| | | | |
|---|---|---|---|
| Template Version | FDP National DPIA Template (Pseudo) version 1.1 240424 | | |
| Document filename | IG2023171- National DPIA – A&E Forecasting Tool v6.0 Draft | | |
| Directorate / Programme | FDP Programme | Product Name | A&E Demand Forecasting Tool |
| Document Reference No | IG2023171 | Information Asset Register Number | *[Insert]* |
| Information Asset / Product Owner Name | [redacted] | Version | 6.0 Final Updated Approved |
| Author(s) | [redacted] | Version issue date | 05/08/2025 |

***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 – A&E Demand Forecasting Tool

# Document Management

## Revision History

| Version | Date | Summary of Changes |
|---|---|---|
| 0.1 | 27/03/2024 | Updating details from Foundry Product Tool to FDP |
| 0.2 | 02/04/2024 | Updates and clarifications |
| 0.3 | 09/04/2024 | Updates and clarifications |
| 0.4 | 12/04/2024 | Updates and clarifications |
| 0.5 | 12/04/2024 | Updates and Final Clean version created for DGG |
| 0.6 | 15/05/2024 | Moved onto FDP DPIA template, updated to reflect DGG comments – Final clean version for final approval |
| 0.7 | 16/05/2024 | Final approval review updates |
| 1.0 | 17/05/2024 | Marked as final approved |
| 2.0 | 16/10/2024 | Updated to reflect additional aggregate data flow |
| 3.0 | 29/10/2024 | Updated to reflect minor wording update |
| 4.0 | 14/11/2024 | Updated to reflect the addition of further weather information |
| 5.0 | 10/12/2024 | Updated to include a minor update which allows a download function for aggregate data only. |
| 5.1 | 28/07/2025 | Updated to include the name change and to include a share of aggregate data. |
| 5.2 | 05/08/2025 | FDP IG Team review |
| 6.0 | 05/08/2025 | Final updated approved |

## Reviewers

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

This document must be reviewed by the following people:

| Reviewer name | Title / Responsibility | Date | Version |
|---|---|---|---|
| [redacted] | Deputy Director IG Delivery Data & Analytics | 27/03/2024 | 0.3 |
| [redacted] | Deputy Director IG Delivery Data & Analytics | 12/04/2024 | 0.4 |
| [redacted] | Head of IG – FDP | 14/11/2024 | 0.6/2.0/3.0/4.0 /5.0 |
| [redacted] | Head of IG – FDP | 05/08/2025 | 5.2 |

## 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 |
|---|---|---|---|
| Jackie Gray | Director of Privacy and Information Governance (Deputy SIRO) | 16/05/2024 | 0.7 |
| [redacted] | [Insert], Product Owner | | 0.7 |
| Rebecca Llewellyn | FDP Programme Delivery Director | | 0.7 |
| [redacted] | Head of IG – FDP | 05/08/2025 | 6.0 |

# 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.

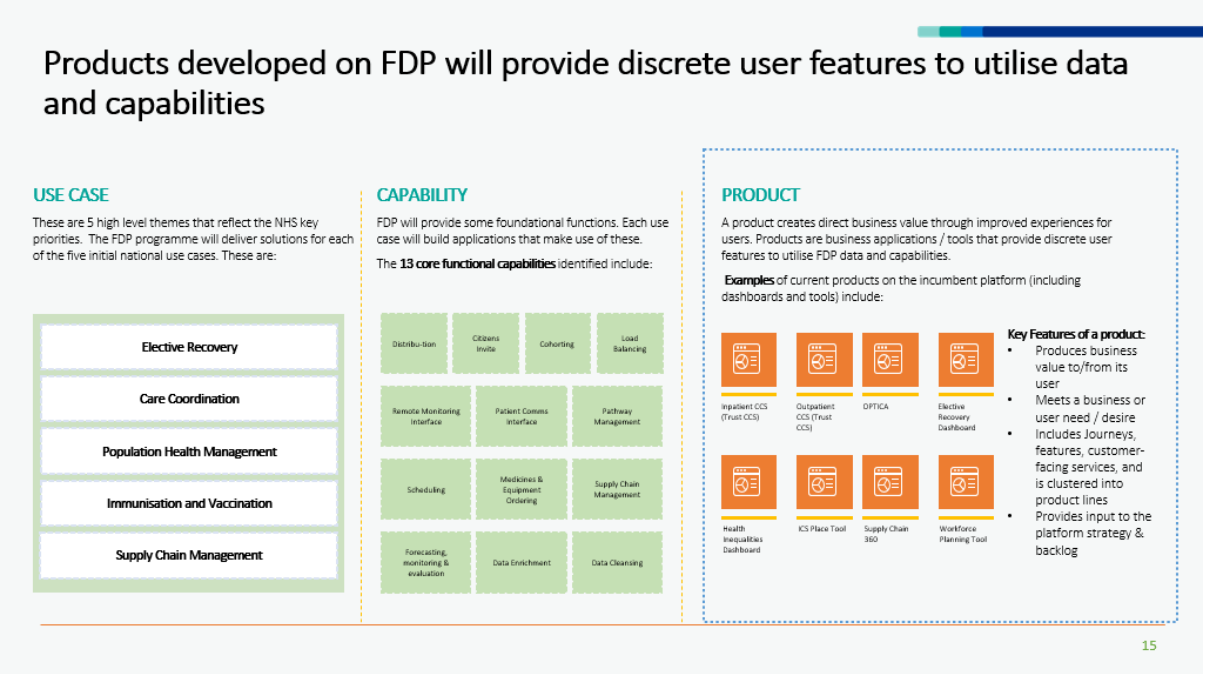
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that Data is managed and used across the NHS in England to transform services and save lives.

