Document filename:	**FDP Product Data Protection Impact Assessment** **Antimicrobial resistance (AMR) - Pseudonymised/De-identified Data**	
Directorate / Programme	**Medical Programmes Analytical Team**	
Document Reference *[insert IAR reference number]*	**IG2023174**	
Information Asset / Product Owner	[redacted]	Version 2.0
Author(s)	[redacted]	Version issue date 16/10/2024

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

Antimicrobial resistance (AMR) - Pseudonymised

Document Management

Revision History

Version	Date	Summary of Changes
0.1	18/03/2024	Minor updates for clarity.
0.2	20/03/2024	Updates made from external reviewers
0.3	21//03/2024	Creation of Final Draft for Approvals
0.4	01/04/2024	Creation of Clean Final Version
0.5	05/04/2024	Updated to reflect feedback
1.0	05/04/2024	Updated to reflect changes to template for consistency and final approval feedback.
1.1	16/10/2024	Updated to include access to aggregated Data by NAO
2.0	16/10/2024	Final updated document

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]			

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	Executive Director of Privacy & IG	05/04/2024	V0.5
[redacted]	[redacted]		

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 in relation to personal data, how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire

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 platform for which they are the data controller. Access for each platform will be governed and managed by each individual organisation.

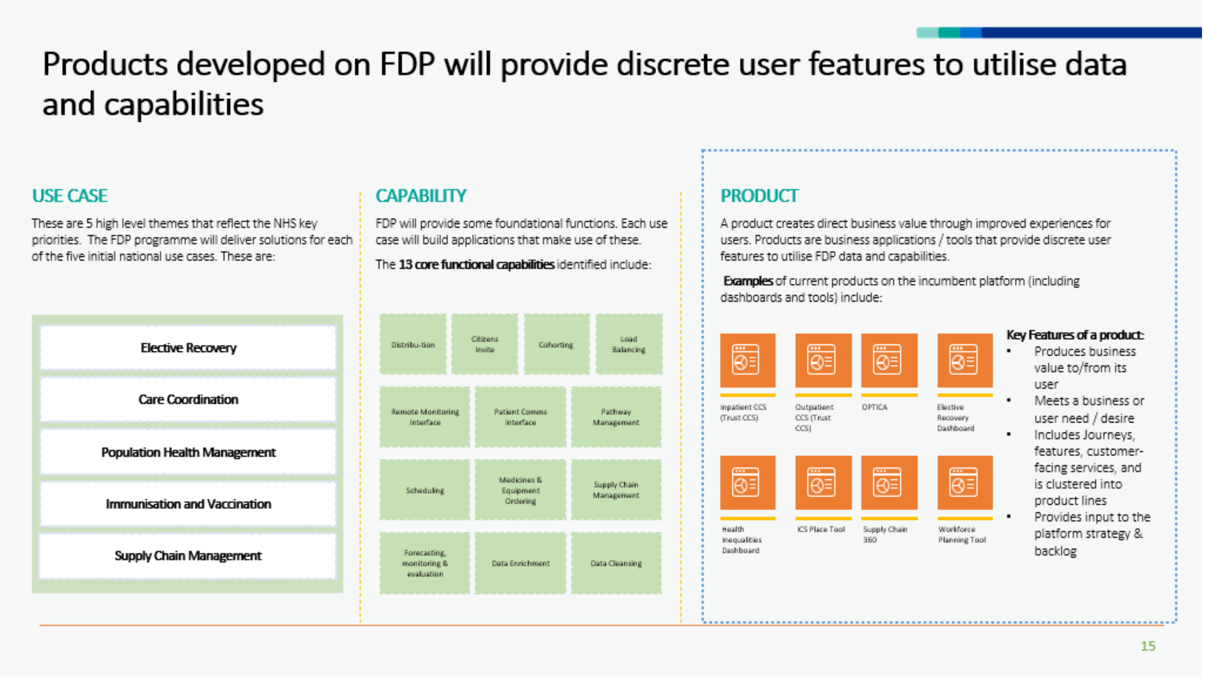
We want the NHS to be the best insight-driven health and care system in the world. This software will provide the foundation to improve the way that data is managed and used across the NHS in England to transform services and save lives.

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.



Products developed on FDP will provide discrete user features to utilise data and capabilities

USE CASE

These are 5 high level themes that reflect the NHS key priorities. The FDP programme will deliver solutions for each of the five initial national use cases. These are:

- Elective Recovery
- Care Coordination
- Population Health Management
- Immunisation and Vaccination
- Supply Chain Management

CAPABILITY

FDP will provide some foundational functions. Each use case will build applications that make use of these.

The **13 core functional capabilities** identified include:

- Distribu-tion
- Citizens Invite
- Cohorting
- Load Balancing
- Remote Monitoring Interface
- Patient Comms Interface
- Pathway Management
- Scheduling
- Medicines & Equipment Ordering
- Supply Chain Management
- Forecasting, monitoring & evaluation
- Data Enrichment
- Data Cleansing

PRODUCT

A product creates direct business value through improved experiences for users. Products are business applications / tools that provide discrete user features to utilise FDP data and capabilities.

Examples of current products on the incumbent platform (including dashboards and tools) include:

- Inpatient CCS (Trust CCS)
- Outpatient CCS (Trust CCS)
- OPTICA
- Elective Recovery Dashboard
- Health Inequalities Dashboard
- ICS Place Tool
- Supply Chain 360
- Workforce Planning Tool

Key Features of a product:

- Produces business value to/from its user
- Meets a business or user need / desire
- Includes Journeys, features, customer-facing services, and is clustered into product lines
- Provides input to the platform strategy & backlog

Key information about the Product

Purpose

The key objectives of the Product and associated dashboards are to:

- Provide a tool to enable monitoring of antimicrobial infection rates at local, regional and national level to benchmark and inform strategy development as recovery progresses
- Provide a tool to enable clinicians and pharmacists (primarily these are pharmacists in antimicrobial stewardship roles in trusts and ICBs) to view population health data in order to understand and improve outcomes as the NHS continues to deal with the recovery from the Covid pandemic
- Provide a means of linking data to support operational improvement, to better understand the causes of infection and optimal management across the NHS
- Provide a tool to enable the assessment of risk factors, to support improved decision making

16/10/2024 – Update to document.

