SCHEDULE 2.1

SERVICES DESCRIPTION

Services Description

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

Adoption the services required to support Product implementation and integration into a User's Tenancy including business process development, stakeholder liaison, ways of working and change management, Product implementation, End User training and technical support and service desk integration and training, Product rollout and go live, transition and early support services;

Early Adopter an NHS Body which is a user of Legacy Products as of the Effective Date or is otherwise identified as such in the Implementation SOW

Legacy Products the products described in the Inventory supported by the Authority's national data platform in use prior to the Effective Date;

PET Integration the integration of the Data Platform with PET in accordance with the PET Requirements;

PET Integration Pattern a template for PET Integration applicable and maintainable consistently across Tenants;

Source Systems The Authority Systems required for the availability of the canonical data model including relevant patient administration systems, staff rostering and scheduling systems and NHS England's UDAL system;

Tenant Deployment On the basis of a Tenant Pattern, the making available to a User of their Tenancy of the Data Platform; the availability of the canonical data model within that Tenancy; integration to Source Systems of that Tenancy; the User's local service desk being trained in the onboarding of End Users, the setting up of PBAC and PBAC's configuration for Transition Products;

the Tenancy supporting PET Integration and the availability of the Core Capabilities;

Tenant Pattern a template for the deployment of a Tenancy to a User consistently applied across all Users;

Transition Product A Product established on the Data Platform based on migrating, rewriting transition or refactoring of a Legacy Product; and

User Access Model this is type of access control model which defines and structures how End Users will be provided access to applications and data within the Data Platform.

2 INTRODUCTION

2.1 This Schedule sets out the Services to be provided by the Supplier.

2.2 The Supplier will provide Services meeting the Authority Requirements, including as described in paragraph 3 and, where applicable, as set out in the Appendices to this Schedule.

3 SERVICES DESCRIPTION

3.1 The Implementation Services are Services relating to Mobilisation and Platform Enablement and the Transition Services, provided in accordance with the Implementation Plan.

3.2 Transition Services are Services relating to the Transition to be executed and completed in accordance with the Data Platform Requirements in tab “01 – Business Requirements" of Appendix 1B (*Single Requirements Catalogue*) to Schedule 2.1 (*Services Description*).

3.3 The Operational Services are Services provided on or after the Go Live Date including Data Platform Services other than Optional Services.

3.4 The Data Platform Services are Services comprising the provision of the Data Platform including the provision of compute, storage and associated infrastructure services enabling User and End User access to the Data Platform Services.

3.5 Training is Services provided to train End Users in the use of the Data Platform as described in the Authority Requirements.

3.6 The Optional Services are Services which are to be provided by the Supplier if required by the Authority in accordance with Clauses 5.13 to 5.16 (*Optional Services*) and a Statement of Work, including in relation to a Use Case.

3.7 The Supplier will deliver the social value commitments set out in Schedule 2.9 (*Social Value Commitments*).

3.8 The Supplier will perform the Services as further described in Appendix 3 (*Additional Supplier's Responsibilities*) to this Schedule.

4 IMPLEMENTATION SERVICES

4.1 The Implementation Services include completion of the Implementation Phases so that the Implementation Milestones are Achieved.

4.2 The Implementation Phases are:

(i) Mobilisation being the Supplier's commencement of activity preparatory to the remainder of Implementation Service delivery and the Implementation Milestones and the Supplier's provision (and Authority's Acceptance) of the Deliverables for Mobilisation as set out in the Implementation SoW;

(ii) Platform Enablement being

- the performance of Implementation Services such that:

  a) the Data Platform is established and ready for live use, including by Early Adopters;

  b) the Core Capabilities are complete, deployed and ready to use within the Data Platform; and

  c) the Supplier's provision (and Authority's Acceptance) of the Deliverables for Platform Enablement as set out in the Implementation SoW

- The Data Platform otherwise meets the Data Platform Requirements;

- The Data Platform supports the canonical data model and Tenant Patterns;

- The Supplier has developed an agreed approach to

  a) the Adoption of the Data Platform by the Early Adopters; and

  b) the PET Integration Pattern.

(iii) Transition (which may be split into two or more phases) being the Adoption of the Data Platform by the Early Adopters, the deployment of a Tenant to each Early Adopter in accordance with the Tenant Pattern, the availability of Transition Products replacing Legacy Products on the Data Platform, and the Supplier's provision (and Authority's Acceptance) of the Deliverables for Transition as set out in the Implementation SoW.

4.3 The Implementation Milestones are set out in the Implementation SoW.

5 DATA CONNECTORS

5.1 The Authority Requirements for Data Connectors include:

Requirement summary	**Reference to specific Requirement(s)**
Component and SDK-based integration using open APIs	[REQ-2.4.6.0.1], [REQ-2.1.2.1.1], [REQ-2.1.1.2.3], [REQ-2.7.2.0.12], [REQ-2.7.2.0.4], [REQ-2.7.2.0.4] and [REQ-2.7.1.0.7] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
Standardised integration service components and support of NHSE's UDAL data service	[REQ-2.1.1.6.5], [REQ-F93FB2], [REQ-0584EE], [REQ-2.5.9.0.1], [REQ-E8124D] and [REQ-2.5.13.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
API integrations following industry standard patterns (Rest API services, HL7/FHIR and supporting the OAuth 2.0 protocol)	[REQ-2.1.1.2.5] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
No point-to-point connections between Platform Applications and Data Platform storage layers	[REQ-2.6.3.0.2], [REQ-2.1.5.2.2], [REQ-2.4.10.0.2], [REQ-2.4.10.0.3], [REQ-2.3.11.0.1], [REQ-491EF3], [REQ-E4436B], [REQ-9198FC], [REQ-2.6.3.0.4], [REQ-E4436B], [REQ-2.4.9.0.2], [REQ-2.3.11.0.1], [REQ-2.1.5.2.1], [REQ-2.3.11.0.3] in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*)

5.2 Additionally the Authority requires that:

(a) Data Connectors are built on open APIs or standardised components generally available, subject to paragraph 5.2 (b);

(b) Where the connection mode described in paragraph 5.2(a) is not available, Data Connectors will not be direct interfaces to Third Party Systems using non-standard interfaces, but will use standard interfaces to connect to additional components operating to mask any underlying complexity of Third Party System data presentation (by using a *façade pattern* model) *so* that the Data Platform uses only standard interfaces (such component a **Connector Component**); and

(c) Where Data Connectors or Connector Components are created by Supplier for the purposes of this Agreement, they constitute Specially Written Software.

Appendices to Schedule 2.1

1 **Data Platform Requirements:**

1A. **Core Capabilities**

1B. **Single Requirements Catalogue**

2 **Accessibility Requirements**

3 **Additional Supplier's Responsibilities**

Appendix 1A- Data Platform Requirements: Core Capabilities

No.	Core Capability	Reference to specific Requirement(s)
1.	**Distribution** - Enabling platform services (Platform Applications) to be created by third parties and distributed to users	[REQ-2.3.1.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
2.	**Citizens Invite** - Identify and communicate with patients/citizens eligible for clinical programmes such as vaccination and population health programmes	[REQ-2.3.4.0.1], [REQ-2907A5], [REQ-8E02B0], [REQ-E696A5], [REQ-149DB3], [REQ-91D416], [REQ-B71CE2], [REQ-681982], [REQ-826396] and [REQ-61AC28] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
3.	**Cohorting** - Ability to identify cohorts of participants from a flexible set of rules and pass these cohorts through to other applications	[REQ-2.3.2.0.1], [REQ-3B45D3], [REQ-7DBFD2], [REQ-D02A45], [REQ-D9D851], [REQ-CF34D7], [REQ-A5D8CE], [REQ-20C323], [REQ-D989C4], [REQ-017CB0], [REQ-F8B762], [REQ-C15FB8], [REQ-175D3C], [REQ-C04137], [REQ-16216A], [REQ-BDE279], [REQ-96BBFD], [REQ-D16004], [REQ-5DE54C], [REQ-CCAD61], [REQ-9BFF3B] and [REQ-9FDCD0] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
4.	**Load Balancing** - To manage demand and operational capacity across services to better utilise system resources and meet clinical and patient needs	[REQ-2.3.5.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
5.	**Patient Comms Interface** - Designed to help improve patient communication to be more efficient at each touch point of a patient journey	[REQ-2.3.4.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
6.	**Pathway Management** - Provide a single view of patients on a particular pathway and the tasks needed to move through the pathway	[REQ-2.3.6.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)

No.	Core Capability	Reference to specific Requirement(s)
7.	**Remote monitoring interface** - To provide a remote monitoring service whereby clinicians can view and monitor a patient's clinical need	[REQ-2.3.7.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
8.	**Scheduling** - System to support scheduling of patients into clinical capacity in areas such as operating theatres, diagnostic scanners, outpatient clinics, community clinics	[REQ-2.3.8.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
9.	**Medicines and equipment ordering** - To allow end-to-end order management system to centralise the ordering, stock check and release of nationally procured medicines, e.g., vaccines	[REQ-2.3.10.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
10.	**Supply Chain Management** - To standardise inventory, procurement and stock allocation	[REQ-2.3.9.0.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
11.	**Forecasting, Monitoring and Evaluation** - Enrich existing datasets with additional data as it is acquired to analyse and inform decision making	This Core Capability is related to ability to add new information to existing datasets; aggregate views of data to allow greater visibility of requirements trends; ability to visualise complex data in an accessible manner; use of advanced analytics systems to classify and process data and produce tailored data sets depending on the requirements of the user; strategic planning tool that enables the ability to forecast and allow scenario planning; enable a dynamic process that organisations can update and input into regularly; allow the monitoring of patient outcomes; and provision of actuarial modelling around changes to the population and its health
12.	**Data Cleansing** - Cleansing of data to ensure one version of the truth Cleansing of data to ensure one version of the truth across the NHS	[REQ-2.1.3.3.1] in Appendix 1B (*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)
13.	**Data Enrichment** - The ability to enrich	[REQ-2.1.1.6.1] and [REQ-2.1.4.2.1] in Appendix 1B

No.	Core Capability	Reference to specific Requirement(s)
	existing datasets with additional data as it is acquired to analyse and inform decision making across multiple services	(*Single Requirements* Catalogue) to this Schedule 2.1 (*Services Description*)

Appendix 1B – Single Requirements Catalogue

Annexed as separate document.

Appendix 2 – Accessibility Requirements

The following accessibility requirements apply to the Data Platform

1 **ACCESSIBILITY PRINCIPLES**

1.0 The following UK guidelines and legislation shall apply to this Appendix:

(a) Web Content Accessibility Guidelines (WCAG 2.1 AA) as referenced in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*), and (from the WCAG Update Date, as defined in Paragraph 2.1(b) of this Appendix 2) WCAG 2.2 AA;

(b) Public Sector Bodies (Websites and Mobile Applications) (No 2) Accessibility Guidelines Regulations 2018;

(c) The Equality Act 2010; and

(d) Accessibility guidance[1] for product and delivery, user research, content, design, development and testing.

1.1 The Data Platform is intended to be used by as many people as possible.

1.2 The Data Platform must be available to persons with access difficulties and be able to support accessibility solutions, as set out in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*).

1.3 The content and designs are sufficiently clear and simple so that they can be used without the need to adapt.

1.4 The following four core accessibility principles shall apply in line with WCAG 2.1 AA:

(a) Perceivable;

(b) Operable;

(c) Understandable; and

(d) Robust.

2 **ACCESSIBILITY STANDARDS**

2.1 The Supplier shall comply with the following accessibility standards and/or obligations:

[1] https://service-manual.nhs.uk/accessibility

(a) Publish an accessibility statement and only declare ‘disproportionate burden’ where all other avenues have been explored;

(b) Where feasible, meet all WCAG 2.1 requirements (or, from the WCAG Update Date (as defined in this Paragraph (b) of this Appendix 2) the requirements of WCAG 2.2) to AA standard. In respect of WCAG 2.2, the Supplier shall conduct an assessment of the Services against the WCAG 2.2 guidelines during 2024 to identify any non-compliance. The Supplier, acting reasonably and in good faith, will agree a date with the Authority by which the Supplier will address any outstanding non-compliant issues (such date not to be later than 31 December 2024) ("**WCAG Update Date**"). Where meeting the WCAG 2.1 or WCAG 2.2 requirements is not feasible or is not able to be accommodated within the scope of the Data Platform Charges, Supplier will provide full details to Authority (by identifying the problem, the mitigation, timeline for review, assistive technology which may be required by the End User) in the accessibility statement;

(c) Facilitate capabilities to be built to the accessibility standards for all analytics, including, but not limited to reports, applications, workflow management and dashboards, as set out in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*);

(d) Meet responsive design principles for platform applications and make accessible via a web-interface as set out in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*);

(e) Support direct User access to the system through the internet using a web browser, secure managed desktops (VDIs e.g. Citrix, Amazon AppStream) and also through APIs. The screens must use responsive/mobile-friendly technology so that they can be clearly presented on tablets and other devices, as set out in Appendix 1B (*Single Requirements Catalogue*) to this Schedule 2.1 (*Services Description*);

(f) Ensure that all buttons, icons, images, filters, tables, search bars, input fields have the correct HTML semantic markup elements or ARIA (Accessible Rich Internet Applications) attributes to enable reading by assistive technology;

(g) where feasible and able to be accommodated within the scope of Data Platform Charges, ensure the site can be read by the Authority's ‘in-house’ assistive technology: ‘Read & Write’ and ‘Dragon Software’;

(h) Provide alternative data formats, for example, ‘Convert to Table for Data Charts’; provide Bar Charts as opposed to Line charts;

(i) Adhere to the Authority's colour palettes (which have been accessibility tested). This includes chart palettes, organisation colour palettes etc.; and

(j) Make reasonable adjustments when required.