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 key objective of the Accident and Emergency (A&E) Forecasting Tool and associated dashboard is to develop a Product that provides intelligence to support local operational decision-makers with resource and capacity management to proactively plan their services for their population. The tool provides a daily forecast of aggregate A&E admissions (+ admissions by age group) 1-3 weeks in advance by considering factors such as weather data on specific days and age groups. The forecasting model underlying the tool is primarily developed by using past aggregated admissions data. In addition, the tool offers accuracy monitoring, so users can assess how close the recent forecasts have been to actual reported admissions.

**Update October 2024:**

Additional aggregate data feed for attendance forecasts, which include scenarios, metrics, segments and version added to the Product. No additional data has been used by the underlying model to produce these attendances forecasts.

**Update November 2024:**

Additional publicly available weather information is being added to the data set.

**Update December 2024:**

**Pre-approved data download**

At the moment, users of FDP products are able to visualize aggregate data on dashboards and users follow the user access management process in the platform to get access to products.

The **pre-approved data download** feature will grant access to users who have access to view aggregate data on dashboards to download the underlying data in CSV or Excel format.

**Update July 2025:**

The product name has been changed to ‘A&E Demand Forecasting Tool’ because the tool now provides forecasts of both admissions and attendances.

The downloadable Aggregate data will be flowed in to the existing System Coordination Centre (SCC) Product to allow ICB-based users to have an integrated few of demand facing their system.

| **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<br>For Data ingested into the Product to create the Product |
| Anonymised Data | ☐ | |
| Aggregated Data | ☒ | For Data ingested into the FDP to create the Product<br>For Data displayed or shared with users of the Product |

| | | |
|---|---|---|
| Operational Data | ☒ | For Data ingested into the FDP to create the Product<br>For Data ingested into the Product to create the Product |
| **Type of Data used in the Product** | | |
| No Personal Data | ☒ | For Data ingested into the FDP to create the Product<br>For Data ingested into the Product to create the Product<br>For Data displayed or shared with users of the Product |
| Personal Data | ☒ | For Data ingested into the FDP to create the Product<br>For Data ingested into the Product to create the Product |
| Special Category Personal Data | ☐ | |

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

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 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 programme to develop meaningful and accessible public communications.

- Information Governance Specialist group. A group of external stakeholders with subject matter expertise in data and information governance.

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 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 programme.

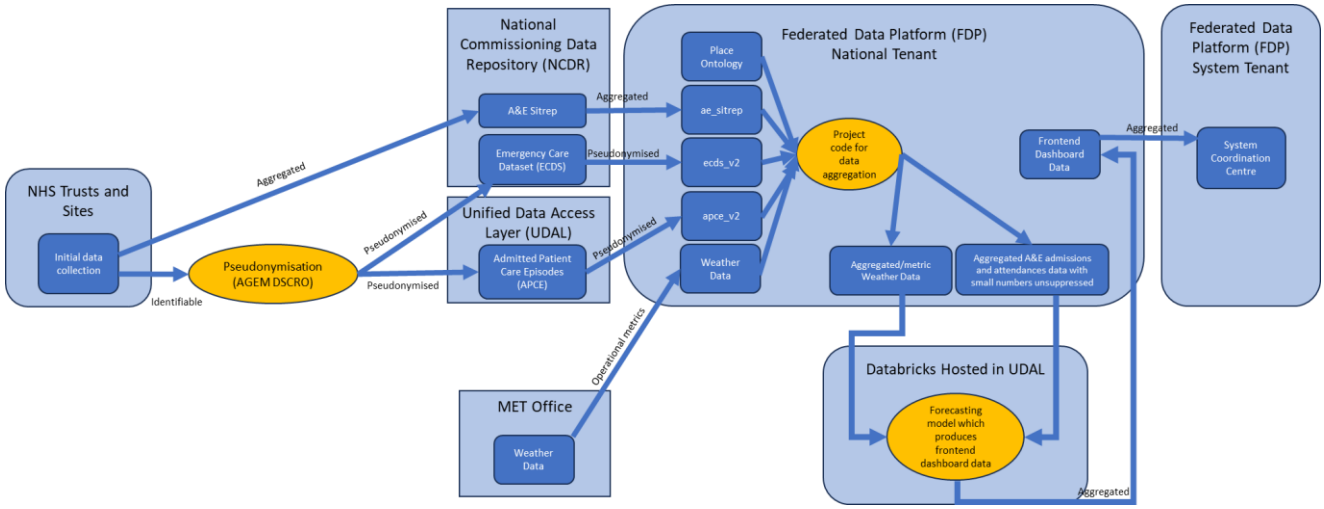
The tool was developed with periodic consultation and recommendations from a Steering committee that has included various SLT members from NHS:

- Chief Data and Analytics Officer
- National Clinical Director for Integrated Urgent and Emergency Care
- Director of Urgent & Emergency Care
- National Strategic Incident Director for the COVID-19 pandemic
- Director of Out of Hospital Urgent and Emergency Care
- Head of profession for statistics
- Director of Performance Information
- Director of UEC Operational Insight
- Senior Policy Advisor

This Accident and Emergency (A&E) Demand Forecasting Tool Product is an existing Product and data flow that is operational on the current Foundry platform and is now migrating to the Federated Data Platform (FDP). Prior to this being introduced on the Foundry platform, engagement took place with stakeholders, and this has continued to support the transfer to FDP.

The development of the tool started in April 2021. It was co-developed with Faculty AI as part of NHS England's contract with them from April 2021 – April 2023. Since the Faculty AI contract ended in April 2023, the tool has been completely owned and maintained by NHS England.