The National Audit Office (NAO) are conducting a review into Antimicrobial Resistance and will be granted access to the dashboard. This access is to Aggregated Anonymised Data only.			
Local or National			
Local	☐	National	☒
Product falls under the following Use Cases			
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 in the Product			
Directly Identifiable Personal Data	☐		
Pseudonymised Personal Data	☒	Processed to create the Aggregated Data in the dashboard.	
Anonymised Data	☐		
Aggregated Data	☒	Displayed in the dashboard.	
Operational Data	☐		
Type of Data used in the Product			
No Personal Data	☐		

Personal Data	☒	Processed to create the Aggregated Data in the dashboard.
Special Category Personal Data	☒	Processed to create the Aggregated Data in the dashboard.

The product DPIAs describe:

- the purpose for the creation of the Product;
- the data which has been processed to create the Product;
- the supporting legal basis for the initial collection of that data;
- the legal basis which enables NHS England to pseudonymise the data for analysis purposes; and
- the data flows which support the creation of the product.

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.

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

The Antimicrobial Resistance dashboard falls under the Population Health Management use case in the Federated Data Platform (FDP). There have been several stages of stakeholder development underpinning the design and content of the AMR dashboard.

Firstly, in 2021 NHS England commissioned NHS Digital to undertake user research and collate requirements from a wide range of stakeholders, including users in national and regional roles, and from a range of professions including pharmacy, nursing, programme management and analytics.

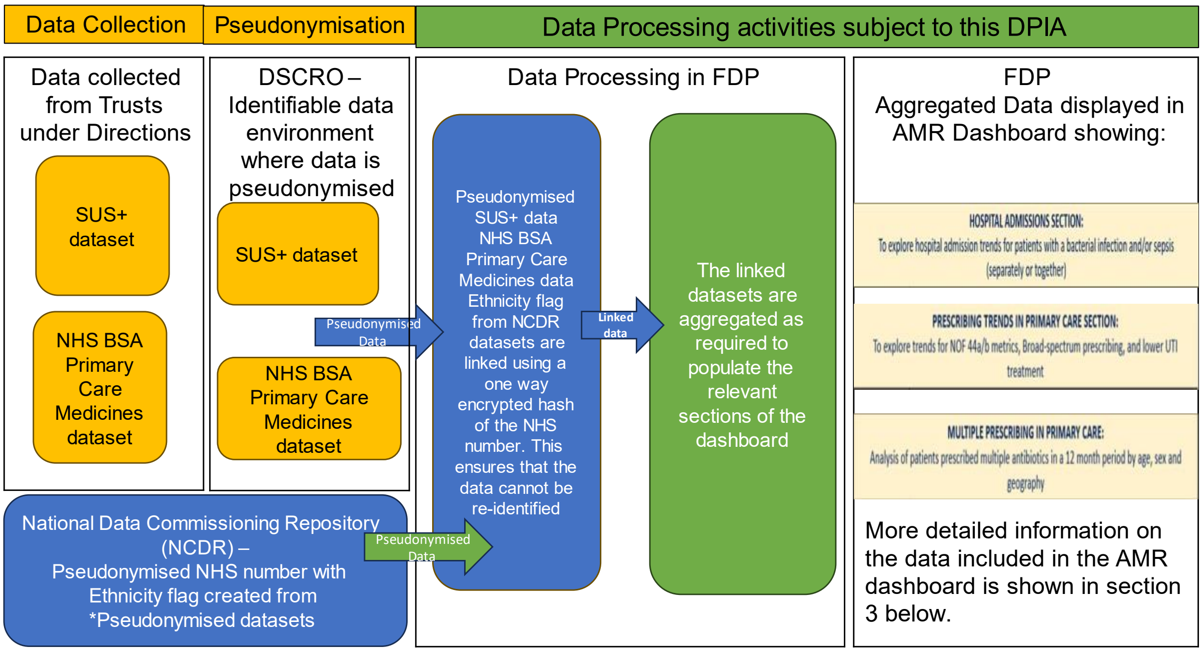
Requirements were assessed in terms of data availability; the vast majority were not possible using the data available in NHS England. Of the remaining requirements, prioritisation was undertaken, and initial requirements related to developing metrics focused on hospital admissions for bacterial infections and sepsis were progressed and initial visualisations in Foundry were created.

A governance group named the 'AMR Data and Dashboard Steering Group', comprising national and regional stakeholders across NHS England and the UK Health Security Agency (UKHSA), was set up to support oversight, direction, and decision-making in relation to the dashboard. This group agreed to the development of further visualisations in Foundry from the list of requirements – focused on primary care antibiotic prescribing and monitoring of the rates of resistance to antibiotics amongst key infections. To ensure the product was optimised for a wider range of users, working groups were convened entailing stakeholders and expected dashboard users working at national, regional, ICB and trust-level. These working groups met weekly and shaped the detail of the design of the dashboard and visualisations. More recently, user engagement work with colleagues working in AMR in national, regional, ICB and trust roles has been undertaken, focused on how the dashboard can be improved and optimised in the long term.

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.

2. Data Flow Diagram


Data Collection
Pseudonymisation
Data Processing activities subject to this DPIA
Data collected from Trusts under Directions
SUS+ dataset
NHS BSA Primary Care Medicines dataset
DSCRO – Identifiable data environment where data is pseudonymised
SUS+ dataset
NHS BSA Primary Care Medicines dataset
Pseudonymised Data
National Data Commissioning Repository (NCDR) – Pseudonymised NHS number with Ethnicity flag created from *Pseudonymised datasets
Pseudonymised Data
Data Processing in FDP
Pseudonymised SUS+ data NHS BSA Primary Care Medicines data Ethnicity flag from NCDR datasets are linked using a one way encrypted hash of the NHS number. This ensures that the data cannot be re-identified
Linked data
The linked datasets are aggregated as required to populate the relevant sections of the dashboard
FDP Aggregated Data displayed in AMR Dashboard showing:
HOSPITAL ADMISSIONS SECTION:
To explore hospital admission trends for patients with a bacterial infection and/or sepsis (separately or together)
PRESCRIBING TRENDS IN PRIMARY CARE SECTION:
To explore trends for NOF 44a/b metrics, Broad-spectrum prescribing, and lower UTI treatment
MULTIPLE PRESCRIBING IN PRIMARY CARE:
Analysis of patients prescribed multiple antibiotics in a 12 month period by age, sex and geography
More detailed information on the data included in the AMR dashboard is shown in section 3 below.