Appendix 3 – Additional Supplier's Responsibilities

Supplier's Responsibilities in Relation to Canonical Data Model

1. The Supplier shall be responsible for developing and maintaining the Data Platform canonical data model (**CDM**) for use across the national, local, and integrated care board (**ICB**) Tenants. The CDM contains standard definitions, metadata, and relationships for data entities, events, and fields which may be relevant for use across the Data Platform Tenants.
2. The Supplier will work with the Authority to define the Authority's Data Platform data schema and governance process for the creation of new data sets and modifications to existing data sets. Once agreed this process would govern the process of maintaining the Data Platform CDM.
3. The Authority's Data Platform Ontologies are responsible for ensuring that ingested datasets are consistent, comprehensive, and reliable for further use in Products (applications) and ad-hoc analysis. The Ontology ensures that ingested datasets are joined and transformed where appropriate and comply with the CDM to result in one version of the truth that is validated and can be relied upon by End Users.
4. There are many Ontologies within the Authority's Data Platform that are used for national and local Products. The Supplier shall ensure that the Ontologies it deploys across local Tenants must be consistent to ensure scalability of Products. These are grouped into areas related to the type of data being ingested.
5. The Supplier shall produce a guidance document that outlines the best practices to be followed to develop and maintain the CDM for the Data Platform during Mobilisation, as per the Implementation SoW.

Authority's Best Practices for Organising and Processing Data in Data Platform

National Tenant

1. The Supplier and the Authority will collaborate and agree on consistent design standards and patterns during Mobilisation. Once agreed, the Supplier shall build and maintain all datasets, pipelines, and applications in a consistent manner in accordance with these design standards and patterns.
2. The Supplier and the Authority shall work together to update and refine these best practices during Mobilisation.

Local Tenant (Trust and Integrated Care System)

1. The Supplier and the Authority shall work together to define the best practices for organising and processing data in local Tenants in the Data Platform during Mobilisation.
2. It is critical that applications across all local tenants use a consistent and shared the CDM and contain localisation to the CDM only where necessary.

Data Flows

1. The Supplier and the Authority will collaborate to agree on system capability to support information governance processes within the Authority and its organisations to enable data flow between Tenants (national, Trust, and ICB).

2. The Supplier shall ensure that the Data Platform provides system approval processes for the relevant data flows in the system including initial ingestion of data into any Tenant and any sharing of data between Tenants.
3. The Supplier shall collaborate with the PET Supplier and the Authority to define roles and responsibilities to align with the information governance requirements.

Data Platform Onboarding Documentation

1. The Supplier shall develop and maintain comprehensive and accessible onboarding documentation to ensure that the Authority and any other third party supplier is able to effectively:
    a. access, navigate, and use the Data Platform technically;
    b. create new Products;
    c. update existing Products;
    d. understand and make updates to the CDM; and
    e. understand and make updates to the Ontologies.
2. The Supplier shall work with the Authority to define and document best practices in relation to the following activities:
    a. Process to ingest new data (with integration to PET);
    b. Technical setup to ingest new data and finding existing data;
    c. Project structure and security (How to request access?);
    d. Engineering best practices;
    e. End User facing style guides and accessibility requirements;
    f. Platform training for onboarding new developers;
    g. Re-deployment services across tenancies; and
    h. Data egress / flow approach between organisations (with integration to PET).
3. The Authority will provide input to the Supplier to support the Supplier in defining and documenting the best practices as set out above.

User Access Model

1. The Supplier shall be responsible for collaborating with the Authority to design and document a User Access Model to manage End User groups, markings, roles, and folder structures for national, trust, and ICB Tenants.
2. The Supplier's provision of the User Access Model must ensure that End Users will only have access to the applications and data that they require for their role.
3. The Supplier shall be responsible for ensuring that there is consistency in the design and implementation of the User Access Model, for it to be effectively implemented and reported upon across all Tenants.
4. The Supplier will collaboratively scope Data Platform capability to fulfil the Authority's audit and reporting requirements for the User Access Model.
5. The detailed User Access Model will be documented by the Supplier during the Mobilisation phase of the delivery plan and implemented as part of Platform Enablement.
6. The Supplier must also document how identity and access management will work for the Data Platform, according to the Authority's chosen external identity and access management solution.

Attached document

Inventory

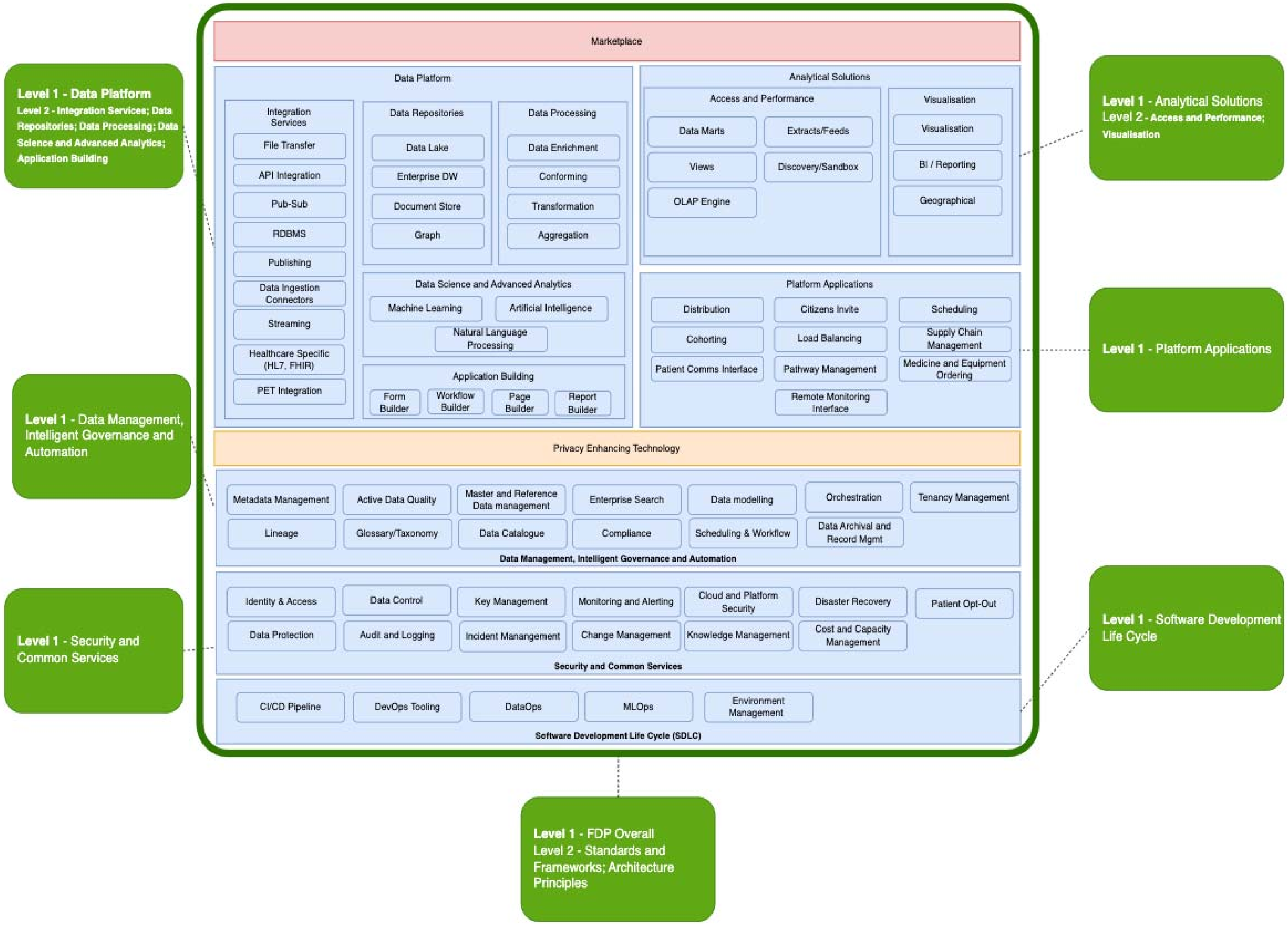
[Redacted under FOIA s43, Commercial interests]

01 - Business Requirements

This tab catalogues the business requirements. These requirements are organised around the three levels as defined in the technical capability model shown below.

02 - Platform Requirements

This tab catalogues the platform requirements. These requirements are organised around the three levels as defined in the technical capability model shown below.



Level 1 - Data Platform
Level 2 - Integration Services; Data Repositories; Data Processing; Data Science and Advanced Analytics; Application Building

Level 1 - Data Management, Intelligent Governance and Automation

Level 1 - Security and Common Services

Level 1 - Analytical Solutions
Level 2 - **Access and Performance; Visualisation**

Level 1 - Platform Applications

Level 1 - Software Development Life Cycle

Level 1 - FDP Overall
Level 2 - Standards and Frameworks; Architecture Principles

Marketplace

Data Platform

Integration Services
- File Transfer
- API Integration
- Pub-Sub
- RDBMS
- Publishing
- Data Ingestion Connectors
- Streaming
- Healthcare Specific (HL7, FHIR)
- PET Integration

Data Repositories
- Data Lake
- Enterprise DW
- Document Store
- Graph

Data Processing
- Data Enrichment
- Conforming
- Transformation
- Aggregation

Data Science and Advanced Analytics
- Machine Learning
- Artificial Intelligence
- Natural Language Processing

Application Building
- Form Builder
- Workflow Builder
- Page Builder
- Report Builder

Analytical Solutions

Access and Performance
- Data Marts
- Extracts/Feeds
- Views
- Discovery/Sandbox
- OLAP Engine

Visualisation
- Visualisation
- BI / Reporting
- Geographical

Platform Applications
- Distribution
- Citizens Invite
- Scheduling
- Cohorting
- Load Balancing
- Supply Chain Management
- Patient Comms Interface
- Pathway Management
- Medicine and Equipment Ordering
- Remote Monitoring Interface

Privacy Enhancing Technology

- Metadata Management
- Active Data Quality
- Master and Reference Data management
- Enterprise Search
- Data modelling
- Orchestration
- Tenancy Management
- Lineage
- Glossary/Taxonomy
- Data Catalogue
- Compliance
- Scheduling & Workflow
- Data Archival and Record Mgmt

Data Management, Intelligent Governance and Automation

- Identity & Access
- Data Control
- Key Management
- Monitoring and Alerting
- Cloud and Platform Security
- Disaster Recovery
- Patient Opt-Out
- Data Protection
- Audit and Logging
- Incident Manangement
- Change Management
- Knowledge Management
- Cost and Capacity Management

Security and Common Services

- CI/CD Pipeline
- DevOps Tooling
- DataOps
- MLOps
- Environment Management

Software Development Life Cycle (SDLC)

03 - IG Requirements

This tab catalogues the Information Governance requirements

04 - Security Requirements

This tab catalogues the security requirements.

05 - WoW Requirements

This tab catalogues the Ways of Working requirements.

Status	Review

Row Labels	**Sum of UUID**
Data Management, Inteligent Governance and Aut	**6**
Data Archival and Record Management	**2**
n/a	2
Enterprise Search	**2**
n/a	2
Tenancy Management	**2**
n/a	2
Data Platform	**4**
Data Repositories	**2**
Graph	2
Integration Services	**2**
Data Ingestion Connectors	2
FDP Overall	**8**
Standards and Frameworks	**8**
n/a	8
SDLC	**2**
DevOps Security Tools	**2**
n/a	2
Security and Common Services	**24**
Audit and Logging	**4**
n/a	4
Change Management	**2**
n/a	2
Cost and Capacity Management	**6**
n/a	6
Disaster Recovery	**2**
n/a	2
Identify and Access	**2**
n/a	2
Incident Management	**2**
n/a	2
Key Management	**2**
n/a	2
Knowledge Management	**2**
n/a	2
Monitoring and Alerting	**2**
n/a	2
Grand Total	**44**

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-2907A5]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Use existing campaign strategy templates	Citizen Invite
[REQ-8E02B0]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Test their citizen invite before sending out	Citizen Invite
[REQ-E696A5]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Set and define KPIs for a campaign strategy to measure uptake	Citizen Invite
[REQ-149DB3]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Save their campaigns before sending out	Citizen Invite
[REQ-91D416]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Define channels of SMS, Email, Digital and physical letters)	Citizen Invite
[REQ-B71CE2]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Define a set of reminders, triggers and events	Citizen Invite
[REQ-681982]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Create communications for a sub-cohort (and filter within the main cohort)	Citizen Invite
[REQ-826396]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Create campaign strategies	Citizen Invite
[REQ-61AC28]	To-be	Other Products	Citizen Invite	The user must be able to create and submit communications campaigns for their approved cohorts	Create a workflow	Citizen Invite
[REQ-3B45D3]	To-be	Other Products	Cohorting	The User must be able to address inequalities in vaccine uptake between groups	View health inequalities within a geographical areas, including national view	Cohorting
[REQ-7DBFD2]	To-be	Other Products	Cohorting	The User must be able to address inequalities in vaccine uptake between groups	Develop visual representations to enable gaps in vaccine uptake	Cohorting
[REQ-D02A45]	To-be	Other Products	Cohorting	The User must be able to address inequalities in vaccine uptake between groups	Benchmark uptake by cohort	Cohorting
[REQ-D9D851]	To-be	Other Products	Cohorting	The User must be able to address inequalities in vaccine uptake between groups	Analyse data by cohort group	Cohorting
[REQ-CF34D7]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	View IG information belonging to that cohort before submitting	Cohorting
[REQ-A5D8CE]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	Save the cohort	Cohorting
[REQ-20C323]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	Preview the cohort before submitted	Cohorting

