025

ADS Specification

ADS Specification Excel

Datasets in UEC Workstation - ADS

11. Provide details of Processors who are Processing Personal Data in relation to this Product

- The Platform Contractor is a Processor acting on behalf of NHS England as a Controller in relation to Processing Pseudonymised Data held on the Platform, and which is used in the Product. The Platform Contract has required Data Processing provisions in it which meet the requirements of UK GDPR. In addition, a separate Data Processing Annex providing specific Processing instructions to the Platform Contractor for this Product will be issued.

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

Users of the dashboard may include:

- NHS England, Integrated Care Boards (ICBs) and NHS Trusts who have access to Aggregated Data and who use the dashboard for analysis of ambulance services and activity delivered across areas.

Access will be granted in line with Role Based Access Controls by the IAO.

13. How long will the Data be retained?

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

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

No identifiable CPI data is processed in these analytical workspaces, for the information provided in pseudonymised form, we ensure that the latest Data supplied is always used with any amended records deleted or archived. We perform Data quality checks at the point on receiving Data and at the end stage of final analysis to ensure that Data is consistent with previous publications. We share these findings and escalate any Data inaccuracies with the Data Controllers

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

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

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

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

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

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

Redaction Rationale – *The information below has been redacted as this includes information relating to information security within NHS England, this has been completed in line with Section 31 (1)(a) of the Freedom of Information Act 2000.*

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

Business Continuity Arrangements

Should the FDP processing fail, the ability to undertake the processing using the Universal Data Access Layer (UDAL) as a backup platform would be implemented.

Specific Access controls for this Product

[redacted]

A small number of NHSE and North England CSU Analysts, responsible for delivery of the dashboard, will have secure permission-based access to the Pseudonymised Data within the ADS purpose of FDP in order to manage the required dashboard aggregate-level visualisations for the users.

[redacted] The product owner and IAO will be required to approve the access based on the Purpose Based Access Controls in place for the Product.

17. In which country/territory will Data be stored or processed?

All Processing of Data will be within the UK only, this is a contractual requirement and one of the key principles of the FDP IG Framework

18. Do Opt Outs apply to the Processing?

The National Data Opt Out policy does not apply to this Product as:

- The collection and analysis of Data by NHS England to create the Product has been carried out under a legal obligation (the Legal Direction) and therefore the National Data Opt out does not apply.
- No Confidential Patient Information will be disclosed to users of the Product via the dashboard which only provides access to Anonymous Aggregated Data.

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

19. Risk mitigations and residual risks

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

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

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

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk.** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
1	Pseudonymised Data may be accidently misused by those with access	1. External suppliers are on contracts with relevant security and data protection clauses contained within the agreements. Internal security and data protection processes are in place within NHS England. 2. 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. 3. The download functionality of data from the FDP is disabled by default, and access to this is controlled by the relevant FDP User which ensures appropriate governance in in place.	Section 12 & 16	Tolerate	Remote	Significant	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
		4. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to data.					
2	Pseudonymised Data may be processed beyond the appropriate retention period.	1.Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place. 2.The business area responsible for the data have a Records Management Information Co-ordinator who will provide advise on how long data should be retained at the point the dashboard is decommissioned in line with the NHS Records Management Code of Practice .	Section 13	Tolerate	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the Personal Data (e.g. policies, procedures, disciplinary controls)	1.Appropriate organisational measures in relation to Data controls and governance are in place to ensure the security of the Data. 2. Organisational measures are adhered to across the Data platform. Any breaches are reported in line with these. 3. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Data.	Set out in the Overarching FDP DPIA and Section 12 & 16 above	Tolerate	Remote	Minimal	Low

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 using at least TLS1.2 3. SLSP in place	Set out in the Overarching FDP DPIA and Section 12 & 16 above	Tolerate	Remote	Minimal	Low
5	Pseudonymised Data could be deliberately manipulated by an internal bad actor in some way to re-identify individual people	1. As the Aggregated Data has small numbers included, a risk assessment was undertaken to ascertain if the data continue to be personal data. This concluded that whilst small numbers are shown, they do not relate to individuals but to counts of activity across the ambulance services and therefore do not directly or indirectly relate to an individual.	Set out in the Overarching FDP DPIA and Section 11, 12 & 16 above	Tolerate	Remote	Significant	Low
6	Unsuppressed small numbers in Aggregated Data [ingested into Product and/or made available via the Product dashboard]	1. As the Aggregated Data has small numbers included, a risk assessment was undertaken to ascertain if the data continue to be personal data. This concluded that whilst small numbers are shown, they do not relate to individuals but to counts of activity across the ambulance services and therefore do not directly or indirectly relate to an individual.	Section 3 & 7	Tolerate	Remote	Minimal	None