*Further details on the datasets which support creation of the Ethnicity flag are included in Section 5 below

3. Purpose of the processing

The key objectives of the Product and associated dashboards are to:

- Provide a tool to enable monitoring of antimicrobial resistance at local, regional and national level to benchmark and inform strategy development as recovery progresses
- Provide a tool to enable clinicians and pharmacists (primarily these are pharmacists in antimicrobial stewardship roles in trusts and ICBs) to view population health data in order to understand and improve outcomes as the NHS continues to deal with the recovery from the Covid pandemic

- Provide a means of linking data to support operational improvement, to better understand the causes of infection and optimal management across the NHS
- Provide a tool to enable the assessment of risk factors, to support improved decision making

The processing of the data to create the information displayed on the dashboard falls under the Population Health Management Use case for FDP which support the organisations capabilities for pathway management, as well as forecasting, monitoring and evaluation.

The King's Fund, in a paper co-authored by the former UK Chief Medical Officer[1], has set out that antimicrobials save lives and add on average 20 years to life expectancy across the globe. AMR is recognised as a key biological risk in the 2023 UK Biological Security Strategy. AMR is now captured as a chronic risk in the UK Government's National Risk Register - the same risk level as climate change and one of six chronic risks that directly impact human health.

The UK Government published the AMR National Action Plan (NAP) **'Confronting antimicrobial resistance 2024 to 2029'** in May 2024, replacing the previous 2019-24 NAP. The NAP was jointly developed by DHSC and DEFRA, working closely with NHSE, UKHSA and the devolved administrations. The NAP sets out the outcomes, targets and commitments to address the rising threat of AMR. NHS England has an agreed set of deliverables (key actions) to be achieved in support of these.

The National Medical Director is the SRO for NHS England's implementation of the NAP.

The core targets (to be achieved by 2029) within the NAP are:

- Target 1a: by 2029, we aim to prevent any increase in a specified set of drug-resistant infections in humans from the 2019 to 2020 financial year (FY) baseline
- Target 1b: by 2029, we aim to prevent any increase in Gram-negative bloodstream infections in humans from the 2019 to 2020 financial year baseline
- Target 2a: by 2029, we aim to increase UK public and healthcare professionals' knowledge on AMR by 10%, using 2018 and 2019 baselines, respectively.
- Target 4a: by 2029, we aim to reduce total antibiotic use in human populations by 5% from the 2019 baseline.
  Target 4b: by 2029, we aim to achieve 70% of total use of antibiotics from the Access category (new UK category) across the human healthcare system

The Data Workstream of the AMR Programme aims to underpin the wider NHSE AMR Programme, by enabling and/or providing timely access to reliable and representative data pertaining to monitoring, measuring and achieving the healthcare commitments and

[1] https://www.kingsfund.org.uk/insight-and-analysis/long-reads/nhs-if-antibiotics-stopped-working

targets set out in the 5 Year UK Government National Action Plan (NAP). It forms part of a portfolio of workstreams within delivery of the Human Health deliverables of the NAP, for which NHSE's National Medical Director is the Senior Responsible Officer.

As part of the 2019-2024 NAP, a commitment was made to design, stand-up, evolve and maintain an AMR centralised, secure data environment that houses the ability to present clear and informative data via an analytical dashboard to key AMR stakeholders. The dashboard will evolve over the coming years to provide relevant information to support delivery of the National Action Plan (NAP).

The scope of the Product is to process data for all patients who interact with community, primary and secondary care, to understand infections, prescribing and associated resistance.

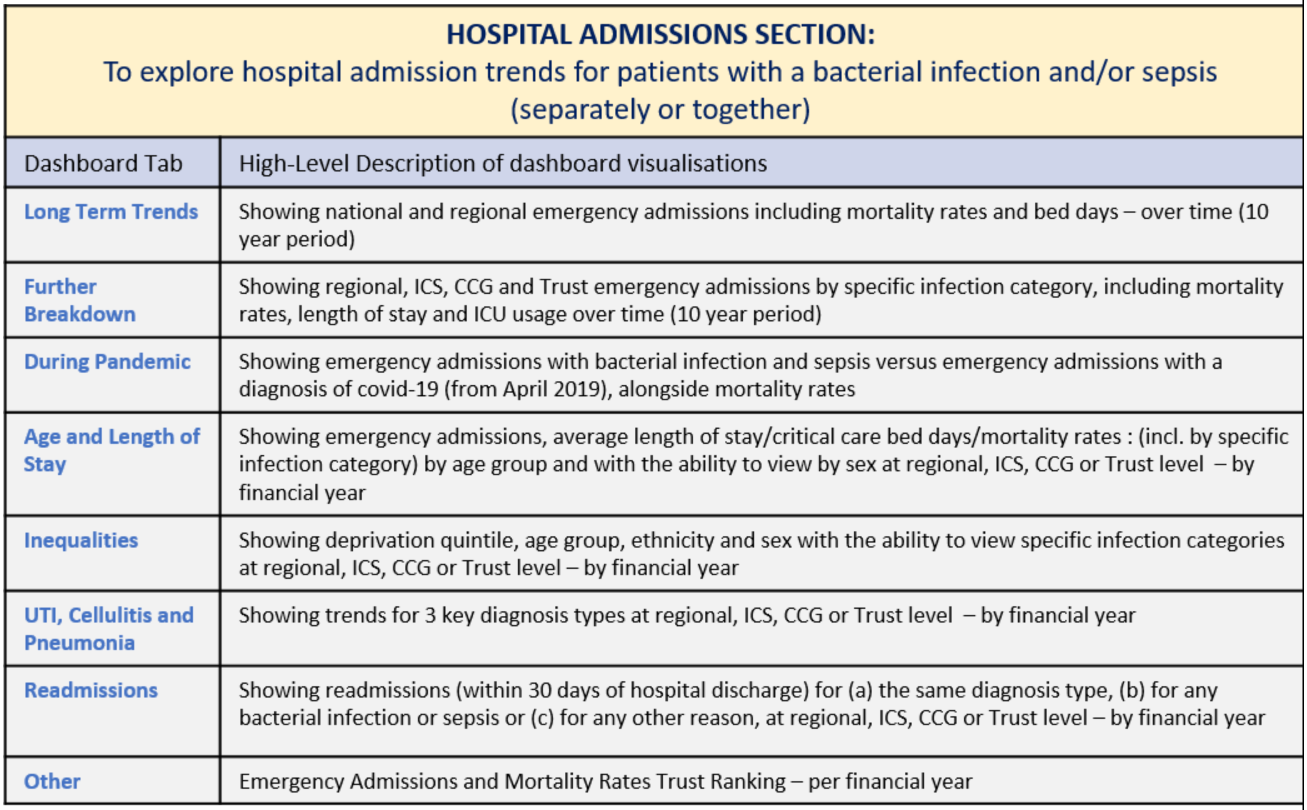
The aggregated dashboards will allow data to be viewed using the following geographical footprints (where applicable, based on dataset access controls):