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-D989C4]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	Filter on the cohort	Cohorting
[REQ-017CB0]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	Create new cohorts	Cohorting
[REQ-F8B762]	To-be	Other Products	Cohorting	The user must be able to create and submit a cohort for approval	Amend cohort criteria	Cohorting
[REQ-C15FB8]	To-be	Other Products	Cohorting	The user must be able to receive information from a citizen or carer within the cohort to confirm suitability and validation of information	Send information to the citizen via channels of SMS, Email, Digital and physical letters)	Cohorting
[REQ-175D3C]	To-be	Other Products	Cohorting	The user must be able to receive information from a citizen or carer within the cohort to confirm suitability and validation of information	Capture whether the information of the citizen is correct or not	Cohorting
[REQ-C04137]	To-be	Other Products	Cohorting	The user must be able to receive information from a citizen or carer within the cohort to confirm suitability and validation of information	Capture whether the citizen requires a pre-assessment or not	Cohorting
[REQ-16216A]	To-be	Other Products	Cohorting	The user must be able to review cohorts	Track and review cohorts	Cohorting
[REQ-BDE279]	To-be	Other Products	Cohorting	The user must be able to review cohorts	Send notifications for approvals	Cohorting
[REQ-96BBFD]	To-be	Other Products	Cohorting	The user must be able to review cohorts	Review IG information belonging to that cohort	Cohorting
[REQ-D16004]	To-be	Other Products	Cohorting	The user must be able to review cohorts	Review cohorts	Cohorting
[REQ-5DE54C]	To-be	Other Products	Cohorting	The user must be able view which of their citizens are in the cohort	View the cohort definition and rules	Cohorting
[REQ-CCAD61]	To-be	Other Products	Cohorting	The user must be able view which of their citizens are in the cohort	View cohort reasoning definitions (for inclusion and exclusion of the cohort)	Cohorting
[REQ-9BFF3B]	To-be	Other Products	Cohorting	The user must be able view which of their citizens are in the cohort	Set and view eligibility	Cohorting
[REQ-9FDCD0]	To-be	Other Products	Cohorting	The user must be able view which of their citizens are in the cohort	Create a workflow to process the citizens	Cohorting
[REQ-E57EC1]	To-be	Other Products	OPTICA	The user must be able to drill down into the Discharge Status for a patient	View Status Type & Status	Discharges
[REQ-8FA94A]	To-be	Other Products	OPTICA	The user must be able to drill down into the Discharge task list for a patient	View Task Stage, Status, Assignee Group, Assignee Detail	Discharges
[REQ-91BB90]	To-be	Other Products	OPTICA	The user must be able to drill down into the Patient Overview	View Whether the patient is in domcare/residential care, direct payment, Individual Service Funds)	Discharges
[REQ-18001D]	To-be	Other Products	OPTICA	The user must be able to drill down into the Patient Overview	View Name, DOB, Provider name, Hours of support/volume of service, Funding (can only tell us if person is part-funded)	Discharges
[REQ-01DE83]	To-be	Other Products	OPTICA	The user must be able to receive alerts displaying priority of tasks	Receive alerts displaying priority of tasks	Discharges

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-CCD348]	To-be	Other Products	OPTICA	The user must be able to report on Patients Discharged by Cumulative Days Delay	Report on Patients Discharged by Cumulative Days Delay	Discharges
[REQ-97007E]	To-be	Other Products	OPTICA	The user must be able to track all discharge tasks and patient status, showing all previous events timelines	Track all discharge tasks and patient status, showing all previous events timelines	Discharges
[REQ-25890A]	To-be	Other Products	OPTICA	The user must have the ability to view patient level information for all Admitted patients	Name, DOB, Admission date, ward, specialty, meets criteria to reside, discharge destination, discharge pathway, estimated discharge date, planned discharge date, site, location authority	Discharges
[REQ-BD936B]	To-be	Other Products	OPTICA	The user must have the ability to view patient level information for all Discharged patients	Name, DOB, Admission date, admission method, admission status, admission type, discharge date, discharge destination, discharge pathway, number of days delay	Discharges
[REQ-40953A]	To-be	Other Products	OPTICA	The user must have the ability to view patient level information on Criteria to Reside	View Planned Discharge Destination, Discharge Date, Discharge Date Confirmed	Discharges
[REQ-1B1EEA]	To-be	Other Products	OPTICA	The user must have the ability to view patient level information on Criteria to Reside	View Latest Checklist Task	Discharges
[REQ-97A9E7]	To-be	Other Products	OPTICA	The user must have the ability to view patient level information on Criteria to Reside	Name, DOB, Admission date, discharge pathway, criteria to reside, ward	Discharges
[REQ-0CCC1E]	Transition	Key Products	111	The User must be able to view ambulance information in real time	View the availability of operational performance on a real time basis	Elective Recovery
[REQ-36965A]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Understand where pressures are building across UEC systems, in particular hospital handover times and where acute sites are under pressure, targeting support conversations to those most in need	Elective Recovery
[REQ-FA7B25]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Understand call volumes and stacking to support discussion around mutual aid and buddy arrangements	Elective Recovery
[REQ-FAAE7A]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Report additional data such as proportion of vehicles, current performance metrics to provide additional context on national basis	Elective Recovery
[REQ-F48110]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Monitor the demand	Elective Recovery
[REQ-C62C1A]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Indicate if services are accurately resourced to meet demand	Elective Recovery

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-C40AA0]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Have multiple views for different types of users	Elective Recovery
[REQ-198AC3]	Transition	Key Products	111	The User must be able to view ambulance information in real time	Estimate the number of log ins per year	Elective Recovery
[REQ-2BB626]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View trends in the data	Vaccines
[REQ-6636F9]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View the total bed capacity	Vaccines
[REQ-5D7513]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View the most at risk trusts	Vaccines
[REQ-3160D9]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View oxygen therapy beds occupied by patients with COVID	Vaccines
[REQ-57F5C1]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View mechanical ventilator beds occupied by patients with COVID	Vaccines
[REQ-0692D9]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View forecasts of estimated daily COVID admissions	Vaccines
[REQ-21C43A]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View forecasts of all bed occupied by patients with COVID	Vaccines
[REQ-157DE5]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View data at a week on week level but also a 3 month level	Vaccines
[REQ-E6F770]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View bed metrics, including non covid bed metrics	Vaccines
[REQ-198281]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	View % of capacity required for patients with COVID	Vaccines
[REQ-7FCD7E]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	Identify missing data	Vaccines
[REQ-266B02]	Transition	Key Products	Early Warning System	The User must be able to make operational decisions	Be grouped by Trust, STP or Region	Vaccines
[REQ-D6F4E2]	Transition	Key Products	Early Warning System	The User must be able to prepare for expected patients with COVID 19	Forecast the expected number of estimated daily COVID admissions	Vaccines
[REQ-4F655D]	Transition	Key Products	Early Warning System	The User must be able to prepare for expected patients with COVID 19	Forecast all beds occupied by patients with COVID	Vaccines
[REQ-DB6613]	Transition	Key Products	Early Warning System	The User must be able to prepare for expected patients with COVID 19	Forecast oxygen therapy beds occupied by patients with COVID	Vaccines
[REQ-A3C753]	Transition	Key Products	Early Warning System	The User must be able to prepare for expected patients with COVID 19	Forecast mechanical ventilator beds occupied by patients with COVID	Vaccines
[REQ-272605]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View what drives the forecasts	Vaccines
[REQ-354513]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View time series for different data sources	Vaccines
[REQ-762456]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View the impact of each data source on the forecast	Vaccines
[REQ-04234C]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View the impact of data sources that are no longer used as N/A	Vaccines
[REQ-8B0184]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View leading indicators information	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-4FBB93]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View forecasts for different regions	Vaccines
[REQ-F4CA1C]	Transition	Key Products	Early Warning System	The User must be able to understand and interpret forecasts	View 'About' forecast explanations	Vaccines
[REQ-F25035]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View the time period the model performance results are based on	Vaccines
[REQ-15FB62]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View the exact number % of points fell within the confidence zone	Vaccines
[REQ-2D4E2A]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View model performance for all metrics	Vaccines
[REQ-AE001B]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View forecast options at Trust and Regional levels	Vaccines
[REQ-57D6E3]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View data for multiple dates at once	Vaccines
[REQ-0DFAA6]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	View data for any days in the past 6 weeks	Vaccines
[REQ-6B6097]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	Validate the model statistically	Vaccines
[REQ-56E198]	Transition	Key Products	Early Warning System	The User must be able to view how forecasts have changed over time	Differentiate when the model did not have access to data when making the forecasts	Vaccines
[REQ-AB21C7]	Transition	Key Products	Early Warning System	The User must be able to view Trust metrics	View high level metrics for Trusts	Vaccines
[REQ-0F2416]	Transition	Key Products	Early Warning System	The User must be able to view Trust metrics	View forecasts for specific Trusts	Vaccines
[REQ-F3ED2E]	Transition	Key Products	Exec Dashboard	The User must be able to view a high level series of dashboards which provide up-to-date information across the NHS	View each area by selecting a Programme Area and deep-dive into data from that area	Elective Recovery
[REQ-3114CA]	Transition	Key Products	Exec Dashboard	The User must be able to view a high level series of dashboards which provide up-to-date information across the NHS	See different Programme areas including Elective Recovery, COVID-19, 111, Ambulance, Cancer, Mental Health, GP etc	Elective Recovery
[REQ-7CDE9A]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Total Staff Absence from 2 weeks ago as a raw number	Elective Recovery
[REQ-ADD230]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Total Staff Absence from 2 weeks ago as a % change	Elective Recovery
[REQ-A085D5]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Total Staff Absence from 1 week ago as a raw number	Elective Recovery
[REQ-3D563D]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Total Staff Absence from 1 week ago as a % change	Elective Recovery
[REQ-5B96F3]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Total Staff Absence as a current figure	Elective Recovery
[REQ-8804D9]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View total current value of COVID-19 Inpatients	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-4C53C3]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View total COVID-19 Critical care patients	Elective Recovery
[REQ-C996AF]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View the named highest region of Inpatients	Elective Recovery
[REQ-32F80B]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Operational Capacity & occupancy of beds due to COVID	Elective Recovery
[REQ-E34028]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Operational Capacity & number of beds available	Elective Recovery
[REQ-D7DCDB]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Operational Capacity & number of acute beds available	Elective Recovery
[REQ-C2C02F]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View number of Inpatients in highest region value	Elective Recovery
[REQ-8B1229]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest region for Total Staff Absence as a number	Elective Recovery
[REQ-F51202]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest region for Total Staff Absence as a name	Elective Recovery
[REQ-FE094D]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number of Acute beds in a named region	Elective Recovery
[REQ-005796]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number of Acute beds as a number	Elective Recovery
[REQ-09AD13]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number of beds in a named region	Elective Recovery
[REQ-FDA72E]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number of beds as a number	Elective Recovery
[REQ-542AD6]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number occupancy of beds due to COVID in a named region	Vaccines
[REQ-E9C23E]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View highest number occupancy of beds due to COVID as a number	Vaccines
[REQ-303F31]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Critical care changes from 2 weeks ago in raw numbers	Elective Recovery
[REQ-353204]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Critical care changes from 2 week ago as a % increase/decrease	Elective Recovery
[REQ-CF84F4]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Critical care changes from 1 week ago in raw numbers	Elective Recovery
[REQ-5BE2EC]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Critical care changes from 1 week ago as a % increase/decrease	Elective Recovery
[REQ-B7906F]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View COVID bed changes from 2 weeks ago in raw numbers	Vaccines
[REQ-238B19]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View COVID bed changes from 2 week ago as a % increase/decrease	Vaccines
[REQ-E16D33]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View COVID bed changes from 1 week ago in raw numbers	Vaccines
[REQ-D9D900]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View COVID bed changes from 1 week ago as a % increase/decrease	Vaccines
[REQ-EA46DD]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View changes from 2 weeks ago in raw numbers	Elective Recovery

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-9BF023]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View changes from 2 week ago as a % increase/decrease	Elective Recovery
[REQ-CD1F96]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View changes from 1 week ago in raw numbers	Elective Recovery
[REQ-700E72]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View changes from 1 week ago as a % increase/decrease	Elective Recovery
[REQ-402AFD]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View bed changes from 2 weeks ago in raw numbers	Elective Recovery
[REQ-DE84E3]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View bed changes from 2 week ago as a % increase/decrease	Elective Recovery
[REQ-640269]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View bed changes from 1 week ago in raw numbers	Elective Recovery
[REQ-ACA5AB]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View bed changes from 1 week ago as a % increase/decrease	Elective Recovery
[REQ-4FACEF]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Acute bed changes from 2 weeks ago in raw numbers	Elective Recovery
[REQ-CA6485]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Acute bed changes from 2 week ago as a % increase/decrease	Elective Recovery
[REQ-4BE8DC]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Acute bed changes from 1 week ago in raw numbers	Elective Recovery
[REQ-85B3FF]	Transition	Key Products	Exec Dashboard	The User should be able to view specific data for each area, such as	View Acute bed changes from 1 week ago as a % increase/decrease	Elective Recovery
[REQ-357623]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Filter by Provider	Elective Recovery
[REQ-774B32]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Filter by ICS	Elective Recovery
[REQ-D1D6A6]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Filter by Geography, ICS, Provider	Elective Recovery
[REQ-32B0E2]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Compare by Provider with selected data points	Elective Recovery
[REQ-4AC1B4]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Compare by ICS with selected data points	Elective Recovery
[REQ-6BDE75]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Combine above filters and comparisons	Elective Recovery
[REQ-5FDF2C]	Transition	Key Products	Exec Dashboard	The User should be able to view the data for each specific area in graph format	Be able compare by Geography with selected data points	Elective Recovery
[REQ-2F469E]	Transition	Key Products	IECCP	Alerts at different geographic levels that improve theatre utilisation	Show when there are available capacity	Elective Recovery