## 2. Data Flow Diagram




**Glossary**

Databricks – The primary platform we use for running, testing, and developing the A&E forecasting model. An important part of the UDAL technical function.

Place Ontology – The datasets in the FDP National Ontology which contain geographic information on which sites belong to which trusts, which trusts belong to which systems etc. This information is required when aggregating A&E admissions data up to different organisational levels. This data is Operational Data.

## 3. Description of the Processing

**Nature and scope of the processing:**

In the Federated Data Platform (FDP), the Pseudonymised secondary care patient level data, namely, Emergency Care Dataset (ECDS) and Admitted Patient Care Episodes (APCE) are aggregated at site, trust, system, region, and national level as well as at broad age groups – 0-5, 6-17, 18-65, 65+, and 75+. All levels of aggregation happen in the FDP. The aggregated data are then used by the tool to generate admissions forecasts at corresponding aggregation levels.

In terms of the ECDS and APCE datasets, when aggregating the Pseudonymised patient-level ECDS and APCE data we only consider a small subset of the information present in these datasets. The only bits of information relevant to our tool are whether or not a patient was admitted to hospital after attending A&E, the date of the admission, the NHS trust or site they were admitted to, and the patient's age at admission (aggregated up to broad age ranges, 0-5, 5-17 etc.). Other sensitive types of information in the source dataset such as gender, reason for admission, or ethnicity are not processed as part of the aggregation of data to create the Product.

Using the information outlined above our pre-processing pipeline then aggregates total admissions up to a trust, date and age segment level. For example, our final dataset might

say that 50 people over the age of 65 were admitted to a particular trust on a certain date but would reveal no personal or identifiable information about any individual patients.

The aggregated ECDS and APCE data, is then used alongside additional datasets, e.g. aggregated A&E sitrep data, and Operational Data: weather data provided by MET office, UK bank holidays and the Trust site data. Please see a full list of datasets in the data specification table in section 10 below.

The tool only uses Aggregated Data and Operational Data and generates output aggregated on geographic and broad age levels.

Even though all model inputs and outputs which relate to patients are aggregated, some of them will contain unsuppressed small numbers. For example, a user would be able to see that 5 people in a particular age group were admitted to a trust on a particular date via A&E. These small numbers are currently unsuppressed as any loss in forecasts fidelity will lessen the utility of the tool. Whilst unsuppressed small numbers are included, the team has engaged with Trusts and Operational Managers in the discovery phase of this use case to prove that it is necessary to show daily admission numbers for individual Trusts at this level. Stakeholder engagement showed strong operational support that daily admission numbers in age cohorts should be shown to optimise capacity planning ~3 weeks in advance. As the numbers surfaced on the dashboard are provided in age bands, the risk a patient being re-identified is considered to be very low.

**Context of the processing:**

The Accident and Emergency (A&E) Demand Forecasting Tool provides intelligence to support local operational decision-makers with resource and capacity management. The efficacy of this is impacted by demand uncertainty and pressures, particularly those related to urgent emergency care.

It provides a daily forecast of aggregate urgent admissions via A&E (+ admissions by age group) 1-3 weeks in advance.

In order to generate these forecasts, we need access to the historical admissions data provided in the Pseudonymised ECDS, APCE data, and the aggregated A&E Sitrep data. Much of the historical data used is sourced from APCE and A&E Sitrep, but since these datasets are not updated on a daily basis, they are supplemented by live daily data from the ECDS.

Weather data from the MET office is used in order to account for the impact of weather on A&E admissions when training the forecasting model.

The anticipated product users are:

- Senior operational planners at trust/ICS/ICB level
- System Control Centre leads
- Bed/site managers.
- Consultants and general managers across emergency care.
- NHS England national and regional operational and UEC teams

However, even at an aggregate level, we need to ensure that we apply the principles of lawfulness, fairness and transparency to the outputs and processing.

The project controls include:

- Regular quality assurance of outputs to ensure that forecasts are robust and statistically accurate
- Support for users in interpreting outcomes and understanding the drivers of analysis. This is done through engagements such as large demo sessions and smaller ad-hoc discussions with current and prospective users to help them take advantage of and understand the tool.

## 4. Purpose of Processing Personal Data for this Product

The primary aim of the Accident and Emergency (A&E) Demand Forecasting Tool and associated dashboard is to develop a Product that provides intelligence to support local operational decision-makers with resource and capacity management. The tool provides a daily forecast of aggregate A&E admissions (+ admissions by age group) 1-3 weeks in advance.

The Trusts consider their patients as their population and this tool supports the Trust to proactively assess how they need to plan and manage their A&E service to meet the needs of their population. The tool is also used by ICBs/ICSs to assess A&E activity, prospectively and retrospectively and therefore supports Population Health management use case of the Federated Data Platform.

The benefit of this Product to users is that it makes aggregate forecasts of admissions via A&E available to use in planning. This helps facilitate a better understanding of likely activity to inform decisions around capacity management and resource utilisation for their population. As shown in the data flow diagram, only the developers of the product have access to Pseudonymised data, which is processed in the Federated Data Platform (FDP) to generate the Aggregated data used in the Product. The forecasting tool only uses Aggregated Data and Operational Data and generates Aggregated Data outputs. The users of the tool only have access to Aggregated Data outputs via the FDP dashboard.

The forecasting tool is primarily developed on past Aggregated admissions data. To generate reliable and realistic forecasts it's imperative to have access to historical data on which to understand the model.

Historical values for average daily temperature from the MET office are also included in the tool. This is done to capture the potential impact of weather on hospital admissions. There is a large amount of evidence showing that weather conditions have a significant influence on the number and type of admissions through A&E departments, i.e. icy conditions are likely to result in falls and the requirement for more plaster technicians to be resourced to deal with broken bones.