- Primary Care Network (PCN)
- Integrated Care Board (ICB)
- Trusts
- Integrated Care System (ICS)
- NHSE Region and National level

National Audit Office (NAO)

Dashboard visualisations available to the listed permission-based users are shown in the tables below:

Table 1

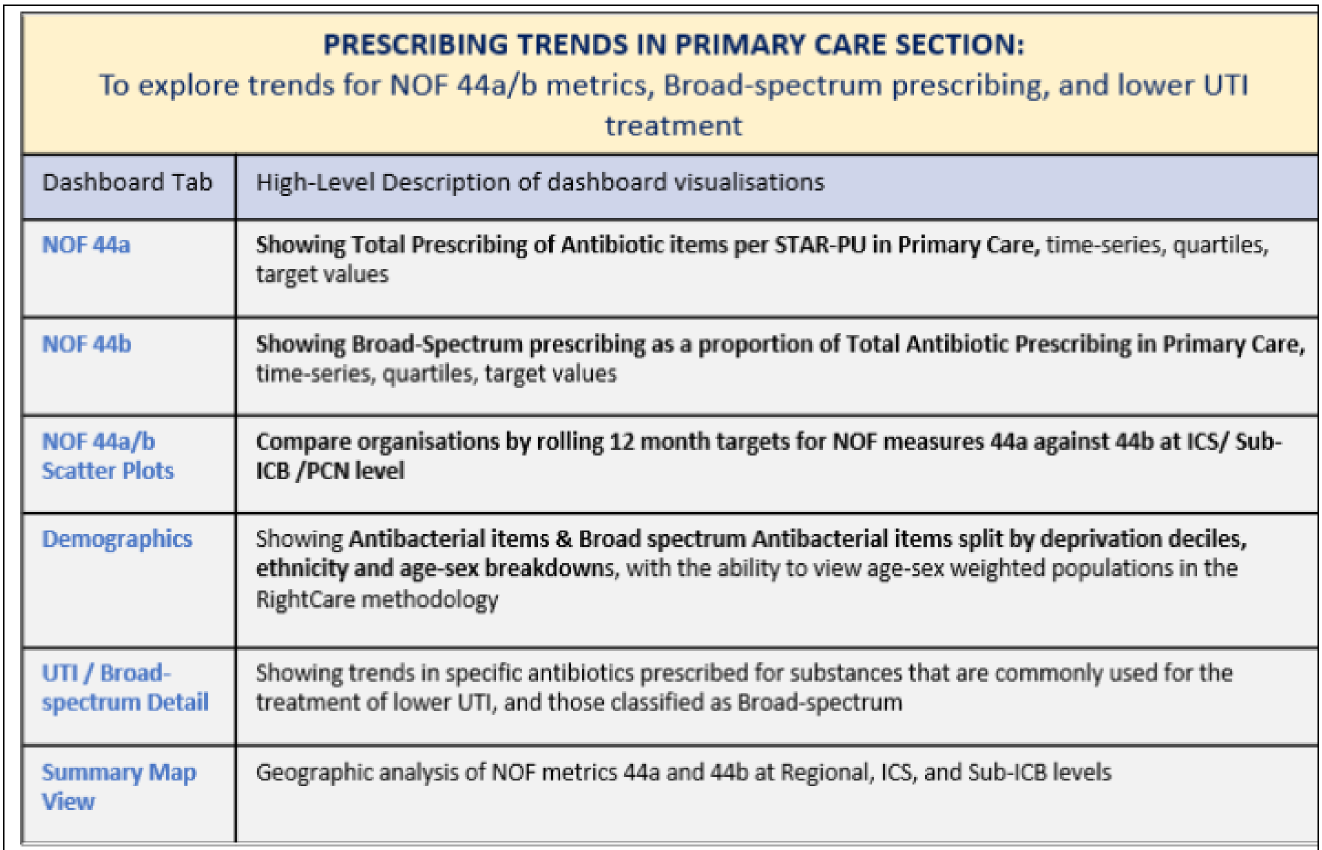


HOSPITAL ADMISSIONS SECTION:

To explore hospital admission trends for patients with a bacterial infection and/or sepsis (separately or together)