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-511505]	Transition	Key Products	IECCP	Alerts at different geographic levels that improve theatre utilisation	Flag when there are unbooked patients due for urgent treatment	Elective Recovery
[REQ-70B5AD]	Transition	Key Products	IECCP	Be able to view and schedule patient theatre procedures	Utilise historical information and data trends to support the planning and booking of theatre sessions	Elective Recovery
[REQ-FF8E2F]	Transition	Key Products	IECCP	Be able to view and schedule patient theatre procedures	Automate operational tasks	Elective Recovery
[REQ-A964F5]	Transition	Key Products	IECCP	Be able to view and schedule patient theatre procedures	Actively book patients in to available theatre sessions	Elective Recovery
[REQ-6205DB]	Transition	Key Products	IECCP	See a system view of theatre capacity	Show numbers of unbooked patients and link to waiting list	Elective Recovery
[REQ-FB5B57]	Transition	Key Products	IECCP	See a system view of theatre capacity	Show information on theatre planning data such as bookings, cancellations, capacity	Elective Recovery
[REQ-10D7F4]	Transition	Key Products	IECCP	See a system view of theatre capacity	Information on patients such as priority status, procedure type, flags for specific risks/conditions	Elective Recovery
[REQ-565AAE]	Transition	Key Products	IECCP	See a system view of theatre capacity	Break information down by geography, trust, specialty, theatre, consultant	Elective Recovery
[REQ-A27DCA]	Transition	Key Products	IECCP	See a system view of theatre capacity	Assess patient readiness status	Elective Recovery
[REQ-92A02B]	Transition	Key Products	IECCP	System view of performance monitoring	View waiting list time improvements	Elective Recovery
[REQ-6136C5]	Transition	Key Products	IECCP	System view of performance monitoring	Calculate touchtime divided by available operating minutes	Elective Recovery
[REQ-9CD093]	Transition	Key Products	IECCP	The user must be able to have a System view of performance	View time for pre-assessment	Elective Recovery
[REQ-A42762]	Transition	Key Products	IECCP	The user must be able to have a System view of performance	View number of bookings	Elective Recovery
[REQ-889CD1]	Transition	Key Products	IECCP	The user must be able to receive alerts at different geographic levels that improve theatre utilisation	View when there are unbooked patients due for urgent treatment	Elective Recovery
[REQ-E8FE82]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View theatre utilisation	Elective Recovery
[REQ-B4A3D6]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View number of pathways reprioritised, confirmed by waitlist	Elective Recovery
[REQ-F540E8]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View number of consultant lists managed in platform	Elective Recovery
[REQ-18FC74]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View number of admitted and non-admitted pathways on waitlist (RTT & non-RTT)	Elective Recovery
[REQ-2E64FE]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View number of >18 & >52 weeks waiters	Elective Recovery
[REQ-9886FE]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View lead time between booking and theatre sessions (time stamps)	Elective Recovery
[REQ-0E6B61]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View % treated within RCS code timeline, Time to receive RCS code, total patients with RCS code	Elective Recovery

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-E2C870]	Transition	Key Products	IECCP	The user must be able to see a system view of performance monitoring	View % OTD cancellations and DNA	Elective Recovery
[REQ-A9DD63]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Show patient numbers on active RTT pathway and non-RTT pathway	Elective Recovery
[REQ-8FC309]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Show numbers of breaching targets, e.g. 18 and 52 week waits	Elective Recovery
[REQ-376B10]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Show number of patients on waiting list, including upcoming bookings	Elective Recovery
[REQ-BAC880]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Have an audit trail of change requests	Elective Recovery
[REQ-3BB2C3]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Have alerts when data quality issues arise	Elective Recovery
[REQ-2C2DBD]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Design and deploy bespoke data quality issues	Elective Recovery
[REQ-F236F0]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Break information down by geography, trust, specialty, consultant	Elective Recovery
[REQ-A8FB65]	Transition	Key Products	IECCP	The user must be able to see a system view of the waiting list	Actively identify the most suitable patient for a theatre slot	Elective Recovery
[REQ-D712D2]	Transition	Key Products	IECCP	The user must be able to view all patients listed for surgery without a pre-operative assessment	View patient details, priority type, TCI date, booking priority	Elective Recovery
[REQ-65901E]	Transition	Key Products	IECCP	The user must be able to view all patients listed for surgery without a pre-operative assessment	View and track outcomes (POA)	Elective Recovery
[REQ-772D40]	Transition	Key Products	IECCP	The user must be able to view all patients listed for surgery without a pre-operative assessment	Identify patients who have DNA or cancelled POAs for rebooking or rescheduling of surgery	Elective Recovery
[REQ-9667D2]	Transition	Key Products	IECCP	The user must be able to view all patients listed for surgerys pre-operative assessment data	Input and display POA booking process information (contact lead, date, and times contact attempted)	Elective Recovery
[REQ-CCDF4D]	Transition	Key Products	IECCP	The user must be able to view all patients listed for surgerys pre-operative assessment data	Display data on patient fitness for surgery and proactively inform rebooking actions	Elective Recovery
[REQ-C071AE]	Transition	Key Products	IECCP	The user must be able to view the outpatient waiting list position	View patient details, requested appointment type, consultant, specialty, priority, status, date added to waitlist, earliest due date, due date, weeks waiting	Elective Recovery
[REQ-BB1C97]	Transition	Key Products	IECCP	The user must be able to see a system view of theatre capacity	Show numbers of unbooked patients and link to waiting list	Elective Recovery
[REQ-4940CA]	Transition	Key Products	IECCP	The user must be able to see a system view of theatre capacity	Information on patients such as priority status, procedure type, flags for specific risks/conditions	Elective Recovery
[REQ-B5FD67]	Transition	Key Products	PPE	The User should be able to click into deliveries to view upcoming and past deliveries	Manage (view, delete, add) for upcoming and past deliveries	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-FD9088]	Transition	Key Products	PPE	The User should be able to click into deliveries to view upcoming and past deliveries	Click into deliveries to view upcoming and past deliveries	Supply Chain
[REQ-D976FD]	Transition	Key Products	PPE	The User should be able to click into stock requests to view upcoming and past deliveries	Manage (approve, amend, reject, add) stock requests	Supply Chain
[REQ-8CADCA]	Transition	Key Products	PPE	The User should be able to click into stock requests to view upcoming and past deliveries	Click into stock requests to view upcoming and past deliveries	Supply Chain
[REQ-C00465]	Transition	Key Products	PPE	The User should land on the homepage from which they are able to navigate through to other pages	View a forecasted view of stock usage alongside an actual view of stock count	Supply Chain
[REQ-572292]	Transition	Key Products	PPE	The User should land on the homepage from which they are able to navigate through to other pages	Manage (approve, delete, add) stock requests	Supply Chain
[REQ-6EDC1A]	Transition	Key Products	PPE	The User should land on the homepage from which they are able to navigate through to other pages	Link view an overall view of PPE stock by type	Supply Chain
[REQ-E8809C]	Transition	Key Products	PPE	The User should land on the homepage from which they are able to navigate through to other pages	Click through to Stability Status	Supply Chain
[REQ-BD337F]	Transition	Key Products	PPE	The User should land on the homepage from which they are able to navigate through to other pages	Click through to Frontline Inventory	Supply Chain
[REQ-CBAD6C]	Transition	Key Products	PPE	User uses Critical Care Equipment to monitor and request new deliveries	View existing deliveries in CCE	Supply Chain
[REQ-75989D]	Transition	Key Products	PPE	User uses Critical Care Equipment to monitor and request new deliveries	Request new delivery	Supply Chain
[REQ-D47BB6]	Transition	Key Products	PPE	User uses Critical Care Equipment to monitor and request new deliveries	Form should be generated to request a new delivery	Supply Chain
[REQ-00EA7F]	Transition	Key Products	PPE	User uses Critical Care Equipment to monitor and request new deliveries	Form should allow conditional selection of equipment	Supply Chain
[REQ-381E3C]	Transition	Key Products	PPE	User uses Region or Trust dashboard to view specific data from different perspectives and with different filtering options	View stock, burn rate, NSDR case rate at a Trust or Regional level	Supply Chain
[REQ-8501E4]	Transition	Key Products	PPE	User uses Region or Trust dashboard to view specific data from different perspectives and with different filtering options	Filter dashboard with a data range	Supply Chain
[REQ-89F8C9]	Transition	Key Products	PPE	User uses Region or Trust dashboard to view specific data from different perspectives and with different filtering options	Filter dashboard by Trust Code, trust Name or Category	Supply Chain
[REQ-ED2DB9]	Transition	Key Products	PPE	User uses Region360 Module to monitor their regional level of PPE	View dashboard which displays regional PPE data	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-BE5686]	Transition	Key Products	PPE	User uses Region360 Module to monitor their regional level of PPE	Click into view Region or Trust data	Supply Chain
[REQ-EB4A52]	Transition	Key Products	PPE	User uses Region360 Module to monitor their regional level of PPE	Click into specific deliveries to see details around it such as	Supply Chain
[REQ-7A3334]	Transition	Key Products	PPE	User uses Region360 Module to monitor their regional level of PPE	Click into Critical Care Equipment	Supply Chain
[REQ-3859F5]	Transition	Key Products	Vaccines	The System must have a range of tools available for Users	Provide management information	Supply Chain
[REQ-79C30B]	Transition	Key Products	Vaccines	The System must have a range of tools available for Users	Do data analysis	Supply Chain
[REQ-7DAA04]	Transition	Key Products	Vaccines	The System must have a range of tools available for Users	Do business analysis	Supply Chain
[REQ-F81E12]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	View health inequalities within the nation	Cohorting
[REQ-B50CC5]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	View health inequalities within a geographical areas, e.g. IMD, ethnicity, age, gender at different geographical hierarchies	Cohorting
[REQ-587A03]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Understand the size of each cohort population	Cohorting
[REQ-5EFB0D]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Understand how health inequalities compare to the nation as a whole	Cohorting
[REQ-DA42A6]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Quantify the true level of inequality in vaccine rollout	Cohorting
[REQ-9A2EAF]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Identify targets requiring possible support to improve equitable vaccine distribution	Cohorting
[REQ-25E6E8]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Identify target areas requiring support	Cohorting
[REQ-4C64FD]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Identify inequalities in vaccine uptakes within the population	Cohorting
[REQ-B062C4]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Develop visual representations to enable gaps in vaccine uptake	Cohorting
[REQ-C28A81]	Transition	Key Products	Vaccines	The User must be able to address inequalities in vaccine uptake between groups	Access and keep updated vaccination activity data	Cohorting
[REQ-54539A]	Transition	Key Products	Vaccines	The User must be able to cancel orders	Submit the cancellation of an order	Supply Chain
[REQ-157FFC]	Transition	Key Products	Vaccines	The User must be able to cancel orders	Cancel orders by choosing an order	Supply Chain
[REQ-B41F59]	Transition	Key Products	Vaccines	The User must be able to edit orders	Enter the number of required doses	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-CF0A79]	Transition	Key Products	Vaccines	The User must be able to edit orders	Choose delivery dates	Supply Chain
[REQ-E91EB6]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	View the % of people to be vaccinated by date	Vaccines
[REQ-B1D2E3]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	View saved plans	Vaccines
[REQ-BC8F2B]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	View PCN log ins per week	Vaccines
[REQ-E8358F]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	View bookings updated	Vaccines
[REQ-10CEEE]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Understand vaccine supply	Vaccines
[REQ-6F7C72]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Understand the required population to vaccinate	Vaccines
[REQ-230314]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Understand the local capacity constraints	Vaccines
[REQ-AC0BAC]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Track progress of PCN vaccination vs supply	Vaccines
[REQ-11DF17]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Track progress and forecast the end of each cohort's vaccination programme	Vaccines
[REQ-491F8E]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Provide operational updates on vaccines progress	Vaccines
[REQ-D647BC]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Plan workforce and estates accordingly	Vaccines
[REQ-8AAAB4]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Monitor when and how much vaccine supply can be expected	Vaccines
[REQ-0D5133]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Manage vaccine supply	Vaccines
[REQ-199372]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Forecast when cohorts will be vaccinated by	Vaccines
[REQ-AE704C]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Estimate cohort vaccination completion	Vaccines
[REQ-4FF5B5]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Effectively manage vaccine allocation	Vaccines
[REQ-C9E388]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Create a plan for vaccine delivery	Vaccines
[REQ-90D647]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Calculate vaccine supply needed per PCN	Vaccines
[REQ-6CB120]	Transition	Key Products	Vaccines	The User must be able to monitor the vaccination supply	Adjust vaccine delivery based on supply	Vaccines
[REQ-F87F7E]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View the replen status	Supply Chain
[REQ-644210]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View the current orders	Supply Chain
[REQ-1A5BA3]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View supply plans	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-F0FAC5]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View past and upcoming deliveries	Supply Chain
[REQ-0AFB35]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View order confirmations	Supply Chain
[REQ-14A1F2]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View cancelled orders	Supply Chain
[REQ-AFD7F2]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View all sites a User has access to	Supply Chain
[REQ-B33A54]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	View a successful order message	Supply Chain
[REQ-1A22DE]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Verify the order	Supply Chain
[REQ-CB60B4]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Enter the number of doses required	Supply Chain
[REQ-C20169]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Create an order	Supply Chain
[REQ-1B3EEB]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Confirm that User details are correct	Supply Chain
[REQ-77E954]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Choose the specific vaccine required	Supply Chain
[REQ-54AECE]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Choose the delivery dates	Supply Chain
[REQ-7E1C5D]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Choose an amount that can be managed in pack sizes	Supply Chain
[REQ-4CE3F5]	Transition	Key Products	Vaccines	The User must be able to order vaccines through an ordering platform	Agree to use the ordering system instead of receiving automatically pushed orders	Supply Chain
[REQ-45867E]	Transition	Key Products	Vaccines	The User must be able to plan the supply of their stock	View existing supply plans	Supply Chain
[REQ-5138DC]	Transition	Key Products	Vaccines	The User must be able to plan the supply of their stock	View different statuses of supply	Supply Chain
[REQ-3E3BEC]	Transition	Key Products	Vaccines	The User must be able to plan the supply of their stock	Review the maximum amount of vaccine that can be drawn down over a time period	Supply Chain
[REQ-C58AFE]	Transition	Key Products	Vaccines	The User must be able to plan the supply of their stock	Request an increase in the maximum amount of the vaccine allocated	Supply Chain
[REQ-6AA2F3]	Transition	Key Products	Vaccines	The User must be able to plan the supply of their stock	Allow sites to order as soon as the max cap is confirmed	Supply Chain
[REQ-3BA03F]	Transition	Key Products	Vaccines	The User must be able to request change to the maximum number of doses	Request a change to the maximum number of doses for a supply plan	Supply Chain
[REQ-DD036A]	Transition	Key Products	Vaccines	The User must be able to request change to the maximum number of doses	Place more than one order per date only if there are two delivery dates that week	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-3F1942]	Transition	Key Products	Vaccines	The User must be able to request change to the maximum number of doses	Access the supply planner from this page	Supply Chain
[REQ-4B6E1B]	Transition	Key Products	Vaccines	The User must be able to understand if there is a sufficient workforce to deliver the vaccination roll out plan	View workforce information by vaccination delivery model, geographical hierarchies, readiness dates, job titles/roles	Vaccines
[REQ-9B3986]	Transition	Key Products	Vaccines	The User must be able to understand if there is a sufficient workforce to deliver the vaccination roll out plan	View duty fill rates, staff availability and unavailability, COVID related absence	Vaccines
[REQ-41EB78]	Transition	Key Products	Vaccines	The User must be able to understand if there is a sufficient workforce to deliver the vaccination roll out plan	View duty fill rates, staff availability and unavailability, COVID related absence	Vaccines
[REQ-C0DB0F]	Transition	Key Products	Vaccines	The User must be able to understand if there is a sufficient workforce to deliver the vaccination roll out plan	Show modelled workforce requirements against recorded available or planned available workforce either overall or for any given area, delivery model, or type of staff	Vaccines
[REQ-D54E52]	Transition	Key Products	Vaccines	The User must be able to understand if there is a sufficient workforce to deliver the vaccination roll out plan	Identify workforce requirements required to deliver vaccinations	Vaccines
[REQ-6E737F]	Transition	Key Products	Vaccines	The User must be able to view all information regarding cancelled orders	View the name of the person who cancelled the order	Supply Chain
[REQ-B0B553]	Transition	Key Products	Vaccines	The User must be able to view all information regarding cancelled orders	View the date an order was cancelled	Supply Chain
[REQ-79FDED]	Transition	Key Products	Vaccines	The User must be able to view all past and upcoming deliveries	View deliveries that have happened in the past week	Supply Chain
[REQ-91C2ED]	Transition	Key Products	Vaccines	The User must be able to view all past and upcoming deliveries	View deliveries that are coming up in the next 7 days	Supply Chain
[REQ-9D4C76]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events by Trust	Vaccines
[REQ-9AA29D]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events by region	Vaccines
[REQ-673760]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events by ICS delivery model	Vaccines
[REQ-F4B5FC]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events at a weekly level	Vaccines
[REQ-FE1941]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events at a daily level, up to hourly as required	Vaccines
[REQ-AC5C88]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View vaccination events at a cumulative level	Vaccines
[REQ-A023D2]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the type of booster received by vaccination type	Vaccines
[REQ-3490D9]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the type of booster received by dose type	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-48BB3F]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the total number of vaccines administered, broken down by first, second, thirds, booster and second booster	Vaccines
[REQ-30A3E8]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the percentage of vaccination events recorded late	Vaccines
[REQ-A5116B]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their third vaccine	Vaccines
[REQ-F169DA]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their second vaccine	Vaccines
[REQ-2ECB2C]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their second booster	Vaccines
[REQ-0178DF]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their first vaccine	Vaccines
[REQ-1D34DE]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their first booster vaccine co administered with the flu vaccine	Vaccines
[REQ-E97438]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View the number of people who have received their first booster	Vaccines
[REQ-076AAA]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View deliver model comparisons for VCs	Vaccines
[REQ-CA9CC1]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View deliver model comparisons for PCNs	Vaccines
[REQ-973455]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View deliver model comparisons for MVSs	Vaccines
[REQ-3C4991]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	View daily vaccination data reports	Vaccines
[REQ-BB338B]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Select multiple options from a dropdown list	Vaccines
[REQ-96D2B7]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the total VC vaccination events	Vaccines
[REQ-FF04F1]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the total LVS vaccination events	Vaccines
[REQ-96A981]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the total LVS pharmacy vaccination events	Vaccines
[REQ-92042E]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the total LVS military and detained estates vaccination events	Vaccines
[REQ-7954F3]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the total HH vaccination events	Vaccines
[REQ-CDA3A3]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the number of doses administered	Vaccines
[REQ-4C1487]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	See the LVS - PCN vaccination events	Vaccines
[REQ-7A1A1C]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Filter by vaccine type	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-AF4432]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Filter by vaccination type	Vaccines
[REQ-27C5AF]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Filter by dose type	Vaccines
[REQ-3D3767]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Filter by delivery model	Vaccines
[REQ-D2039D]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by vaccine type	Vaccines
[REQ-8F453C]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by ethnicity	Vaccines
[REQ-CE9122]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by dose	Vaccines
[REQ-2175DA]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by delivery model	Vaccines
[REQ-577CF3]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by cohort	Vaccines
[REQ-EF0D25]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Drill down for uptake by age	Vaccines
[REQ-3327F8]	Transition	Key Products	Vaccines	The User must be able to view how vaccine rollout is performing	Download graphs, visuals and data	Vaccines
[REQ-87F20D]	Transition	Key Products	Vaccines	The User must be able to view stock information	View waste data by region, STP or site	Supply Chain
[REQ-C8B5C5]	Transition	Key Products	Vaccines	The User must be able to view stock information	View the Mutual Aid doses received by region, STP or site	Supply Chain
[REQ-80EE26]	Transition	Key Products	Vaccines	The User must be able to view stock information	View a graph of vaccinations against the stock	Supply Chain
[REQ-0C13F0]	Transition	Key Products	Vaccines	The User must be able to view stock information	Analyse latest stock holding breakdowns by region, STP and site	Supply Chain
[REQ-717A8F]	Transition	Key Products	Vaccines	The User must be able to view stock information	Compare the Allocations and Immform orders for Hospital Hubs and VCs	Supply Chain
[REQ-B7BFC4]	Transition	Key Products	Vaccines	The User must be able to view stock information	Analyse waste in the system	Supply Chain
[REQ-E08ABC]	Transition	Key Products	Vaccines	The User must be able to view stock information	Analyse the stock	Supply Chain
[REQ-FF408B]	Transition	Key Products	Vaccines	The User must be able to view stock information	Analyse mutual aid	Supply Chain
[REQ-10D3A0]	Transition	Key Products	Vaccines	The User must be able to view Supply Chain Alerts	View the Negative Estimated Stock	Supply Chain
[REQ-D97126]	Transition	Key Products	Vaccines	The User must be able to view Supply Chain Alerts	View Late Stock Report	Supply Chain
[REQ-F9A7E1]	Transition	Key Products	Vaccines	The User must be able to view Supply Chain Alerts	View Excess Stock	Supply Chain
[REQ-275013]	Transition	Key Products	Vaccines	The User must be able to view Supply Chain Alerts	Change status of alerts	Supply Chain
[REQ-3B4454]	Transition	Key Products	Vaccines	The User must be able to view the contents of their order	View the different items ordered	Supply Chain