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
	could lead to the identification of an individual						
7	Insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures supporting the Product.	1. Full details are described in the Overarching FDP DPIA. 2.For national Products migrating from Foundry to FDP, there is no change in the Product, its operation or the technical measures supporting it. New governance processes for migrating existing Products have been put in place, including approval of relevant DPIAs by the DGG and the Deputy SIRO. This updated DPIA has also been put in place to assess the risks consistently across all national Products.	Set out in the Overarching FDP DPIA and Section 3, 12 & 16 above	Tolerate	Remote	Minimal	Low
8	Subject Access Requests will not include a search of FDP or the Product, preventing individuals from having access to all Personal	1. Existing internal NHSE procedures for managing DSARs have been updated to include consideration of any Personal Data held in FDP.	Section 15	Treat	Remote	Minimal	Low

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
	Data held about them						
9	Failure to provide appropriate transparency information to data subjects.	1. The NHSE General FDP Privacy Notice has been published and a separate Product Privacy Notice has been produced and will be published on NHS England's website with a link to it from the General FDP Privacy Notice.	Sections 8 and 9	Tolerate	Remote	Significant	Low
10	Increased access to Special Category Personal Data is given to staff who would not normally access that Data within their role.	1. Role Based and Purpose Based Access Controls are in place. The addition of the Restricted View function to sit over the Purpose Based Access Controls ensures only those who need access to Special Category Personal Data are able to access this 2. The Data Processed to produce the Product has been Pseudonymised before being ingested into FDP. 3. Only analysts responsible for developing the Product have access to the Pseudonymised Data.	Section 12 & 16	Treat	Possible	Minimal	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
11	The platform becomes inaccessible to users which could cause	1. The FDP Contractor is required to have Business Continuity Plans in place. 2. The Product Owner has Business Continuity Plans in place which cover the inaccessibility/unavailability of the Product.	Section 16	Tolerate	Remote	Significant	Low
12	Inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product.	1. The Product will only collect a sub-set of Personal Data from existing NHSE datasets. 2. It is our responsibility to ensure that all Data that is ingested into FDP for use in this Product is up to date and accurate for the purposes for which it is Processed within the Product. We will use our existing processes relating to the source datasets for maintaining accuracy.	Section 14	Tolerate	Remote	Significant	Low
13	Users will attempt to access FDP and the Product from outside the UK, increasing	1. It is clearly articulated within the FDP IG Framework that no personal/patient data should leave or be accessible from outside of the UK without the express prior approval from the Data Governance Group.	Section 17	Treat	Remote	Minimal	Low

Risk No	Risk	Steps to mitigate the risk	DPIA section in which step is described	Effect on risk. Tolerate / Terminate / Treat / Transfer	Likelihood of harm Remote / Possible / Probable	Severity of harm Minimal / Significant / Severe	Residual risk None / Low / Medium / High
	the data security risk.	2. It is within the Platform Contract that no access to the system should take place from outside the UK. 3. There are technical security measures in place to prevent access from outside the UK.					
14	Users will not have their permissions revoked when they leave their role/ organisation and may continue to have access to Data they are no longer entitled to access	1. As part of migrating national Products from Foundry to FDP, any users who have not accessed a migrating Product since January 2024 will have their access disabled. User accounts are also checked on a Product-by-Product basis with Product Owners regarding who should transition and if their access is still valid.	Section 12 & 16	Treat	Remote	Significant	Low

20. Actions

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

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

Action No	**Actions required.** (Date and responsibility for completion)	**Risk No impacted by action**	**Action owner** (Name and role)	**Date to be completed**
1	Ongoing review of unsuppressed data to ensure it remains Anonymous Aggregated Data or Operational Data when any new data items are added to the Product, or when any changes are made the dashboard visualisations.	6	Information Asset Owner – [redacted]	Ongoing at each change of the Product and update to this DPIA
2	Update DPIA to explain how Purpose Based Access Controls will be applied for this Product, including who will authorise analyst access and user dashboard access. Update does not require DPO or SIRO approval.	1 & 3	Information Asset Owner – [redacted]	End of April 2024

21.Completion and signatories

The completed DPIA should be submitted to the NHSE Privacy Transparency and Trust IG Team (for review).