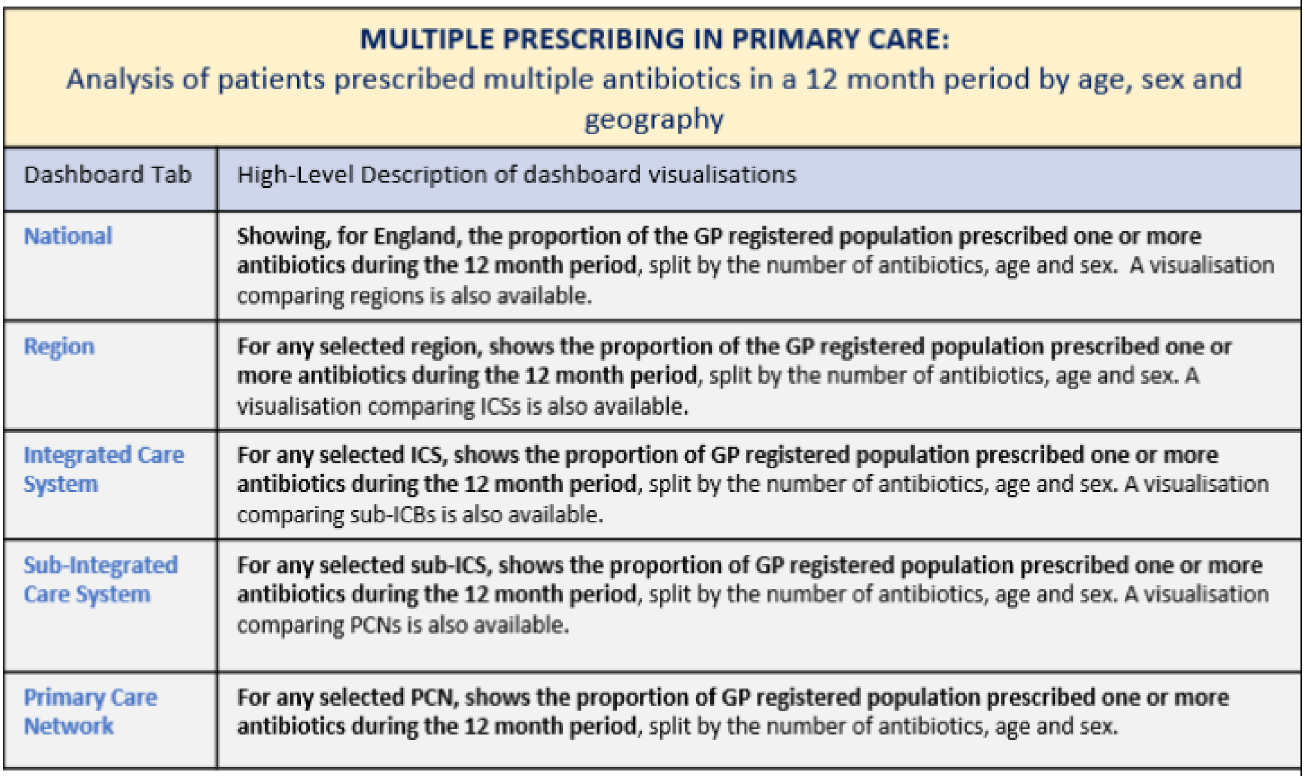
Dashboard Tab	High-Level Description of dashboard visualisations
Long Term Trends	Showing national and regional emergency admissions including mortality rates and bed days – over time (10 year period)
Further Breakdown	Showing regional, ICS, CCG and Trust emergency admissions by specific infection category, including mortality rates, length of stay and ICU usage over time (10 year period)
During Pandemic	Showing emergency admissions with bacterial infection and sepsis versus emergency admissions with a diagnosis of covid-19 (from April 2019), alongside mortality rates
Age and Length of Stay	Showing emergency admissions, average length of stay/critical care bed days/mortality rates : (incl. by specific infection category) by age group and with the ability to view by sex at regional, ICS, CCG or Trust level – by financial year
Inequalities	Showing deprivation quintile, age group, ethnicity and sex with the ability to view specific infection categories at regional, ICS, CCG or Trust level – by financial year
UTI, Cellulitis and Pneumonia	Showing trends for 3 key diagnosis types at regional, ICS, CCG or Trust level – by financial year
Readmissions	Showing readmissions (within 30 days of hospital discharge) for (a) the same diagnosis type, (b) for any bacterial infection or sepsis or (c) for any other reason, at regional, ICS, CCG or Trust level – by financial year
Other	Emergency Admissions and Mortality Rates Trust Ranking – per financial year

Tables 2/3



PRESCRIBING TRENDS IN PRIMARY CARE SECTION:
To explore trends for NOF 44a/b metrics, Broad-spectrum prescribing, and lower UTI treatment

Dashboard Tab	High-Level Description of dashboard visualisations
NOF 44a	**Showing Total Prescribing of Antibiotic items per STAR-PU in Primary Care,** time-series, quartiles, target values
NOF 44b	**Showing Broad-Spectrum prescribing as a proportion of Total Antibiotic Prescribing in Primary Care,** time-series, quartiles, target values
NOF 44a/b Scatter Plots	**Compare organisations by rolling 12 month targets for NOF measures 44a against 44b at ICS/ Sub-ICB /PCN level**
Demographics	Showing **Antibacterial items & Broad spectrum Antibacterial items split by deprivation deciles, ethnicity and age-sex breakdowns**, with the ability to view age-sex weighted populations in the RightCare methodology
UTI / Broad-spectrum Detail	Showing trends in specific antibiotics prescribed for substances that are commonly used for the treatment of lower UTI, and those classified as Broad-spectrum
Summary Map View	Geographic analysis of NOF metrics 44a and 44b at Regional, ICS, and Sub-ICB levels



MULTIPLE PRESCRIBING IN PRIMARY CARE:
Analysis of patients prescribed multiple antibiotics in a 12 month period by age, sex and geography

Dashboard Tab	High-Level Description of dashboard visualisations
National	**Showing, for England, the proportion of the GP registered population prescribed one or more antibiotics during the 12 month period**, split by the number of antibiotics, age and sex. A visualisation comparing regions is also available.
Region	**For any selected region, shows the proportion of the GP registered population prescribed one or more antibiotics during the 12 month period**, split by the number of antibiotics, age and sex. A visualisation comparing ICSs is also available.
Integrated Care System	**For any selected ICS, shows the proportion of GP registered population prescribed one or more antibiotics during the 12 month period**, split by the number of antibiotics, age and sex. A visualisation comparing sub-ICBs is also available.
Sub-Integrated Care System	**For any selected sub-ICS, shows the proportion of GP registered population prescribed one or more antibiotics during the 12 month period**, split by the number of antibiotics, age and sex. A visualisation comparing PCNs is also available.
Primary Care Network	**For any selected PCN, shows the proportion of GP registered population prescribed one or more antibiotics during the 12 month period**, split by the number of antibiotics, age and sex.

AMR Guidance Tab:
The dashboard also contains a guidance tab with general information about the content of each section of the dashboard. It also contains a change log and list of contents of the dashboard. It does not contain any data.

4. 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
1	There is a risk that pseudonymised data may be 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 manipulated in some way to re-identify individual people
6	There is a risk that unsuppressed small numbers in aggregated data (made available via the dashboard) could lead to the identification of an individual

5. Description of the Processing

The SUS+ and NHS BSA Primary Care Medicines Datasets are collected under Directions (as set out in the legal basis section below). These datasets have previously been pseudonymised within a secure DSCRO environment by NHS England to remove identifiers and derive/mask personal data items e.g. post code, date of birth. NHSE is required under the NHS England De-Identified Data Analytics and Publication Directions 2023 to pseudonymise data in order that it can be used for analytical purposes.