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-086BEC]	Transition	Key Products	Vaccines	The User must be able to view the contents of their order	View recently deleted bundles	Supply Chain
[REQ-4A0C30]	Transition	Key Products	Vaccines	The User must be able to view the contents of their order	Group orders as bundles under one title	Supply Chain
[REQ-A1C96A]	Transition	Key Products	Vaccines	The User must be able to view the contents of their order	Add extra items	Supply Chain
[REQ-7F9847]	Transition	Key Products	Vaccines	The User must be able to view the replen status	View the list of order bundles that have been rejected	Supply Chain
[REQ-5A9D89]	Transition	Key Products	Vaccines	The User must be able to view the replen status	View the list of order bundles that have been accepted	Supply Chain
[REQ-8DB229]	Transition	Key Products	Vaccines	The User must be able to view the site information and stock	View information about the site	Supply Chain
[REQ-455E87]	Transition	Key Products	Vaccines	The User must be able to view the site information and stock	View a report about the stock	Supply Chain
[REQ-160B94]	Transition	Key Products	Vaccines	The User must be able to view the site information and stock	Update site information to submit a change request	Supply Chain
[REQ-8C1FC8]	Transition	Key Products	Vaccines	The User must have a tool that displays reports on how many COVID vaccinations have been completed	View how many COVID Vaccinations have been completed	Vaccines
[REQ-B1C43A]	Transition	Key Products	Vaccines	The User must have a tool that displays reports on how many COVID vaccinations have been completed	Filter by site	Vaccines
[REQ-8D8480]	Transition	Key Products	Vaccines	The User must have a tool that displays reports on how many COVID vaccinations have been completed	Filter by region	Vaccines
[REQ-98BBA9]	Transition	Key Products	Vaccines	The User must have a tool that monitors the readiness of vaccination sites	Monitor the readiness of vaccination sites	Vaccines
[REQ-87991D]	Transition	Key Products	Vaccines	The User must have a tool that monitors the readiness of vaccination sites	Monitor the performance of vaccination sites	Vaccines
[REQ-4BCB69]	Transition	Key Products	Vaccines	The User must have a tool that monitors the readiness of vaccination sites	Monitor the capacity of vaccination sites	Vaccines
[REQ-121041]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View waste data	Supply Chain
[REQ-B1BB9D]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View usage data	Supply Chain
[REQ-54FD6C]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View stock returns	Supply Chain
[REQ-7EAF8A]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View mutual aid data	Supply Chain
[REQ-351D50]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View delivery data	Supply Chain
[REQ-EA61D0]	Transition	Key Products	Vaccines	The User must have a tool that provides supply chain reporting	View data across the COVID vaccination supply chain	Supply Chain
[REQ-34B0B5]	Transition	Key Products	Vaccines	The User must have training before using the new system	Training resources must be available	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-7EAD43]	Transition	Key Products	Vaccines	The User will need a payments system to pay for vaccines	Pay for vaccine jabs	Vaccines
[REQ-08A60C]	Transition	Key Products	Vaccines	The User will need a set of tools to cover data insights, modelling and reporting	Visualise data	Vaccines
[REQ-B53077]	Transition	Key Products	Vaccines	The User will need a set of tools to cover data insights, modelling and reporting	Provide support decision making	Vaccines
[REQ-E4B60A]	Transition	Key Products	Vaccines	The User will need a set of tools to cover data insights, modelling and reporting	Model assumptions to develop, review and analyse different scenarios	Vaccines
[REQ-9B3FD4]	Transition	Key Products	Vaccines	The User will need a set of tools to cover data insights, modelling and reporting	Help teams understand performance	Vaccines
[REQ-0FC789]	Transition	Key Products	Vaccines	The User will need a set of tools to cover data insights, modelling and reporting	Analyse data collected through tech systems	Vaccines
[REQ-2465E5]	Transition	Key Products	Vaccines	The User will need reporting on co-administration of the Flu and COVID vaccines	Support developers in creating a scalable Vaccines data model ('ontology')	Vaccines
[REQ-48E172]	Transition	Key Products	Vaccines	The User will need reporting on co-administration of the Flu and COVID vaccines	Ingest new data as agreed by the Parties and configure pipelines for the Flu vaccine data asset	Vaccines
[REQ-28E77A]	Transition	Key Products	Vaccines	The User will need reporting on co-administration of the Flu and COVID vaccines	Configure two dashboards to help monitor Flu vaccination event performance and vaccine uptake	Vaccines
[REQ-AF3156]	Transition	Key Products	Vaccines	The User will need reporting on co-administration of the Flu and COVID vaccines	Configure co-administration of Flu and COVID vaccinations views in COVID vaccination reporting dashboards	Vaccines
[REQ-323C7C]	Transition	Key Products	Vaccines	The User will need to adapt reporting and data assets to align with the changing requirements	Support the changing mix of delivery models	Vaccines
[REQ-05014C]	Transition	Key Products	Vaccines	The User will need to adapt reporting and data assets to align with the changing requirements	Support reporting on the vaccination of children	Vaccines
[REQ-C666B5]	Transition	Key Products	Vaccines	The User will need to adapt reporting and data assets to align with the changing requirements	Configure data pipelines and amend existing reports to support the administration of booster doses	Vaccines
[REQ-EB4D58]	Transition	Key Products	Vaccines	The User will need to adapt reporting and data assets to align with the changing requirements	Configure a dashboard to support the flexible definition of population cohorts to be used in uptake monitoring reports	Vaccines
[REQ-FB2231]	Transition	Key Products	Vaccines	The User will need to adapt reporting and data assets to align with the changing requirements	Assist with the refinement of the cohort definition of Healthcare Workers and Social Care Workers	Vaccines

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-CB86B1]	Transition	Key Products	Vaccines	The User will use the landing page to view key metrics for the Vaccine Supply Chain	View the number of Alerts in the last two weeks	Supply Chain
[REQ-164019]	Transition	Key Products	Vaccines	The User will use the landing page to view key metrics for the Vaccine Supply Chain	View the last updated time for different datasets	Supply Chain
[REQ-29CBE5]	Transition	Key Products	Vaccines	The User will use the landing page to view key metrics for the Vaccine Supply Chain	View key metrics	Supply Chain
[REQ-0FBB19]	Transition	Key Products	Vaccines	The User will use the System to view allocation data	View allocation data	Supply Chain
[REQ-6C3E33]	Transition	Key Products	Vaccines	The User will use the System to view Deliveries and ETAs	View data about item deliveries	Supply Chain
[REQ-F3A309]	Transition	Key Products	Vaccines	The User will use the System to view metrics for each site	View different statistics about each site	Supply Chain
[REQ-A61BCC]	Transition	Key Products	Vaccines	The User will use the System to view metrics for each site	For each site and vaccines supplier a User will view the stocktake	Supply Chain
[REQ-85AC05]	Transition	Key Products	Vaccines	The User will use the System to view metrics for each site	For each site and vaccines supplier a User will view the smart stock estimate	Supply Chain
[REQ-9A0812]	Transition	Key Products	Vaccines	The User will use the System to view metrics for each site	For each site and vaccines supplier a User will view the crude stock estimate level	Supply Chain
[REQ-81FF07]	Transition	Key Products	Vaccines	The User will use the System to view order data	View order data	Supply Chain
[REQ-5F3B91]	Transition	Key Products	Vaccines	The User will use the System to view order data	Place orders via the ordering platform	Supply Chain
[REQ-FF8D6E]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View the Allocation Date	Supply Chain
[REQ-6F8113]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View a graph for Vaccine Type	Supply Chain
[REQ-F40AD6]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View a graph for Source Type	Supply Chain
[REQ-2056E7]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View a graph for Orders and Vaccinations	Supply Chain
[REQ-7AD39F]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View a graph for Dose Type	Supply Chain
[REQ-205850]	Transition	Key Products	Vaccines	The User will use the System to view Ordering and Allocation information	View a graph for Allocations	Supply Chain
[REQ-FD4A47]	Transition	Key Products	Vaccines	The User will use the System to view stock levels	See the levels of stock available	Supply Chain
[REQ-F16D9E]	Transition	Key Products	Vaccines	There must be technical support and maintenance available	Log tickets for support	Vaccines
[REQ-1B7A15]	Transition	Other Products	Scheduling	Ability to set the waitlist strategy	View to filter and select Waitlist Optimisation Rules	Elective Recovery
[REQ-26078D]	Transition	Other Products	Scheduling	Ability to set the waitlist strategy	View Priority, Procedure Date/Time, Patient details, Suggested schedules	Elective Recovery