Weather data, in this instance the average daily temperature, is matched to the Place Ontology data i.e. data on NHS trusts. For example, it was 11 degrees at Bolton Trust on

the 12th of Jan. This data never gets directly linked to any personal data. The aggregated data then flows into the tool to generate the aggregated outputs.

In addition, the tool offers accuracy monitoring, so users can assess how close the recent forecasts have been to actual reported admissions. This is done by allowing the user to overlay the forecast generated by the tool on top of the actual admissions numbers for a chosen date in the past. This functionality is displayed in Figure 5 below. It provides an extra level of assurance in using the forecasts.

Illustrative example of some of the visualisations available to users below (scale removed):

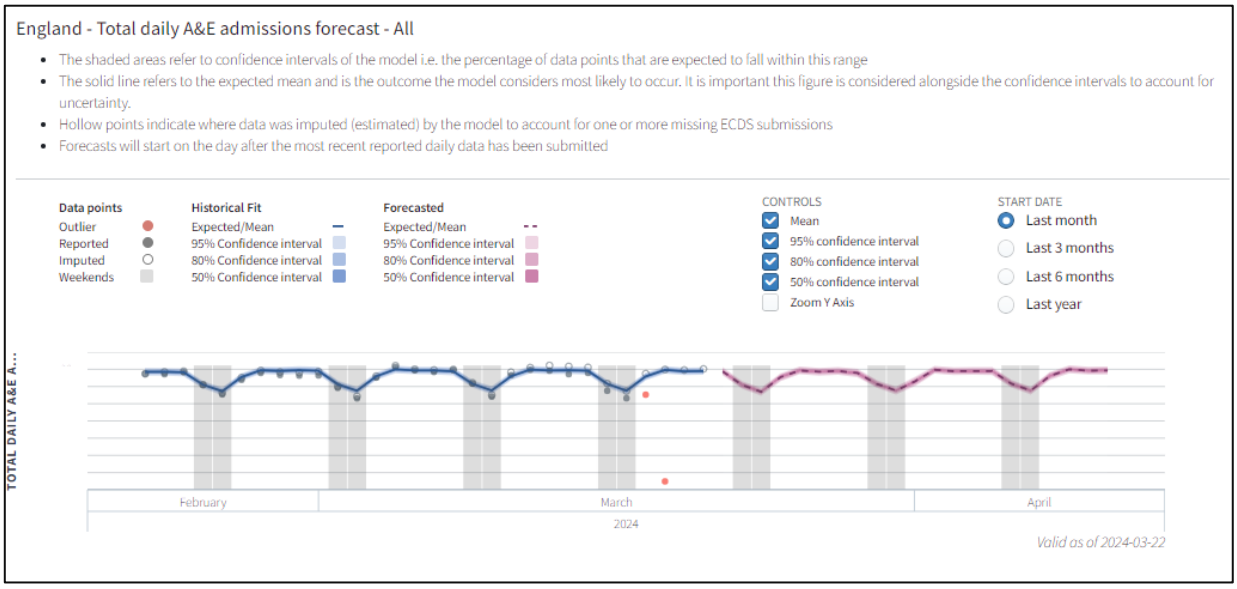



**Figure 1: National forecast and historical admissions**

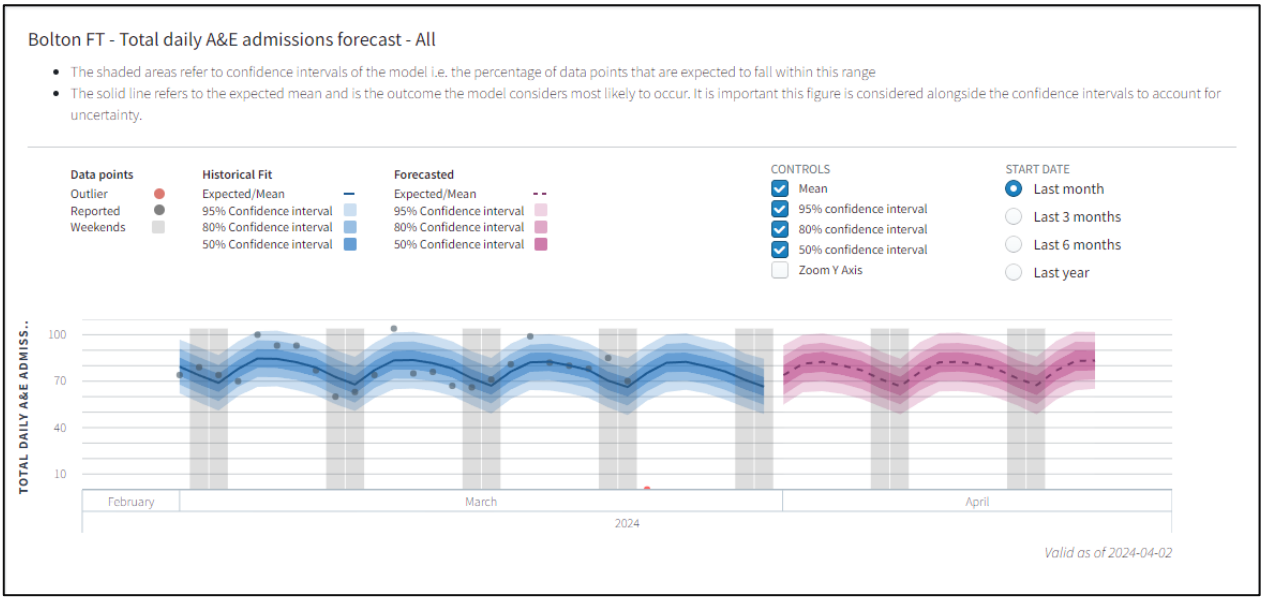



**Figure 2: Trust level forecast and historical admissions for Bolton FT**

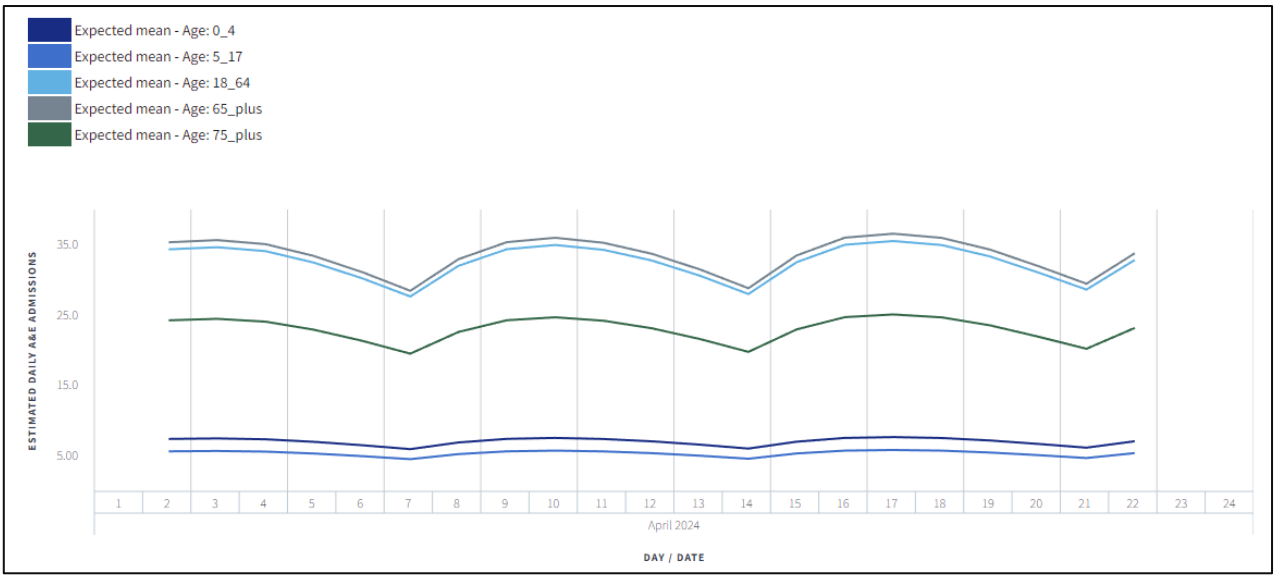



**Figure 3: Forecast with age breakdown an NHS FT**

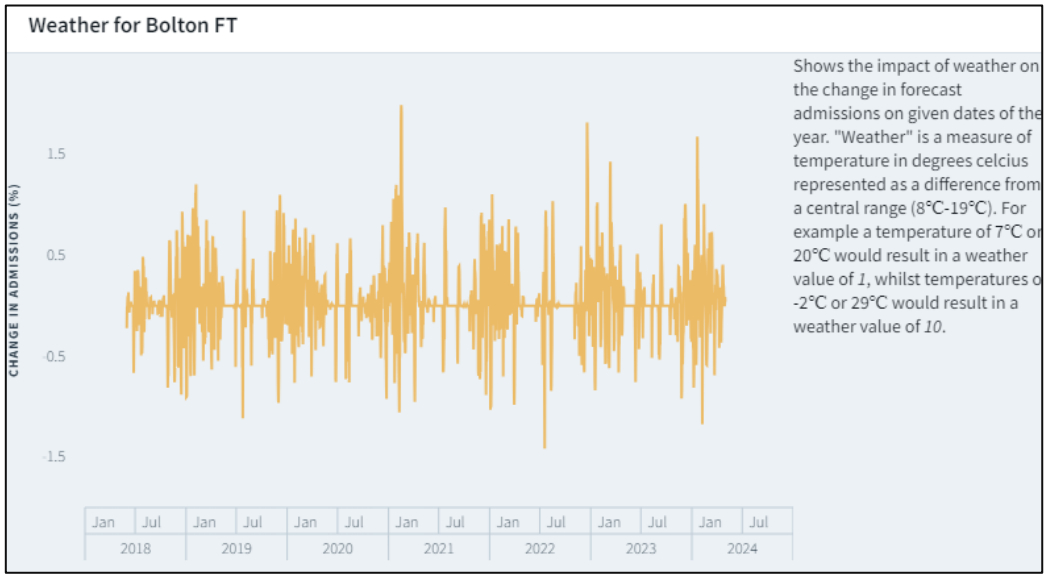



**Figure 4: Impact of weather on historical admissions according to our model**

Figure 5: Forecast (pink) made on 12/03/2024 overlayed on actual admissions number for an NHS FT

# 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**<br>*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 ingested into the FDP and/or the Product and/or 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. |
| 8 | There is a risk of failure to provide appropriate transparency information to data subjects. |

| | |
|---|---|
| 9 | There is a risk that increased access to Special Category Personal Data is given to NHS England staff who would not normally access that Data within their role. |
| 10 | There is a risk that the platform becomes inaccessible to users which could cause delays in the management of patient care and availability of Data. |
| 11 | There is a risk that inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product. |
| 12 | There is a risk that users will attempt to access FDP and the Product from outside the UK, increasing the data security risk. |
| 13 | There is a risk that users will not have their permissions revoked when they leave their role/organisation. |