Ethnicity Flag - The following pseudonymised datasets held within the NHSE National Commissioning Data Repository are used to derive an ethnicity flag:

- Master Patient Index (a register containing demographic data for all patients registered with a GP Practice in England)
- Secondary Use Services Data (SUS)
- Assuring Transformation Data
- Maternity Data (MSDS)
- Community Data (CSDS)

- Mental Health Data
- Improving Access to Psychological Therapies (IAPT) Data and
- SLAM (Contract Monitoring Activity Data which is not personal data).

The derived ethnicity flag with Pseudonymised NHS number is linked with the SUS+ and NHS BSA Primary Care Medicines datasets to create the aggregated data for the AMR dashboards.

The patient-level Pseudonymised datasets, as detailed in the data flow diagram in section 2, are run through pipelines which aggregate the data and show it in the AMR dashboard as visualisations. The outputs of the dashboard are purely aggregate.

The dashboard will present Aggregated Data with small numbers to ensure that the system can monitor and respond accordingly to patients. Small numbers will be shown in the dashboard, as suppression would skew the capability of the data in respect of patient outcomes.

Whilst the Aggregated Data displayed in the dashboard does show small numbers, this data has been further aggregated by month and organisation and therefore it is considered there is no risk that an individual could be re-identified from the data or linked with other data which would enable re-identification.

The data will be made available via the dashboards, managed through Purpose Based Access Control (PBAC) to national, regional, and local analysts, in line with the platform access model, for analysis in line with the population health management use case.

Data Visualisation
The Product consists of a suite of dashboard visualisations providing Aggregated Data to users which is accessible via web-based interfaces as set out in Section 3 above.

6. Compliance with the Data Protection Principles

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

Data Protection Principle	Section addressed in this DPIA
Lawfulness, fairness and transparency	Section 7 (Lawfulness); Section 8 (Fairness); Section 9 (Transparency)
Purpose limitation	Section 3
Data minimisation	Section 10
Accuracy	Section 14
Storage limitation	Section 13
Integrity and confidentiality (security)	Section 16
Accountability	Accountability is addressed throughout the DPIA. In particular, section 21 includes approval of the residual risks by the Information Asset Owner.

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

Statutory authority *this is for national products only, please remove highlight or remove as necessary*

NHSE's various statutory authorities for collecting, processing, analysing and sharing personal 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 personal data
Secondary Use Services+	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 the Health and Social Care Act 2012 s.261(5)(d) and s.13Z3 (e) and (f)
NHS BSA Primary Care Medicines	NHS Business Services Authority (NHSBSA) Medicines Data Directions 2019	NHS England De-Identified Data Analytics and Publication Directions 2023	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)
The following pseudonymised datasets held within the NHSE National Commissioning Data Repository (NCDR) are used for this product - Master Patient Index, SUS, Assuring Transformation Data, Maternity Data (MSDS), Community Data (CSDS), Mental Health and Improving Access to Psychological Therapies (IAPT) Data Set These datasets are used to derive ethnicity by scanning each dataset to see where ethnicity has been	The datasets processed in the NCDR are collected under Directions from the Secretary of State for Health for NHSE purposes. The directions are above and: Primary care registration management Directions 2018 - NHS England Digital Assuring transformation data collection Directions 2015 - NHS England Digital	NHS England De-Identified Data Analytics and Publication Directions 2023	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)

recorded and then recording it against the pseudonymised NHS number.	Establishment of information systems for NHS Services: maternity services Directions 2018 - NHS England Digital Community Services Data Set Directions 2020 - NHS England Digital Mental health services Directions 2020 - NHS England Digital Improving Access to Psychological Therapies Directions 2021 - NHS England Digital		

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 aggregated 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 data disclosed via the dashboard is Anonymous Aggregated Data and is not Confidential Patient 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.

In terms of the people's expectations, information about the Antimicrobial Resistance Programme is already available on the NHS England website (NHS England » Antimicrobial resistance (AMR).

The Product has 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 care to individuals. The processing of this data will allow a stronger evidence base for change and improvement.

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 is Aggregated Data which is considered to be Anonymous.

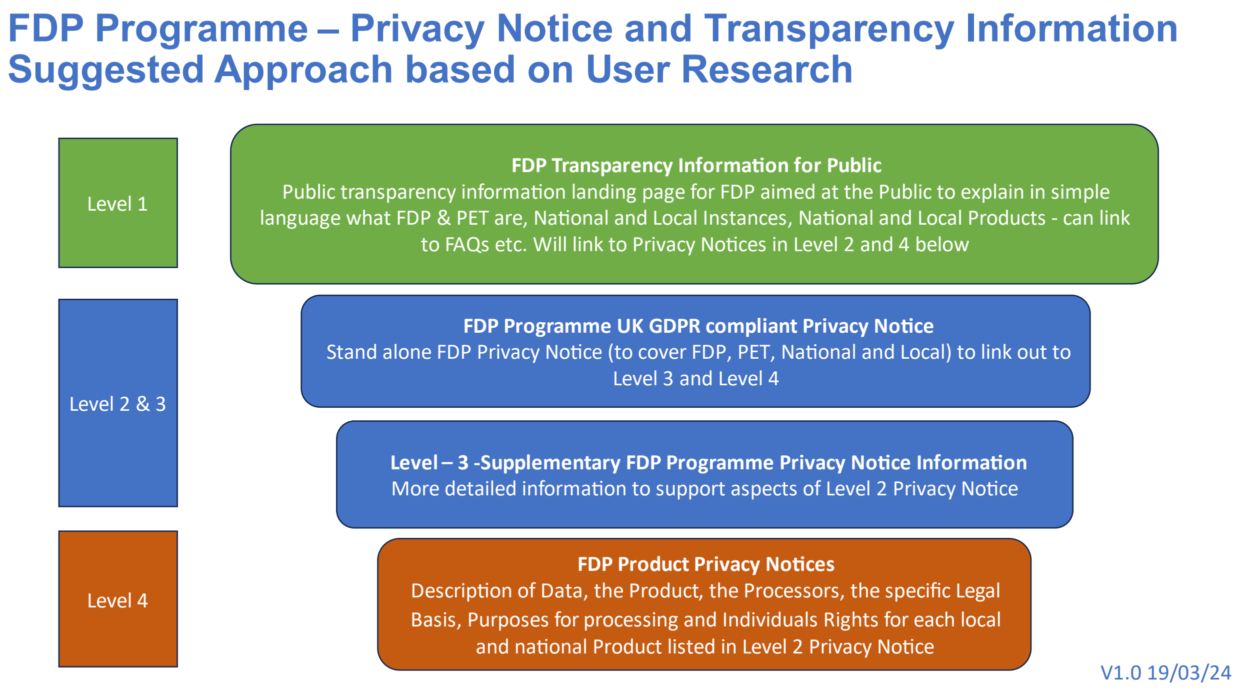
9.What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

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 will be 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 .