UUID	Transition/To-be	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Use Case
[REQ-1FE2E4]	Transition	Other Products	Scheduling	Ability to set the waitlist strategy	View Intended procedure description	Elective Recovery
[REQ-A2B22F]	Transition	Other Products	Scheduling	Be able to view and schedule patient theatre procedures	View Unbooked Minutes, Adjusted Booked Utilisation, Booked Utilisation	Elective Recovery
[REQ-1A10F5]	Transition	Other Products	Scheduling	Be able to view and schedule patient theatre procedures	View Theatre type, Specialty, Consultant	Elective Recovery

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.2.1.1.1]	Platform	Analytical Solutions	Access and Performance	Data Marts	Structure and manipulate data into datasets representative of a specific business area. These data sets must be ready for consumption.
[REQ-2.1.5.4.1]	Platform	Data Platform	Application Building	Report builder	Enable the development of analytical solutions (visualisations and dashboards) using No Code / Low Code tools following industry best practice.
[REQ-2.2.1.4.1]	Platform	Analytical Solutions	Access and Performance	Extracts/Feeds	The ability to build data extracts
[REQ-2.2.1.3.1]	Platform	Analytical Solutions	Access and Performance	OLAP Engine	Perform multidimensional analysis on large volumes of data at high speed.
[REQ-2.2.1.2.1]	Platform	Analytical Solutions	Access and Performance	Views	Easily and/or automatically update any caches of data either programmatically, on a schedule, or as the underlying data changes
[REQ-2.2.1.2.2]	Platform	Analytical Solutions	Access and Performance	Views	Create, alter and delete virtual tables, that are always up-to-date, based on the output of queries and share for reuse
[REQ-2.2.1.2.3]	Platform	Analytical Solutions	Access and Performance	Views	Cache (e.g. store in high performance disk and/or in memory) and/or model data in the platform to enable faster, more performant access e.g. for faster (development and running of) reports and dashboards
[REQ-2.6.4.0.1]	Platform	SDLC	MLOps	n/a	Test and deploy machine learning models e.g. including continual learning and AI to enhance models over time based on actual events. Ensure that the deployment process is seamless and fully integrated into the data science process
[REQ-2.6.4.0.2]	Platform	SDLC	MLOps	n/a	Provide and enforce traceability between at least: - versions of code; - versions of software environments and dependencies; - versions of data; - training runs; - versions of artifacts (e.g. machine learning models, configs, etc.) and - versions of deployed models, ML pipelines and endpoints etc.
[REQ-2.6.4.0.3]	Platform	SDLC	MLOps	n/a	Provide a fully integrated, elastically scalable host for machine learning models with a seamless deployment process to serve model predictions / inferences. This must include both batch and real-time endpoints

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.6.4.0.4]	Platform	SDLC	MLOps	n/a	Provide a mechanism to train and tune machine learning models including support for debugging of training runs/experiments and parameter optimisation
[REQ-2.6.4.0.5]	Platform	SDLC	MLOps	n/a	Develop, test, deploy, host and operate machine learning pipelines easily and quickly using code-first (e.g. Python, R) and / or low-code / no-code tooling. ML pipelines must support at least the follow stages: - preparing data and feature engineering, - building models - training models - hyperparameter tuning - testing - model deployment and management
[REQ-2.6.4.0.6]	Platform	SDLC	MLOps	n/a	Integrate seamlessly with DataOps processes including the ability to trigger machine learning pipelines manually, on a schedule, on a trigger, as part of a data pipeline, or when data drift is detected
[REQ-2.6.4.0.7]	Platform	SDLC	MLOps	n/a	Support out-of-the-box support , and tightly integration with, common data science frameworks (e.g. scikit-learn, MLlib, PyTorch, TensorFlow, Keras, spaCy) and common data science processes (e.g. hyperparameter tuning, tracking metrics across training runs and epochs, etc.)
[REQ-2.6.4.0.8]	Platform	SDLC	MLOps	n/a	Run automated tests, out-of-the-box where possible, for machine learning pipelines and models including testing for fairness, bias, expandability. Where tests are not applied automatically, they should be quick and easy to implement for data scientists
[REQ-2.4.5.0.1]	Platform	Data Management, Intelligent Governance and Automation	Master and Reference Data Management	n/a	The platform should have the ability to effectively store and manage master data, as well as the ability to store or call additional sets of data with the purposed of providing additional context

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.2.1.5.1]	Platform	Analytical Solutions	Access and Performance	Discovery/Sandbox	Provision sandbox environments for internal end users e.g. data scientists, containing data that allows them to experiment with IG approved datasets, data models, data pipelines and transformations for reporting and analytical purposes and integrate these with SDLC
[REQ-2.6.5.0.1]	Platform	SDLC	Environment Management	n/a	Provision of ephemeral environments complete with synthetic data, IG Approved Datasets and platform services to support the development and testing of products
[REQ-2.2.1.5.2]	Platform	Analytical Solutions	Access and Performance	Discovery/Sandbox	Allow internal end-users to interrogate data in their own sandbox and Personalise their own data products, using best practice, industry standard patterns and create new analytical solutions
[REQ-2.2.2.3.1]	Platform	Analytical Solutions	Visualisation	Geographical	Provide geographical representations (maps) of the data, using geographical attributes (address, postcode, region, coordinates). For example, to produce a UK heatmap of vaccination uptake or to produce a flow diagram of patient movement through a hospital building.
[REQ-2.2.2.2.1]	Platform	Analytical Solutions	Visualisation	BI / Reporting	Produce KPI and Operational Reports that support trend analysis and the identification of performance outliers
[REQ-2.2.2.2.2]	Platform	Analytical Solutions	Visualisation	BI / Reporting	Build on-demand, scheduled and/or automatically triggered sets of information and visualisations to be used as required.
[REQ-2.2.2.1.1]	Platform	Analytical Solutions	Visualisation	Visualisation	Visualise data using reports and dashboards, including comprehensive set of out-of-the-box visualisations (e.g. bar charts, line charts, scatters, waterfalls, sankeys, network diagrams, word clouds, maps etc.) and custom visualisations
[REQ-2.2.2.1.2]	Platform	Analytical Solutions	Visualisation	Visualisation	Support user interactions on reports and dashboards including, but not limited to, filters, slicers, navigation, cross-filtering of visuals, tooltips, drill-downs, drill-throughs, and other more complex interactions
[REQ-2.2.2.1.3]	Platform	Analytical Solutions	Visualisation	Visualisation	Produce images, diagrams, infographics or animations to effectively communicate the information contained in the data.
[REQ-2.2.2.1.4]	Platform	Analytical Solutions	Visualisation	Visualisation	Add story telling to data visualisations including, but not limited to, add commentary / explanatory text, bookmarking views of the dashboard to revisit in meetings, exporting automatically to a presentation, collating elements from across multiple dashboards / reports into a single story

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.2.2.2.3]	Platform	Analytical Solutions	Visualisation	BI / Reporting	Report on / visualize data in near-real-time and real-time through reports, dashboards and other visuals
[REQ-2.2.2.1.5]	Platform	Analytical Solutions	Visualisation	Visualisation	Meet accessibility standards, and responsive design principles for reports and dashboards, and make accessible via mobile, web and desktop.
[REQ-2.4.10.0.1]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Use a comprehensive set of out-of-the-box time-based and event-based methods as part of application workflows e.g. schedules, tumbling windows, trigger manually as and when needed, triggers based on file uploads, trigger based on external application calling an API, triggers based on a user entering data into a platform application that meets a certain criteria
[REQ-2.4.10.0.2]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Robustly and gracefully operate platform applications and application workflows including, but not limited to, handling bad data part way through a workflow or back-end process, data validation / reject data if it doesn't meet a defined standard, sending alerts to the users or central service team, automatically recovering from failed workflows, handling errors by specifying success and error paths, etc.
[REQ-2.4.10.0.3]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Quickly and easily monitor and debug application workflows
[REQ-2.4.10.0.4]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Provide configurable alerting services within workflows that will send notifications to defined users based on status and thresholds (e.g. duration of task at defined status > 2 hrs)

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.10.0.5]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Support the execution of APIs within the workflow in order to call 3rd party APIs and ML model endpoints as tasks
[REQ-2.1.5.2.1]	Platform	Data Platform	Application Building	Workflow Builder	Develop application workflows using a comprehensive set of out-of-the-box components, connectors, tasks, operators etc. e.g. logical operators, loops, conditionals, approval steps, workflow branching
[REQ-2.1.5.2.2]	Platform	Data Platform	Application Building	Workflow Builder	Develop and re-use templates and components for workflows
[REQ-2.3.11.0.1]	Platform	Platform Applications	n/a	n/a	Build, share and reuse common functional components or library code to ensure common functions are used consistently throughout the platform and delivery of business features is optimised.
[REQ-2.1.5.2.3]	Platform	Data Platform	Application Building	Workflow Builder	Support the automation of routine processes and promote continual service improvement through the continual development of operational workflows
[REQ-2.4.10.0.6]	Platform	Data Management, Intelligent Governance and Automation	Scheduling & Workflow	n/a	Support high concurrency of workflows (>10k) both per tenant and across tenants, with relevant user visibility, monitoring and alerting
[REQ-2.3.11.0.2]	Platform	Platform Applications	n/a	n/a	Meet accessibility standards, and responsive design principles for platform applications and make accessible via mobile, web and desktop.
[REQ-2.1.5.1.1]	Platform	Data Platform	Application Building	Form Builder	Validate inputs at point of data entry
[REQ-2.1.5.1.2]	Platform	Data Platform	Application Building	Form Builder	Build and reuse common data entities in data capture parts of applications and in forms e.g. All fields for "patient" should only need to be defined once and reused in all data capture

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.5.1.3]	Platform	Data Platform	Application Building	Form Builder	Build and operate applications which capture new data into FDP, including structured, semi-structured and unstructured (textual) information, as well as binary data such as images.
[REQ-2.1.5.1.4]	Platform	Data Platform	Application Building	Form Builder	Automatically generate data capture elements or entire applications from the data model or specific data entities
[REQ-2.1.5.1.5]	Platform	Data Platform	Application Building	Form Builder	Allow end-users to perform "write-backs" to the data storage layers of the platform from within the platform (e.g. platform applications)
[REQ-2.1.5.1.6]	Platform	Data Platform	Application Building	Form Builder	Create, manage and publish forms or other interfaces to gather data from end-users. A low-code / no-code option would be preferred.
[REQ-2.4.7.0.1]	Platform	Data Management, Intelligent Governance and Automation	Enterprise Search	n/a	Intuitively search (e.g. natural language search, autocomplete etc.), browse and filter the data catalog for data assets through an easy-to-use interface
[REQ-2.4.6.0.1]	Platform	Data Management, Intelligent Governance and Automation	Data Catalogue	n/a	Discover, explore and query the data catalogue using secure, open APIs to determine the number of data assets (files, database, tables, attributes, metrics) by type, owner, location, size and other metadata
[REQ-2.4.6.0.2]	Platform	Data Management, Intelligent Governance and Automation	Data Catalogue	n/a	Raise queries or comments against the definition or accuracy of any given data set or report, in a simple and straightforward manner

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.6.0.3]	Platform	Data Management, Intelligent Governance and Automation	Data Catalogue	n/a	Easily create and maintain a data catalogue including the ability to explain the various data objects, provide classifications, define what they represent, record their lineage and how they relate to other objects, record their level of curation/quality, and add other metadata (e.g. owner, location, type etc.)
[REQ-2.4.6.0.4]	Platform	Data Management, Intelligent Governance and Automation	Data Catalogue	n/a	Classify / tag data based on sensitivity, and other attributes e.g. department, region, owner, and ensure these can be used when searching and filtering the catalogue for datasets
[REQ-2.4.6.0.5]	Platform	Data Management, Intelligent Governance and Automation	Data Catalogue	n/a	Support scanning of the data architecture across the platform to identify new, updated and deleted data assets and update the data catalogue accordingly
[REQ-2.4.4.0.1]	Platform	Data Management, Intelligent Governance and Automation	Glossary/Taxonomy	n/a	Provide a business glossary that is accessible, reliable, robust and aligns to the agreed NHS taxonomy and terms
[REQ-2.4.9.0.1]	Platform	Data Management, Intelligent Governance and Automation	Data Modelling	n/a	Store, access and share structural, and schema-related information about the data objects held in FDP in both and tabular and graphical format

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.9.0.2]	Platform	Data Management, Intelligent Governance and Automation	Data Modelling	n/a	Define and maintain conceptual, logical and physical data models. Models should be shareable in multiple formats.
[REQ-2.4.13.0.1]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Support the review and approval of changes to the canonical data model by a central governance organisation, to ensure that the proposed changes will make sense and can be applied across all tenants
[REQ-2.4.8.0.1]	Platform	Data Management, Intelligent Governance and Automation	Compliance	n/a	Define and enforce a set of common data architecture standards. These would be rules and guidelines that apply to (at least) the data, data connectors, data ingest, data sharing, data pipelines, data capture and data models, and should include NHS data standards. It must be possible to define rules using configuration
[REQ-2.4.13.0.2]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Compare metadata relating to data structures and definitions across all tenants in order to identify differences and support overall data governance.
[REQ-2.1.3.4.1]	Platform	Data Platform	Data Processing	Aggregation	Create, store and share data aggregated for analytical, privacy, compliance, and / or performance reasons. These aggregates must automatically update as further data flows into the platform unless specifically designed to the contrary.
[REQ-2.1.4.2.1]	Platform	Data Platform	Data Science & Advanced Analytics	Artificial Intelligence	Apply custom and external Artificial Intelligence services to analyze, produce insight, enrich datasets or process unstructured data