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

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

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

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

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

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

| Source Dataset | Statutory Authority for collection of Data | Statutory Authority for Processing & Analysis of Data | Statutory Authority for sharing of Data |
|---|---|---|---|
| Secondary Use Services+(Admitted Patient Care Episodes) | Spine services (no 2) 2014 Direction | NHS England De-Identified Data Analytics and Publication Directions 2023 | No Personal Data is shared. Aggregated Data may be shared under Health and Social Care Act 2012 s.261(5)(d) and s.13Z3 (e) and (f) |
| Emergency Care Dataset (ECDS) for urgent and emergency care | Emergency care Data set collection Directions 2017 | NHS England De-Identified Data Analytics and Publication Directions 2023 – NHS Digital | No Personal Data is shared. Aggregated Data may be shared under the Health and Social Care Act 2012 s.261(5)(d) and s.13Z3 (e) and (f) |
| A&E SitRep Data | Section 13E of the NHS Act 2006:<br>Securing continuous improvement in quality of services provided to individuals for or in connection with<br>a. the prevention, diagnosis or treatment of illness, or<br>b. the protection or improvement of public health | | |
| Met Office Weather Data | NA- Publicly available information | NA | NA |

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

**Article 6 – Personal Data**

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

**Article 9 – Special Category Personal Data**

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

**Common Law Duty of Confidentiality**

- **Legal obligation –** NHSE is required by law to process Confidential Patient Data it collects, Pseudonymises and analyses to create the Pseudonymised Data and the Aggregated Data input 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.

## 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.

Currently, the scope of the project is to infer aggregate level information (e.g. aggregate numbers of activity) NOT to infer specific information about an individual.

There is no risk to individuals from the data processed in the predictive tool as the tool will not be influencing any decisions about individual patient care. It is a capacity planning tool only. Conversely, it will positively benefit patient care through hospitals being able to more accurately predict demand and plan their services and resourcing accordingly.

The high-level uses of the FDP have been developed through consultation with stakeholders.

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

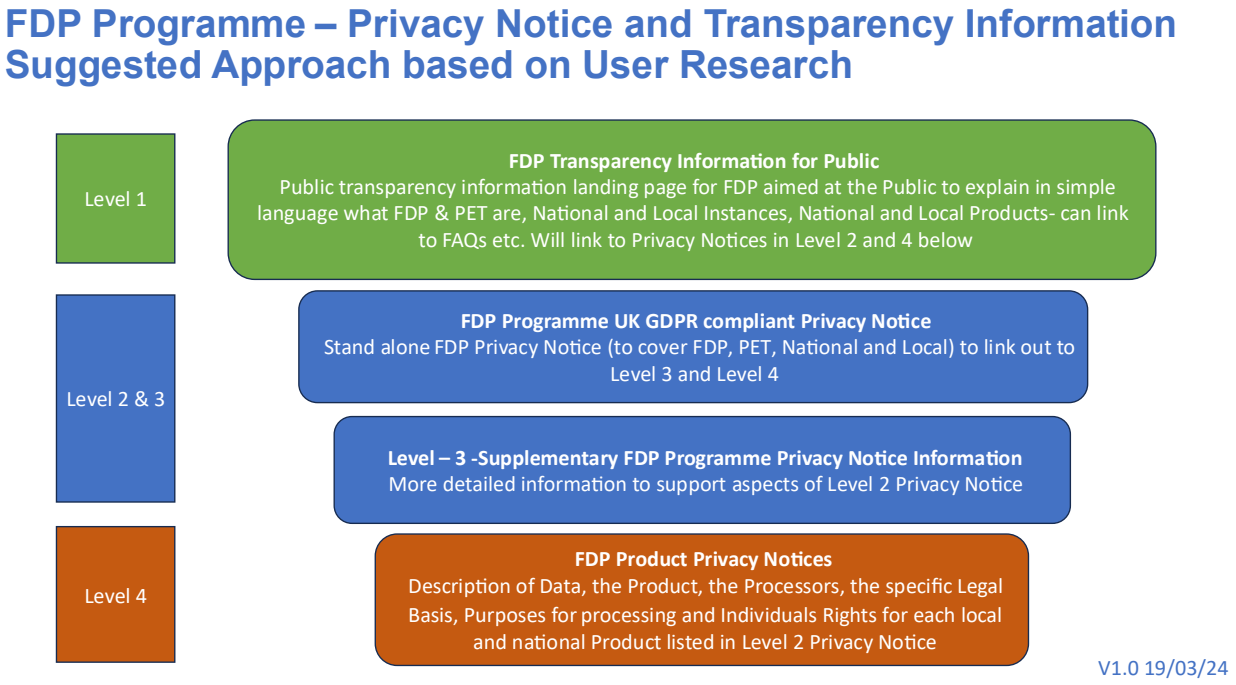
There is a range of information available on the NHS England website about FPD and how it works. This is Level 1 Transparency information.

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?

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

| **Data Categories** [*Information relating to the individual's*] | **Yes/No** | **Justify** *[there must be justification for Processing the Data items. Consider which items you could remove, without compromising the purpose for Processing]* |
|---|---|---|
| **Personal Data** | | |
| Name | No | |
| Address | No | |

| **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]* |
|---|---|---|
| Postcode | No | Within the ECDS the postcode has been derived to Middle Super Output which means that postcodes are aggregated to an average population of 6000 people or 2600 households, however this data is not used within the tool. |
| Date of Birth | No | |
| Age | Yes | Yes – to generate aggregate data at broad age groups e.g. 0-5, 6-17, 18-65, 65+, 75+. This is necessary for the tool as it informs operational planning decisions. |
| Sex | No | |
| 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 NHS number is included within the ECDS dataset however this is not processed or used within the tool |
| 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) | No | |
| Device MAC Address (Wireless Network Interface) | No | |
| *Spare – add Data item (as necessary)* | No | |
| *Spare – add Data item (as necessary)* | No | |
| **Special Category Data** | es/No | |
| Physical / Mental Health or Condition, Diagnosis/Treatment | No | |
| Sexual Life / Orientation | No | |
| Religion or Other Beliefs | No | |
| Racial / Ethnic Origin | No | |
| Biometric Data (Fingerprints / Facial Recognition) | No | |
| Genetic Data | No | |
| **Criminal Conviction Data** | | |
| Criminal convictions / alleged offences / outcomes / proceedings / sentences | No | |