The IAO (Information Asset Owner) should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the Processing, including new data items Processed, change of purpose, and/or system changes)

The DPIA accurately reflects the Processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Name	
Signature	
Date	

FOR DATA PROTECTION OFFICER USE ONLY

22. Summary of high residual risks

Risk no.	**High residual risk summary**

Summary of Data Protection Officer advice:

Name	
Signature	
Date	
Advice	

Where applicable: ICO (Information Commissioners Office) consultation outcome:

Name	
Signature	
Date	
Consultation outcome	

Next Steps:

- **DPO to inform stakeholders of ICO consultation outcome**
- **IAO along with DPO and SIRO (Senior Information Risk Owner) to build action plan to align the Processing to ICO's decision**

Annex 1: Defined terms and meaning

The following terms which may be used in this Document have the following meaning:

Defined Term	Meaning
Aggregated Data	Counts of Data presented as statistics so that Data cannot directly or indirectly identify an individual.
Anonymisation	Anonymisation involves the application of one or more anonymisation techniques to Personal Data. When done effectively, the anonymised information cannot be used by the user or recipient to identify an individual either directly or indirectly, taking into account all the means reasonably likely to be used by them. This is otherwise known as a state of being rendered anonymous in the hands of the user or recipient.
Anonymised Data	Personal Data that has undergone Anonymisation.
Anonymous Data	Anonymised Data, Aggregated Data and Operational Data.
Approved Use Cases	Means one of the five initial broad purposes for which Products in the Data Platform can be used as outlined in Part 1 of Schedule 2 (Approved Use Cases and Products) of the IG Framework, or any subsequent broad purpose agreed to be a use case through the Data Governance Group
Categorisation of Data	Means one of the following categories of Data: • Directly Identifiable Personal Data • Pseudonymised Data • Anonymised Data, • Aggregated Data • Operational Data In the case of Directly Identifiable Personal Data or Pseudonymised Data this could be Personal Data or Special Category Personal Data.
Common Law Duty of Confidentiality	The common law duty which arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
Confidential Patient Data	Information about a patient which has been provided in circumstances where it is reasonable to expect that the information will be held in confidence, including Confidential Patient Information.

Defined Term	Meaning
Confidential Patient Information	Has the meaning given in section 251(10) and (11) of the NHS Act 2006. See Appendix 6 of the National Data Opt Out Operational Policy Guidance for more information[1]
Controller	Has the meaning given in UK GDPR being the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (subject to Section 6 of the Data Protection Act 2018)
Data Governance Group	Means a national group established by NHS England to provide oversight to the approach to Data Processing and sharing across all Instances of the Data Platform and NHS-PET which will include membership from across FDP User Organisations
Data Platform or Platform	The NHS Federated Data Platform
Data Processing Annex	The annex to the schedule containing Processing instructions in the form set out in the FDP Contracts.
Data Protection Legislation	The Data Protection Act 2018, UK GDPR as defined in and read in accordance with that Act, and all applicable data protection and privacy legislation, guidance, and codes of practice in force from time to time
Direct Care	A clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care[2].
Directly Identifiable Personal Data	Personal Data that can directly identify an individual.
DPIA(s)	Data Protection Impact Assessments in a form that meets the requirements of UK GDPR
FDP	Federated Data Platform
FDP Contract	The NHS-PET Contract and the Platform Contract
FDP Contractor(s)	The NHS-PET Contractor and/or the Platform Contractor

[1] https://digital.nhs.uk/services/national-Data-opt-out/operational-policy-guidance-document/appendix-6-confidential-patient-information-cpi-definition

[2] See the National Data Guardian Direct Care Decision Support Tool: https://assets.publishing.service.gov.uk/media/5f2838d7d3bf7f1b1ea28d34/Direct_care_decision_support_tool.xlsx