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.3.2.1]	Platform	Data Platform	Data Processing	Conforming	Process data as it is ingested and ensure it aligns to a pre-defined model (original raw data should also be stored as-is)
[REQ-2.4.3.0.1]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Remove or improve (bad) raw inbound data automatically against a common template.
[REQ-2.1.3.1.1]	Platform	Data Platform	Data Processing	Data Enrichment	Improve or supplement data from a specific source by combining it with data from other sources, either static or dynamic. The complementary sources may be internal or external. The methods available to combine the data must be flexible and comprehensive including, but not limited to, union, union all, except, intersect, left join, right join, inner join, full outer join, self join, cross join, fuzzy match, probabilistic match, and unequal joins
[REQ-2.4.11.0.1]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Quickly and easily orchestrate data pipelines (e.g. processing, transformation etc.) through both low-code / no-code interfaces and code-first methods.
[REQ-2.4.11.0.2]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Quickly and easily monitor and debug data orchestrations and data pipelines

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.11.0.3]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Orchestrate data pipelines (e.g. processing, transformation etc.) using a metadata driven approach e.g. running a template data pipeline multiple times using a configuration file
[REQ-2.4.11.0.4]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Orchestrate data pipelines (e.g. processing, transformation etc.) using a comprehensive set of out-of-the-box components, tasks, operators etc. e.g. loops, conditionals, execute pipeline,
[REQ-2.4.11.0.5]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Develop data pipelines (e.g. processing, transformation etc.) easily and quickly using either code-first or low-code approaches
[REQ-2.4.11.0.6]	Platform	Data Management, Intelligent Governance and Automation	Orchestration	n/a	Develop and use templates for all or part of data pipelines and data workflows / orchestrations
[REQ-2.1.1.2.1]	Platform	Data Platform	Integration Services	API Integration	Support the use of 3rd party engines via industry-standard APIs for processing data in FDP.
[REQ-2.1.4.1.1]	Platform	Data Platform	Data Science & Advanced Analytics	Machine Learning	Provide a data science workspace capability that supports the development and execution of machines learning and statistical models for the interpretation of datasets.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.3.3.1]	Platform	Data Platform	Data Processing	Transformation	Performantly and easily apply the full, comprehensive range of data processing / transformation out of the box including cleansing, reading and writing, joins (including unequal joins, and fuzzy / probabilistic matching), filters, derived columns, pivoting, merge, upserts, and windowing
[REQ-2.1.2.1.1]	Platform	Data Platform	Data Repositories	Data Lake	Host, run and operate a repository designed to store, process and secure large amounts of structured, semi-structured and unstructured data. It can store data in its native format, but open formats are preferred. It must store data as appropriate as it flows through the various stages of transformation and consumption e.g. storing data in it's raw format, storing data in a cleansed format, storing the fully derived/modelled data, storing final outputs
[REQ-2.1.2.1.2]	Platform	Data Platform	Data Repositories	Data Lake	Host the entire data model without the reliance of running datasets outside of the platform
[REQ-2.4.12.0.1]	Platform	Data Management, Intelligent Governance and Automation	Data Archival and Record Management	n/a	Archive data according to NHS Policies (IG and Technical). The archive solution must manage the archive in such a way to reliably store and clear down data that has expired in order to optimize storage.
[REQ-2.1.2.3.1]	Platform	Data Platform	Data Repositories	Document Store	Store data in an object focused manner, a singled document relates to an object and any related metadata.
[REQ-2.1.2.2.1]	Platform	Data Platform	Data Repositories	Enterprise Data Warehouse	Store structured data in a relational format that consolidate data from multiple sources into a conformed accessible data structure.
[REQ-2.1.2.4.1]	Platform	Data Platform	Data Repositories	Graph	Store data based on the relationships between different elements in an evolutive and flexible manner.
[REQ-2.1.1.2.2]	Platform	Data Platform	Integration Services	API Integration	Push/pull data in and out of FDP via a machine-readable interface, for example using FHIR, HL7 or other domain standard message structures where appropriate.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.1.8.1]	Platform	Data Platform	Integration Services	Healthcare Specific (HL7, FHIR)	Support industry standard healthcare data interchange formats including HL7 and FHIR. Provide out-of-the-box data connectors to commercial off-the-shelf software such as Electronic Healthcare Record and Patient Administration Systems, and the variety of clinical and operational management systems used in different NHS settings.
[REQ-2.1.1.6.1]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Ingest from external data sources to enrich the data held in FDP. These external data sources may range from nationwide datasets (data from MoD, ONS, weather forecast…), to regional datasets needed by the ICS (data from local authorities, educational system…), to specific datasets Trusts require (data from local charities, specialist data…)
[REQ-2.1.1.6.2]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Provide system specific connectors for specialized operational systems where the number of COTs packages is low and there are few dominant products serving a large percentage of the market.
[REQ-2.1.1.6.3]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Interface management services to provide governance and control of interface usage. Currently an NHS Digital APIGEE based API management service is in place and should be used in preference.
[REQ-2.1.1.6.4]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Provide integration services that support secure and managed API, event stream together with legacy file transfer and relational table protocols, where possible using standard message formats such as HL7 V2, V3 and FHIR
[REQ-2.1.1.6.5]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Provide integration services that cater to all types of data flows including batch, near real-time and event-driven; structured data, semi-structured data, unstructured data, and binary data such as images.
[REQ-2.1.1.6.6]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Ingest from external sources and re-use NHSE national level integration systems.
[REQ-2.1.1.6.7]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Ingest data at many levels of the healthcare structure. For instance, data could flow from a Trust's COTS system (noting that Trusts may have multiple duplicate systems for a certain type of data), or from an ICS data warehouse.
[REQ-2.1.1.6.8]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Extend the type and number of integration services offered via pre-defined and built elements. These connectors can be utilized in code-first, no-code or low-code patterns.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.1.6.9]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Support standard and/or commonly used integration mechanisms (e.g. for data ingestion or data sharing/publishing). These connectors can be utilized in code-first, no-code or low-code patterns.
[REQ-2.1.1.8.2]	Platform	Data Platform	Integration Services	Healthcare Specific (HL7, FHIR)	Enable end-users to access data using HL7's FHIR standard (Restful APIs, Documents, Messages, etc.) to, for example, run push/pull queries for detailed end-user analysis and reporting.
[REQ-2.1.1.6.10]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Support efficient and secure bi-directional dataflows between NHS organisations at a National, Regional, Local level, Trusts and ICS
[REQ-2.1.1.6.11]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Scale up/down and out/in, in anticipation of adopting new data sources, whether structured, semi-structured or unstructured data (including but not limited to the following database connections: ODBC, JDBC, etc.)
[REQ-2.1.1.6.12]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Interface with other systems/apps/data sources using out the box connectors to facilitate ingestion and write back including on-premise/cloud etc. with appropriate historic data, fully reconciled, ensuring no loss of service
[REQ-2.1.1.6.13]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate with IoT devices via ingestion feeds and other digital applications for data capture e.g. using MQTT, AMQP, CoAP, DDS
[REQ-2.1.1.6.14]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate existing NHS products/systems/capabilities via a single integration layer (internal & external at all NHS operational hierarchies) and ensure interoperability through a secure data integration mechanism (data transfers and high processing speeds).
[REQ-2.1.1.1.1]	Platform	Data Platform	Integration Services	File Transfer	Support delivering data into the FDP system via files. Files could either be posted into the system or pulled from source location.
[REQ-2.1.1.5.1]	Platform	Data Platform	Integration Services	Publishing	Share the data model to other tenants of the FDP, as well as external applications / systems (with appropriate governance, security and privacy in place) . This must be possible both manually and automatically, depending on the use case.
[REQ-2.1.1.5.2]	Platform	Data Platform	Integration Services	Publishing	Share data to other tenants of the FDP, as well as external applications / systems (with appropriate governance, security and privacy in place) . This must be possible both manually and automatically, depending on the use case.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.1.3.1]	Platform	Data Platform	Integration Services	Pub-Sub	Push message data out of FDP to be consumed by external systems, including in real-time
[REQ-2.2.1.4.2]	Platform	Analytical Solutions	Access and Performance	Extracts/Feeds	Format, review and validate data prior to sharing outside of tenant. Data Extracts should comply with Information Governance Policies and specific DPIA processes
[REQ-2.1.1.3.2]	Platform	Data Platform	Integration Services	Pub-Sub	Ingest, consume and share event streams e.g. capturing event data from a Kafka stream for reporting real-time / near real-time data
[REQ-2.1.1.3.3]	Platform	Data Platform	Integration Services	Pub-Sub	Ingest, consume and share data via publish-subscribe mechanisms, including FDP messaging systems and external or national event management infrastructure e.g. pub-sub
[REQ-2.1.1.4.1]	Platform	Data Platform	Integration Services	RDBMS	Connect to remote relational databases and consume information from them based on a schedule or triggered events with appropriate governance.
[REQ-2.1.1.7.1]	Platform	Data Platform	Integration Services	Streaming	The ability to process data generated continuously by many data sources, dealing with issues including out-of-sequence data; decisions on what data in the persistence layer is to be discarded, overwritten or retained for audit purposes; raising alerts based on conditions within processed data.
[REQ-2.1.1.7.2]	Platform	Data Platform	Integration Services	Streaming	The ability to produce "sliding windows" from a continuous stream of data
[REQ-2.1.1.7.3]	Platform	Data Platform	Integration Services	Streaming	The ability to produce "tumbling windows" from a continuous stream of data
[REQ-2.5.9.0.1]	Platform	Security and Common Services	Cloud and Platform Security	n/a	Security Requirements are defined in 04 - Security Requirements (Level 3 = Cloud Security)
[REQ-2.4.13.0.3]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Create and Maintain Tenants based on configured tenancy profile with a full suite of data platform capabilities as defined in the capability model and in line with IG and Security Policy.
[REQ-2.6.1.0.1]	Platform	SDLC	CI/CD Pipeline	n/a	Provide open interfaces to the CI/CD pipelines in order to enable deployment of products and platform services to a defined Tenant

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.1.4.3.1]	Platform	Data Platform	Data Science & Advanced Analytics	Natural language processing	Provide natural language processing and other functions to interrogate and make unstructured data useable in platform applications, reports and dashboards.
[REQ-2.7.1.0.1]	Platform	FDP Overall	Standards and Frameworks	n/a	Provide a service management system to comply with ISO 2000001 [https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-3:v1:en]
[REQ-2.4.13.0.4]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Isolate each tenant as appropriate (e.g. logically), unless otherwise specified in order to provide sufficient flexibility to each tenant without impacting other tenants
[REQ-2.1.1.2.3]	Platform	Data Platform	Integration Services	API Integration	Directly access the storage layer (e.g. data lake), after appropriate authentication and authorisation, from external tools to facilitate an open, interoperable platform
[REQ-2.7.1.0.2]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with Government Web Content Accessibility Guidelines (WCAG 2.1 level AA) [https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag]
[REQ-2.7.1.0.3]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with DCB1605 Accessible Information [https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1605-accessible-information]
[REQ-2.7.1.0.4]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with Clinical Safety Standards where appropriate according to context and usage of the platform application [https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems]

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.13.0.7]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Apply data privacy measures as data moves between Tenants * Data owner-specific tenants: for example, a direct care data for a specific Trust * ICS and sub-national tenants: where use cases access a larger data set and typically with data privacy measures applied * National tenants: where use cases access a population-sized data set and typically with further data privacy measures applied
[REQ-2.1.1.6.15]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate with established data sources including Secondary Uses Service (SUS+), Data Provisioning Service (DPS) and Organisational Data Service (ODS).
[REQ-2.1.1.6.16]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate with established data transfer mechanisms including Strategic Data Collection Service (SDCS), Bureau Service Portal (BSP), and The Message Exchange for Social Care and Health (MESH)
[REQ-2.1.1.6.17]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate with established services including: Data Registers Service (DRS), National Opt-out Service, Master Person Service (MPS), Organisation, Standards, Codes and Reference (OSCAR), NHS Digital Terminology Server, NHS Data Model and Data Dictionary Service
[REQ-2.1.1.2.4]	Platform	Data Platform	Integration Services	API Integration	Integrate with the Unified Data Access Layer (UDAL) to promote reuse of common data access services, promote API based technologies and provide a degree of data resilience at a national level.
[REQ-2.5.12.0.1]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide automated recommendations for optimising workloads (incl. processing and storage components) based on price and/or performance to support continuous improvement across the platform (e.g. query optimisation).
[REQ-2.5.12.0.2]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Tag Resources to support the breakdown of cost, compute, storage and network traffic by platform resource, resource type, tenant, use-case/product, product owner.
[REQ-2.2.1.1.2]	Platform	Analytical Solutions	Access and Performance	Data Marts	Support, as needed (i.e. dependent on use case), high performance workloads through, for example, lower latency, higher I/O storage
[REQ-2.7.1.0.5]	Platform	FDP Overall	Standards and Frameworks	n/a	Support Open Development Approach e.g. InnerSource (https://resources.github.com/InnerSource/fundamentals/) to allow products to be developed across the FDP ecosystem

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.12.0.2]	Platform	Data Management, Intelligent Governance and Automation	Data Archival and Record Management	n/a	Support the permanent, logical and physical, deletion of data (e.g. in application workflows, data workflows etc.)
[REQ-2.5.12.0.3]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide elastically scalable platform services to support the scale up/down in accordance with workload demands
[REQ-2.4.13.0.5]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	create and maintain tenancy profiles aligned to each of the tenancy organisation types Trusts, Care Providers, ICS, Regional or National. Tenancy profiles should not only define the available platform capabilities but also comply with the relevant IG policies.
[REQ-2.1.1.6.18]	Platform	Data Platform	Integration Services	Data Ingestion Connectors	Integrate with established technologies (e.g. Tableau, Power BI, Databricks) to exploit existing license agreements, skills and training.
[REQ-2.7.1.0.6]	Platform	FDP Overall	Standards and Frameworks	n/a	Ensure user experience and compliance of WCAG 2.1 AA at all levels. Ref: https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag
[REQ-2.5.4.0.1]	Platform	Security and Common Services	Audit and Logging	n/a	Comprehensively audit and log all operations executed on the platform in order to provide accountability and traceability of user actions and support complex defect tracing an a multi component environment.
[REQ-2.7.1.0.7]	Platform	FDP Overall	Standards and Frameworks	n/a	Support direct user access to the system through the internet using a web browser, secure managed desktops (VDIs e.g. Citrix, Amazon AppStream) and also through APIs. The screens must use responsive / mobile-friendly technology so that they can be clearly presented on tablets and other devices
[REQ-2.7.1.0.8]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with NHSE Accessible Information Standard [https://www.england.nhs.uk/about/equality/equality-hub/patient-equalities-Programme/equality-frameworks-and-information-standards/accessible info]