Please see the detailed Dataset List below which identifies the source Datasets. The Data Specification with the list of data items is to be attached here:[ ]

| DATASET | GRANULARITY | SOURCE | USAGE |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **EMERGENCY CARE DATASET (ECDS) FOR URGENT AND EMERGENCY CARE** | Pseudonymised Data | NCDR | Used to generate aggregate admissions data for the model |
| **ADMITTED PATIENT CARE EPISODES (APCE)** | Pseudonymised Data | UDAL | Used to generate aggregate admissions data for the forecasting model |
| **ACCIDENT & EMERGENCY (A&E) SITREP** | Aggregated Data | NCDR | Used to generate aggregate admissions data for the forecasting model |
| **MET OFFICE WEATHER DATA** | Operational Data | MET Office | Used to account for effect of weather on A&E admissions |
| **NHS SITE ONTOLOGY DATASET** | Operational Data | FDP (Place Ontology) | Used to map sites to trusts |
| **NHS TRUST MERGER DATASET** | Operational Data | FDP (Place Ontology) | Used to keep track of trust mergers and adjust aggregations appropriately |
| **NHS TRUST ONTOLOGY DATASET** | Operational Data | FDP (Place Ontology) | Used to map trusts to ICSs and regions for aggregation |
| **1. SCHEMA_ANALYSIS_SEASONAL_AVERAGE RI.FOUNDRY.MAIN.DATASET.71E48B5C-7B38-4B0F-9691- 40BA82FDB585 2. WEATHER_FORECAST_RAW RI.FOUNDRY.MAIN.DATASET.93718B79-C94C-476B-802F-24A0CF471FC6 3. WEATHER_TIMESERIES_RAW** | Publicly available | | Used to assist in the analysis of A&E attendance |

| | | | |
|---|---|---|---|
| **RI.FOUNDRY.MAIN.DATASET.072E9890-7486-4E71-8B9F-C2AC04D5621F** | | | |

## 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 Data held on the Platform, and which is used in the Product. The Platform Contract has required Data Processing provisions in it which meet the requirements of UK GDPR. In addition, a separate Data Processing Annex providing specific Processing instructions to the Platform Contractor for this Product will be issued. A copy of this Data Processing Annex is attached here:

  AE Forecasting Tool - Annex - V1.0 Final

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

Only aggregate summary outputs are available to users via the dashboard in the Product

Small numbers are not suppressed in these outputs as the aggregation is done at age band level which ensures that the risk of re-identification is very low. Any further suppression would negatively impact the utility of the tool.

The categories of users who can view the dashboard are as follows:

- Senior operational planners at trust/ICS/ICB level
- System Control Centre leads
- Bed/site managers.
- Consultants and general managers across emergency care.
- NHS England national and regional operational and UEC teams

Access is granted by the Asset Owner through Role Based and Purpose Based Access Controls

## 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

Any inaccuracies in the underling data used in the Product are addressed through existing NHSE data collection quality assurance processes before the data flows through into FDP and the Product.

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

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

The following rights under UK GDPR apply to the Processing of Personal Data (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?

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

**Specific Access controls for the Accident and Emergency (A&E) Forecasting Tool**

Access to product in National Data Platform

- Access to the Product follows standard protocol Access - NHS National Data Platform via Multi Factor Authentication
- Access to the tool's aggregated outputs is at different tiered levels - system, region, and national

Access to Pseudonymised patient level datasets

- Only the developers of the tool have access to the Pseudonymised patient level datasets for the purpose of aggregating the data to be used in the tool. Users only have access to aggregated data via dashboard as shown in the data flow diagram in (2)
- The data processing pipeline generating aggregated datasets can only be changed by developers after a standard approval process requiring a review and approval by information governance colleagues and a senior member of the Data, Management and Integration Service (DMIS) team. Any changes to the Pseudonymised Data

processed to produce the Product would also require a change and re-approval of this DPIA.

The project controls will include:

- Regular quality assurance of outputs to ensure that forecasts are robust and statistically accurate
- Support for users in interpreting outcomes and understanding the drivers of analysis. This is done through engagements such as large demo sessions and smaller ad-hoc discussions with current and prospective users to help them take advantage of and understand the tool.

**Business Continuity Arrangements**

Should the FDP processing fail, the ability to undertake the processing using UDAL as a backup platform would be implemented.

The Product Owner and IAO will be required to approve user 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.

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 Processors on contracts with relevant security and data protection clauses contained within the agreements. Internal security and data protection processes are in place within NHS England.<br>2. No external users have access to Pseudonymised Data through the dashboards in the Product. All internal users are required to sign security operating procedures that confirm their responsibilities to protect Data. Internal users are also subject to contractual confidentiality requirements.<br>3. The download functionality of Data from the FDP is disabled by default, and access to this is controlled by the | Section 12 & 16 | Tolerate | Remote | Significant | Low |