Defined Term	Meaning
FDP Programme	The NHS England Programme responsible for the procurement and implementation of the FDP across the NHS
FDP User Organisations	NHS England, ICBs, NHS Trusts and other NHS Bodies (including a Commissioned Health Service Organisation) who wish to have an Instance of the Data Platform and who have entered into an MoU with NHS England. In the case of a Commissioned Health Service Organisation, the MoU is also to be entered into by the relevant NHS Body who has commissioned it
General FDP Privacy Notice	A privacy notice providing information on the Personal Data Processed in the Data Platform and by NHS-PET generally, including the Approved Use Cases for which Products will Process Personal Data
ICB	Integrated Care Board
ICS	Integrated Care System
Incident	An actual or suspected Security Breach or Data Loss Incident
Instance	A separate instance or instances of the Data Platform deployed into the technology infrastructure of an individual FDP User Organisation
National Data Opt Out	The Department of Health and Social Care's policy on the National Data Opt Out which applies to the use and disclosure of Confidential Patient Information for purposes beyond individual care across the health and adult social care system in England. See the National Data Opt Out Overview[3] and Operational Policy Guidance for more information[4]
NHS-PET Contract	The Contract between NHS England and the NHS-PET Contractor relating to the NHS-PET Solution dated 28 November 2023 as may be amended from time to time in accordance with its terms
NHS-PET Contractor	IQVIA Ltd
NHS-PET Solution	The privacy enhancing technology solution which records Data flows into the Data Platform and where required treats Data flows to de-identify them.
Ontology	Is a layer that sits on top of the digital assets (Datasets and models). The Ontology creates a complete picture by mapping Datasets and models used in Products to object types, properties, link types, and action types. The Ontology

[3] https://digital.nhs.uk/services/national-Data-opt-out/understanding-the-national-Data-opt-out

[4] https://digital.nhs.uk/services/national-Data-opt-out/operational-policy-guidance-document

Defined Term	Meaning
	creates a real-life representation of Data, linking activity to places and to people.
Operational Data	Items of operational Data that do not relate to individuals eg stocks of medical supplies.
Personal Data	Has the meaning given in UK GDPR being any information relating to an identified or identifiable natural person ('Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . For the purposes of this DPIA this also includes information relating to deceased patients or service users. Personal Data can be Directly Identifiable Personal Data or Pseudonymised Data.
Personal Data Breach	Has the meaning given in UK GDPR being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed
Platform Contract	The agreement between NHS England and the Platform Contractor in relation to the Data Platform dated 21 November 2023 as may be amended from time to time in accordance with its terms
Platform Contractor	Palantir Technologies UK Ltd
Product	A product providing specific functionality enabling a solution to a business problem of an FDP User Organisation operating on the Data Platform.
Product Privacy Notice	A privacy notice providing information on the Personal Data Processed in the Data Platform and by NHS-PET in relation to each Product, including the purposes for which the Product Processes Personal Data
Process or Processing	Has the meaning given in UK GDPR being any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction
Processor	Has the meaning given in UK GDPR being a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller
Programme	The Programme to implement the Data Platform and NHS-PET across NHS England, NHS Trusts and ICBs

Defined Term	Meaning
Pseudonymisation	Has the meaning given in UK GDPR being the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person
Pseudonymised Data	Personal Data that has undergone Pseudonymisation
Purpose Based Access Controls or PBAC	Means user access to Data is based on the purpose for which an individual needs to use Data rather than their role alone as described more fully in Part 2 of Schedule 3
Role Based Access Controls or RBAC	Means user access is restricted to systems or Data based on their role within an organisation. The individual's role will determine what they can access as well as permission and privileges they will be granted as described more fully in Part 2 of Schedule 3
Special Category Personal Data	Means the special categories of Personal Data defined in Article 9(1) of UK GDPR being Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic Data, biometric Data for the purpose of uniquely identifying a natural person, Data concerning health or Data concerning a natural person's sex life or sexual orientation.
Transition Phase	Is the first phase of rolling out the Data Platform which involves NHS England and local FDP User Organisations who currently use Products, moving their existing Products onto the new version of the software that is in the Data Platform. There is no change to the Data that is being processed, the purposes for which it is processed or the FDP User Organisations who are Processing the Data during the Transition Phase. The Transition Phase will start in March 2024 and is expected to run until May 2024.
UK GDPR	UK GDPR as defined in and read in accordance with the Data Protection Act 2018