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

Level 1

FDP Transparency Information for Public
Public transparency information landing page for FDP aimed at the Public to explain in simple language what FDP & PET are, National and Local Instances, National and Local Products - can link to FAQs etc. Will link to Privacy Notices in Level 2 and 4 below

Level 2 & 3

FDP Programme UK GDPR compliant Privacy Notice
Stand alone FDP Privacy Notice (to cover FDP, PET, National and Local) to link out to Level 3 and Level 4

Level – 3 -Supplementary FDP Programme Privacy Notice Information
More detailed information to support aspects of Level 2 Privacy Notice

Level 4

FDP Product Privacy Notices
Description of Data, the Product, the Processors, the specific Legal Basis, Purposes for processing and Individuals Rights for each local and national Product listed in Level 2 Privacy Notice

V1.0 19/03/24

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 derived in the secure Identifiable Data processing environment(s) (DSCROs) before flowing into the pseudonymised data environments such as UDAL/NCDR/FDP.

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
Personal Data		
Name		
Address		

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		
Gender	Yes	To show demographic differences in metrics
Living Habits	Yes	Carer support indicator
Professional Training / Awards / Education		
Income / Financial / Tax situation / Financial affairs		
Email Address		
Physical Description		
General Identifier e.g. NHS No	Yes	Pseudonymised NHS number required for data linkage
Home Phone Number		
Online Identifier e.g. IP Address/Event Logs		
Website Cookies		
Mobile Phone / Device No / IMEI No		
Location Data (Travel / GPS / GSM Data)		
Device MAC Address (Wireless Network Interface)		
Banking information e.g. account number, sort code, card information		
Spare – add data item (as necessary)		
Spare – add data item (as necessary)		
Special Category Data		
Physical / Mental Health or Condition	Yes	Medical **diagnosis codes** and procedure codes associated with AMR conditions (Table 1 above) Pseudonymised prescribing information – no free text fields
Sexual Life / Orientation		
Religion or Other Beliefs		
Trade Union membership		
Racial / Ethnic Origin	Yes	To understand and reduce inequalities impacting patient care.
Biometric Data (Fingerprints / Facial Recognition)		
Genetic Data		
Criminal Conviction Data		
Criminal convictions / alleged offences / outcomes / proceedings / sentences		

Please see below Data Specification:

- Discharge Modelling and AMR Data Specification

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

In Pseudonymised form only, the NHS BSA primary care medicines dataset is linked to SUS+ dataset which then has an ethnicity flag added to the combined dataset. Please see the data specification embedded above.

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

Data is shared with a range of Dashboard Users. The data shared is Aggregated Data considered to be Anonymous.

Users of the Dashboard may include:

- NHS England national and regional AMR stakeholders
- UK Health Security Agency (UKHSA) National and Regional AMR stakeholders
- Department for Health and Social Care
- NHS Business Services Authority (NHS BSA)
- National Institute for Health and Care Excellence
- Commissioning Support Units supporting on work related to AMR
- Local Authorities
- Integrated Care Boards (ICBs)
- Public Health Collaboratives
- NHS Trusts
- Place-based partnerships
- Primary Care Networks (PCNs)
- Academic Health Science Networks (AHSNs) National Audit Office (NAO)

13.How long will the personal data be retained?

The data which is aggregated to create the AMR dashboards will be kept in line with business requirements in provision of the dashboard. At the point that the dashboard 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. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

NHS England is not collecting data directly from individuals.

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

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 within this Product:

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

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

***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 sets out the technical and organisational controls for the platform.

Specific Access controls for the AMR Dashboard

[redacted]

Following this, an SQL account will be created which the application will use to read/write the database for certain task(s). This will restrict unwarranted access.

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 SUS+, NHS BSA Primary Medicines and ethnicity data within the AMR purpose of FDP in order to manage the required dashboard aggregate-level visualisations for the users.

[redacted] The product owner and IAO can approve the access based on the Purpose Based Access Controls in place for the AMR data, and are able to delegate this to other members of the Medical Programmes Analytical Team or the AMR programme team to ensure adequate cover and that access requests can be processed in a timely manner.

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

All processing of Personal 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 dashboard 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 through the dashboard, which only provides access to Anonymous Aggregated Data.

Type 1 Opt Outs do not apply because the datasets used to create the dashboard do not contain confidential patient information that has been collected by NHS England from GP Practices.

19.Risk mitigations and residual risks

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

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

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

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
1	Pseudonymised data may be 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	Section 16	Tolerate	Remote	Minimal	Low

Risk No	**Risk**	**Steps to mitigate the risk**	**DPIA section in which step is described**	**Effect on risk** Tolerate / Terminate / Treat / Transfer	**Likelihood of harm** Remote / Possible / Probable	**Severity of harm** Minimal / Significant / Severe	**Residual risk** None / Low / Medium / High
		relevant FDP User which ensures appropriate governance in in place. 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 advice on how long data should be retained at the point the dashboard is decommissioned.	Section 13	Tolerate	Remote	Minimal	Low
3	Insufficient organisational measures are in place to ensure appropriate security of the pseudonymised data (e.g. policies, procedures, disciplinary controls)	1.Appropriate organisation measures in relation to data controls and governance are in place to ensure the security of the data. 2. Organisational measures are adhered to across the data platform. Any breaches are reported in line with these. 3. Role Based Access Controls and Purpose Based Access Controls are in place to limit access to data.	Set out in the Overarching FDP DPA and Section 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 DPA and Section 16 above	Tolerate	Remote	Minimal	Low
5	Data that has had identifiers removed could be manipulated in some way to re-identify individual people	1. Access to NHS Data which has been pseudonymised remains in control of the NHS in line with contractual arrangements 2. Staff are trained and fully aware of their responsibilities when analysing data to only use the minimum required for their purpose and that it is a criminal offence under the DPA 2018 to knowingly re-identify an individual 3. Contracts of employment and other organisational policies provide further safeguards against data misuse 4. Specific data processing instructions are provided to the Platform Contractor which limits their processing of the Pseudonymised Data to this Product and which prohibits any reidentification	Set out in the Overarching FDP DPA and Section 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
6	There is a risk that unsuppressed small numbers in Aggregated Data (made available via the dashboard) could lead to the identification of an individual	As the Aggregated Data displayed in the dashboard has small numbers included, a risk assessment was undertaken to ascertain if the data continues to be Personal Data. Whilst small numbers are shown, they have been further aggregated at month and organisational level and therefore it would not be possible to re-identify an individual in the data or for the output to be linked with other data which would enable re-identification to the users of the dashboard. The data is therefore considered to be Aggregated Data which is Anonymous.	Section 5	Tolerate	Remote	Minimal	None