| Risk No | Risk | Steps to mitigate the risk | DPIA section in which step is described | Effect on risk. Tolerate / Terminate / Treat / Transfer | Likelihood of harm Remote / Possible / Probable | Severity of harm Minimal / Significant / Severe | Residual risk None / Low / Medium / High |
|---|---|---|---|---|---|---|---|
| | | Product Owner which ensures appropriate governance in in place.<br>4. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Pseudonymised Data to only those with a legitimate need which in this case is limited to the developers of the Product (only 4 developers have access).<br>5. The FDP access audit logs ensure that all access is logged and can be fully audited. | | | | | |
| 2 | Pseudonymised Data may be processed beyond the appropriate retention period. | 1.Compliance with the Data Security Protection Toolkit (DSPT) requires Records Management policies to be in place.<br>2. The business area responsible for the Data have a Records Management Information Co-ordinator who will provide advice on how long Data should be retained at the point the dashboard is decommissioned.<br>3. See the FDP National Ontologies DPIA in relation to data in the Person Ontology. | Section 13 | 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 |
|---|---|---|---|---|---|---|---|
| 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.<br>2. Organisational measures are adhered to across the Data platform. Any breaches are reported in line with these.<br>3. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to Data. | Set out in the Overarching FDP DPIA and Section 12 & 16 above | Tolerate | Remote | Minimal | Low |
| 4 | Insufficient technical measures are in place to ensure appropriate security of the Personal Data (e.g. encryption, access controls) | 1. Data is encrypted in storage<br>2. All Data to and from the platform is encrypted in transit using at least TLS1.2<br>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 | 1. External suppliers are Processors on contracts with relevant security and data protection clauses contained within the agreements. Internal security and data protection processes are in place within NHS England.<br>2. Staff are trained and fully aware of their responsibilities when analysing | Set out in the Overarching FDP DPIA and Section 11, 12 & 16 above | Tolerate | Remote | Significant | Low |

| Risk No | Risk | Steps to mitigate the risk | DPIA section in which step is described | Effect on risk. Tolerate / Terminate / Treat / Transfer | Likelihood of harm Remote / Possible / Probable | Severity of harm Minimal / Significant / Severe | Residual risk None / Low / Medium / High |
|---|---|---|---|---|---|---|---|
| | individual people | 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<br>3. Contracts of employment and other organisational policies provide further safeguards against Data misuse<br>4. Specific Data Processing instructions are provided to the Platform Contractor which limits their Processing of the Pseudonymised Data to this Product, and which prohibits any reidentification<br>5. The download functionality of Data from the FDP is disabled by default, and access to this is controlled by the Product Owner which ensures appropriate governance in in place.<br>6. Only small number (4 currently) developers have access to the Pseudonymised Data in the Person Ontology | | | | | |
| 6 | Unsuppressed small numbers in Aggregated Data ingested into Product and/or made available via the | As the Aggregated Data ingested into the Product and made available via the Product dashboard has small numbers included, a risk assessment was undertaken to ascertain if the Data continue to be Personal Data. Whilst small numbers are included and shown | 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 |
|---|---|---|---|---|---|---|---|
| | Product dashboard could lead to the identification of an individual | they are aggregated in age bands and it is considered that the risk of re-identification to the users of the dashboard is low. The Data is therefore considered to be Aggregated Data which is Anonymous. | | | | | |
| 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.<br>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 | 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 | Sections 8 and 9 | 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 |
|---|---|---|---|---|---|---|---|
| | | to it from the General FDP Privacy Notice. | | | | | |
| 9 | 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.<br>2. The Data Processed to produce the Product has been Pseudonymised before being ingested into FDP.<br>3. Only small number of analysts (currently 4) responsible for developing the Product have access to the Pseudonymised Data. | Section 12 & 16 | Treat | Possible | Minimal | Low |
| 10 | The platform becomes inaccessible to users which could cause | 1. The FDP Contractor is required to have Business Continuity Plans in place.<br><br>2. The Product Owner has Business Continuity Plans in place which cover the inaccessibility/unavailability of the Product. | Section 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 |
|---|---|---|---|---|---|---|---|
| 11 | Inadequate data quality in source IT systems results in errors, inconsistencies and missing information that could compromise the integrity and reliability of the Data in the Product. | 1. The Product will only collect a sub-set of Personal Data from existing NHSE datasets. The Product will not collect Personal Data directly from individuals.<br><br>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 |
| 12 | Users will attempt to access FDP and the Product from outside the UK, increasing the data security risk. | 1. It is clearly articulated within the FDP IG Framework that no personal/patient data should leave or be accessible from outside of the UK without the express prior approval from the Data Governance Group.<br><br>2. It is within the Platform Contract that no access to the system should take place from outside the UK.<br><br>3. There are technical security measures in place to prevent access from outside the UK. | 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 |
|---|---|---|---|---|---|---|---|
| 13 | Users will not have their permissions revoked when they leave their role/ organisation and may continue to have access to Data they are no longer entitled to access | 1. As 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.<br><br>2. The Ontology Information Asset Owner is responsible for granting access to developers accessing the Pseudonymised Data in the Personal Ontology to create the Product and will review their access on any change in role.<br><br>3. Ongoing process for reviewing user access to dashboard to be confirmed. | 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 | [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. Update does not require DPO or SIRO approval. | 1, 3, 5, 10 & 14 | [redacted] | Prior to publication of the DPIA |
| 3 | Provide details of the process in place to review access to the Product and to remove access where users change role or leave the organisation | 14 | [redacted] | Prior to publication of the DPIA |
| 4 | Add Data Item Specification into Section 10 | N/A | [redacted] | Prior to publication of the DPIA |
| 5 | Add Annex into Section 11 | N/A | [redacted] | Prior to publication of the DPIA |

# 21.Completion and signatories

The completed DPIA should be submitted to the NHSE Privacy Transparency and Trust IG Team via england.pttigadvice@nhs.net (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:<br>• Directly Identifiable Personal Data<br>• Pseudonymised Data<br>• Anonymised Data,<br>• Aggregated Data<br>• Operational Data<br>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 |