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, including who will authorise analyst access and user dashboard access. Update does not require DPO or SIRO approval.	1 & 3	[redacted]	End of April 2024

21.Completion and signatories

The completed DPIA should be submitted to the PTT 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 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 PRIVACY, TRANSPARENCY AND TRUST AND OFFICE OF THE DPO USE ONLY

22. Summary of high residual risks

Risk no.	High residual risk summary

Summary of DPO (Data Protection Officer) advice:

Name	
Signature	
Date	
Advice	

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 may 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), 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.
Commissioned Health Service Organisations	Means organisations who provide health services in England pursuant to arrangements made with an NHS Body exercising functions in connection with the provision of such services.
Common Law Duty of Confidentiality	The common law duty which arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
Confidential Patient Data	Information about a patient which has been provided in circumstances where it is reasonable to expect that the information will be held in confidence, including Confidential Patient Information.
Confidential Patient Information	Has the meaning given in section 251(10) and (11) of the NHS Act 2006. See Appendix 6 of the National Data Opt Out Operational Policy Guidance for more information[1]
Contract Documentation	The Platform Contract, the NHS-PET Contract, the MoU and the DPAs
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 Loss Incident	Means any event that results, or may result, in unauthorised access to Personal Data held by the FDP Contractor under the Contractual Documentation, and/or actual or potential loss and/or destruction of Personal Data in breach of the Contractual Documentation, including any Personal Data Breach
Data Platform	The NHS Federated Data Platform
Data Processing Agreement	The form of data processing agreement to be entered into between each of the FDP Contractors and an ICB, an NHS Trust or another NHS Body in the form as required by the Platform Contract, the NHS-PET Contract and the MoUs.
Data Processing Schedule	The schedule containing Processing instructions in the form set out in the Data Processing Agreement.
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
Data Security and Protection Toolkit (DSPT)	The Data Security and Protection Toolkit is an online self-assessment tool that FDP User Organisations are required to complete annually to demonstrate they are meeting required data protection and security standards;
Direct Care	A clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care[2].
Directly Identifiable Personal Data	Personal Data that can directly identify an individual.
DPA(s)	Data Processing Agreements between each of the FDP User Organisations and each of the FDP Contractors in the form required under the Platform Contract, the NHS-PET Contract, and the MoU
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
FDP Data Principles	Means the principles set out in Part 2 of Schedule 3 (FDP Data Principles)
FDP Incident Management Protocol	Means an incident management protocol to be agreed between the FDP Contractors, NHS England and FDP User Organisations and approved by the Data Governance Group
FDP IG Audit and Assurance Framework	Means a document setting out the types of assurance reviews and audits that should be carried out by FDP User Organisations, including frequency, reporting and follow up actions, to assure compliance with the MoU and this IG Framework Document
FDP Programme	The NHS England Programme responsible for the procurement and implementation of the FDP across the NHS
FDP Specialist External IG Advisory Group	The advisory group established by NHS England to provide specialist IG advice to the FDP Programme which includes membership from external organisations including the Office of the

	National Data Guardian and the Information Commissioner's Office
FDP User Organisations	NHS England, ICBs, NHS Trusts and other NHS Bodies (including a Commissioned Health Service Organisation) who wish to have an Instance of the 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
IG Documentation	The information governance documentation referred to in Section 7 (Information Governance Documentation)
IG Framework Document, or Document	Means this IG framework document
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
Joint Controller	Has the meaning given in UK GDPR, being where two or more Controllers jointly determine the purposes and means of Processing Personal Data
Joint Controller Arrangement	Has the meaning given in UK GDPR being an arrangement between two or more Joint Controllers who shall in a transparent manner determine their respective responsibilities for compliance with the obligations under UKGDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of UKGDPR and reflecting the respective roles and relationships of the Joint Controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject
Local FDP User Organisation	An FDP User Organisation other than NHS England
Machine Data	AWS monitoring data and logs of engineering activity e.g. environment stand up
MoU	The Memorandum of Understanding signed between NHS England and an NHS Trust, ICB or other NHS Body as may be amended from time to time in accordance with its terms
National Data Opt Out	The Department of Health and Social Care's policy on the National Data Opt Out which applies to the use and disclosure of Confidential Patient Information for purposes beyond individual care across the health and adult social care system in England. See the National Data Opt Out Overview[3] and Operational Policy Guidance for more information[4]
Near Miss	Means circumstances in which a Personal Data Breach could have occurred
NHS Body	Has the meaning given in the NHS Act 2006
NHS FDP System IG Group	The user group established by NHS England for local IG leads to discuss and agree IG documentation for the initial and the subsequent deployment of other local Products
NHS-PET 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 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.
Parties	NHS England, the Platform Contractor, the NHS-PET Contractor, and FDP User Organisations
Personal Data	Has the meaning given in UK GDPR being any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . For the purposes of this IG Framework Document 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. A list of approved Products is set out in Part 2 of Schedule 2
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
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
Security Breach	Is a breach of security, and includes in the case of the Platform Contractor, a Breach of Security as defined in Schedule 2.4 (Security Management) of the Platform Contract
Special Category Personal Data	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.
User Organisation System	FDP User Organisation IT systems from which source information is obtained that is Processed within the Data Platform and NHS-PET
User Organisation System Contractor	Third party contractors providing User Organisation Systems to FDP User Organisations as their Processor
UK GDPR	UK GDPR as defined in and read in accordance with the Data Protection Act 2018