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.7.1.0.9]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with NHS Service Standard Principles [https://service-manual.nhs.uk/standards-and-technology/service-standard]
[REQ-2.7.1.0.10]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with NHS Records Management Code of Practice [https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/]
[REQ-2.7.1.0.11]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with NHS Architecture Principles [https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-architecture/principles]
[REQ-2.7.1.0.12]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with GDS Service Standard Principles [https://www.gov.uk/service-manual/service-standard]
[REQ-2.5.4.0.2]	Platform	Security and Common Services	Audit and Logging	n/a	Have a record of all interactions and events that occur on the platform which includes information on who performed the action and when. The logs cannot be altered or interfered with. This must support governance, auditing (to support SOC2 reports), and forensics needs. In relation to audit logs, the Authority expectation is that these are configurable in terms of the level of data collected. The Authority would expect logs to collect, for example, metadata and data regarding analytics queries submitted to the Data Platform, but not their results. Platform logging aggregation from different Tenants into NHSE Tenant is not required, however the ability to understand local tenants is required.
[REQ-2.5.1.0.1]	Platform	Security and Common Services	Identify and Access	n/a	Security Requirements are defined in 04 - Security Requirements (Level 3 = IDAM)
[REQ-2.4.7.0.2]	Platform	Data Management, Intelligent Governance and Automation	Enterprise Search	n/a	The platform should feature a dynamic Enterprise Search capability, allowing users of the system to search and discover data assets within FDP and other key file stores and data repositories which are relevant to their role and previous activity on the platform.
[REQ-2.5.13.0.1]	Platform	Security and Common Services	Patient Opt-Out	n/a	The ability to action retrospective patient opt-outs from the platform data layers for all tenants

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.2.0.1]	Platform	Data Management, Intelligent Governance and Automation	Lineage	n/a	Support the output of data lineage in an accessible and sharable user-friendly format that provides auditability of data processing and usage through the end-to-end transformation
[REQ-2.4.2.0.2]	Platform	Data Management, Intelligent Governance and Automation	Lineage	n/a	Easily and automatically track data lineage and provenance from source to presentation (along all transformations) to ensure data integrity, quality, management, data quality, fault diagnosis, security and full auditability.
[REQ-2.4.9.0.3]	Platform	Data Management, Intelligent Governance and Automation	Data Modelling	n/a	Quickly, easily and automatically propagate data model changes across tenancies and catalogues (and anywhere else the model is used) in a controlled, governed way in order maintain consistency and compatibility with dashboards, platform apps and the services using them.
[REQ-2.4.9.0.4]	Platform	Data Management, Intelligent Governance and Automation	Data Modelling	n/a	Extend data models within tenancies to accommodate local, regional or national needs. These various models will exist in parallel, providing control and standardization through the central model, while allowing for flexibility, innovation, and extension at regional and local levels
[REQ-2.4.3.0.2]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Support data stewardship through flexible and robust workflows and automated processes that enable the management of data quality

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.1.0.1]	Platform	Data Management, Intelligent Governance and Automation	Metadata management	n/a	Store, measure, report on metadata. Metadata is information about the data, such as data source, data of transaction, CRUD logs, request logs…
[REQ-2.4.1.0.2]	Platform	Data Management, Intelligent Governance and Automation	Metadata management	n/a	Capture and process technical, business and process metadata (metadata management)
[REQ-2.4.8.0.2]	Platform	Data Management, Intelligent Governance and Automation	Compliance	n/a	The ability to actively assess compliance to data, metadata management and Information Governance standards
[REQ-2.4.3.0.3]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Provide visible quality indicators for data sets to reflect the level of checks which have been done and convey the level of confidence there is in the data quality (for data quality assurance), and make this information available in the data catalogue / data dictionary
[REQ-2.4.3.0.4]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Monitor and assess quality of data against standards and expected norms during operation

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.3.0.5]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Alert users and other systems when data standards are not met, reach certain criteria or are trending in a negative direction.
[REQ-2.4.3.0.6]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Implement data quality controls and checks on data being ingested, processed, and shared to protect curated data sets, self-serve capabilities and reports from bad data
[REQ-2.4.3.0.7]	Platform	Data Management, Intelligent Governance and Automation	Active Data Quality	n/a	Implement agreed mechanisms that will optimize data quality and monitor outcomes. This may include profiling, reconciliation, exception management, use of alternative sources for example
[REQ-2.4.8.0.3]	Platform	Data Management, Intelligent Governance and Automation	Compliance	n/a	Facilitate capabilities to be built to NHS accessibility standards for all analytics, including, but not limited to reports, applications, workflow management and dashboards
[REQ-2.3.1.0.1]	Platform	Platform Applications	Distribution	n/a	Enabling platform services (Platform Applications) to be created by third parties and distributed to users
[REQ-2.3.4.0.1]	Platform	Platform Applications	Citizens Invite	n/a	Communicate with a cohort of citizens or patients to encourage them to participate in a clinical Programme using the Patient Comms Interface. Also known as campaign management.
[REQ-2.3.2.0.1]	Platform	Platform Applications	Cohorting	n/a	Group (or cohort) members of the population or patients based on common traits and user definable rules.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.3.5.0.1]	Platform	Platform Applications	Load Balancing	n/a	Match demand for health services with resource availability in different settings. Also known as Demand Management.
[REQ-2.3.10.0.1]	Platform	Platform Applications	Medicine and Equipment Ordering	n/a	Create medicines and medical equipment orders and facilitate end to end order management, including the ordering, stock management and (re)distribution within NHS locations across ICS, Regions or Nationally.
[REQ-2.3.6.0.1]	Platform	Platform Applications	Pathway Management	n/a	Provide views and/or updates to the patient's journey along a clinical pathway, using multiple datasets.
[REQ-2.3.3.0.1]	Platform	Platform Applications	Patient Comms Interface	n/a	Designed to help improve patient communication to be more efficient at each touch point of the patients journey
[REQ-2.3.7.0.1]	Platform	Platform Applications	Remote Monitoring Interface	n/a	Integrate with remote monitoring device services for clinicians to receive and process their patient’s health data.
[REQ-2.3.8.0.1]	Platform	Platform Applications	Scheduling	n/a	Support for scheduling, for example of patient interactions with clinicians or clinical settings.
[REQ-2.3.9.0.1]	Platform	Platform Applications	Supply Chain Management	n/a	Provide a regional and national overview of inventory within care settings, supply chain and supplier stock in order to reduce NHS stock holding and redistribute in times of shortage. Starting with PPE and including other national ordering inventory data thereafter.
[REQ-2.6.1.0.2]	Platform	SDLC	CI/CD Pipeline	n/a	Use industry standard tools to support automated deployment process across a multi tenanted environment.
[REQ-2.6.1.0.3]	Platform	SDLC	CI/CD Pipeline	n/a	Use industry standard tools to support automated testing including the use of repeatable, scripted test scenarios to cover functional, non-functional and security tests.
[REQ-2.6.1.0.4]	Platform	SDLC	CI/CD Pipeline	n/a	Manage and scale the deployment of upgrades and fixes across tenancies in a controlled way to maintain the consistency of service provision.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.6.3.0.1]	Platform	SDLC	DataOps	n/a	Support the use of Reproducible Analytical Pipelines (RAPs) where open, sharable code is version-controlled, can be written using widely-used open-source languages (e.g. Python, R etc.), which can be easily peer-reviewed, and can make use of reusable functions where appropriate, with unit and regression tests predefined, and dependency management included. It should be possible for RAPs to be fully packaged and easily accessible and reusable, with environment management, in a way that allows for continuous integration and continuous development (CI/CD).
[REQ-2.6.3.0.2]	Platform	SDLC	DataOps	n/a	Support and enable out-of-the-box the full lifecycle of data processing / transformation processes (e.g. develop, test, deploy, run, monitor, and modify) within the platform.
[REQ-2.6.5.0.2]	Platform	SDLC	Environment Management	n/a	Efficiently and quickly generate and use realistic, representative synthetic / mock / test data for non-production purposes
[REQ-2.6.3.0.3]	Platform	SDLC	DataOps	n/a	Enable the continual development of the data model, following DevOps / DataOps best practices and processes (e.g. version control, testing, automated deployment), and manage the impact of changes on data as it flows through the system
[REQ-2.6.3.0.4]	Platform	SDLC	DataOps	n/a	Provide a distributed version control system (e.g. Git) so that all developers involved in the development and operations processes have a full copy of the code and its history.
[REQ-2.6.3.0.5]	Platform	SDLC	DataOps	n/a	Support multiple programming languages (e.g. SQL, Python, R etc.) within DataOps and Orchestration services.
[REQ-2.6.3.0.6]	Platform	SDLC	DataOps	n/a	Provide a configurable automated testing framework that covers Code Quality/Accessibility, Unit, Functional, Progression Testing (new features), Regression Testing and Performance Testing. This automated testing framework run as part of the CI/CD pipelines
[REQ-2.6.1.0.5]	Platform	SDLC	CI/CD Pipeline	n/a	Quickly and easily promote changes from lower to higher environments (e.g. from development, to test, to production), with little-to-no manual effort whilst adhering to governance requirements (e.g. reviews and approvals). This must support the overall SDLC, as well as DataOps and MLOps

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.6.5.0.3]	Platform	SDLC	Environment Management	n/a	Start development of new features or changes quickly and easily, with minimal manual effort and minimal setup e.g. creation and preparation of development/test environments, with the appropriate data, git integration, and CI/CD pipelines, should be automated. This must support the overall SDLC, as well as DataOps and MLOps
[REQ-2.6.2.0.1]	Platform	SDLC	DevOps Tooling	n/a	Provide the necessary tooling for IT Development. This includes, but is not limited to, code repositories, testing tools, libraries, security/scanning tools.
[REQ-2.6.2.0.2]	Platform	SDLC	DevOps Tooling	n/a	Allow developers and analysts to use external IDEs and tooling for reusable analytical and/or functional components e.g. PyCharm, VSCode, Rstudio etc.
[REQ-2.5.6.0.1]	Platform	Security and Common Services	Incident Management	n/a	Provide the necessary tooling for service management and integrate with existing tooling (which is currently federated across many organisations) as appropriate. This includes service repositories, risk management tools and incident management tools.
[REQ-2.5.10.0.1]	Platform	Security and Common Services	Knowledge Management	n/a	Gather, store, browse and share documentation in a manageable way. This documentation will cover the system, the code, the data, and any relevant information for both users and support teams.
[REQ-2.4.13.0.6]	Platform	Data Management, Intelligent Governance and Automation	Tenancy Management	n/a	Support the deployment of new/updated services and products (data models, analytical solutions, platform applications) across defined Tenant(s)
[REQ-2.6.5.0.4]	Platform	SDLC	Environment Management	n/a	Establish and Manage Environments in line with Environment Strategy (Dev, Test, non-Prod and Prod), ensuring integration with CI/CD pipelines and associated triggers (e.g. Pull Requests etc.)
[REQ-2.7.2.0.1]	Platform	FDP Overall	Architecture Principles	n/a	Security and Privacy by Design - Build robust data security from the ground up to ensure data risk, cyber risk and data privacy are integrated into the fabric of the platform and supporting service
[REQ-2.1.5.3.1]	Platform	Data Platform	Application Building	Page Builder	Ability to build web pages that support the navigation, context and descriptions of analytical solutions and Platform Applications

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.4.12.0.3]	Platform	Data Management, Intelligent Governance and Automation	Data Archival and Record Management	n/a	The ability to implement and manage data lifecycle policies across the platform
[REQ-2.5.5.0.1]	Platform	Security and Common Services	Key Management	n/a	FDP must provide the ability to manage (create, exchange, store, replace and destroy) cryptographic keys
[REQ-2.5.6.0.2]	Platform	Security and Common Services	Incident Management	n/a	Provide services that allow incidents to the logged, tracked and resolutions shared
[REQ-2.5.7.0.1]	Platform	Security and Common Services	Monitoring and Alerting	n/a	The ability to measure and report on performance, health and usage metrics, or specific events and raise alerts when certain criteria are met.
[REQ-2.5.8.0.1]	Platform	Security and Common Services	Change Management	n/a	The ability to plan and manage the schedule of new releases to avoid system conflicts and track impact across one or many tenants. All changes must be logged, and a history of change must be kept.
[REQ-2.5.10.0.2]	Platform	Security and Common Services	Knowledge Management	n/a	create and maintain a curated open library of code and methods, with adequate technical documentation, for common and rare analytic tasks
[REQ-2.5.11.0.1]	Platform	Security and Common Services	Disaster Recovery	n/a	Disaster recovery options must be regularly tested.
[REQ-2.5.12.0.9]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide the capability to create and assign custom tags to resource workloads to support configurable hierarchies and usage/cost breakdowns.
[REQ-2.6.5.0.5]	Platform	SDLC	Environment Management	n/a	The ability to embed Security Controls into the Development and Operations lifecycle, to minimise the risk of security breaches, whilst allowing development to continue at a reasonable pace.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.7.2.0.2]	Platform	FDP Overall	Architecture Principles	n/a	Scalable and Cost Effective- Right-sized architecture & embed cost efficiency to support existing workload and adoption size with embedded capability to scale effectively to meet future growth ambitions. It is expected that where Trusts don't require analytical solutions or products from the FDP Tenant it is anticipated that a tenant is still provided to support the National flow of data for statutory duties. The Tenant must have the capability for adoption of products and analytical capabilities in the future.
[REQ-2.7.2.0.3]	Platform	FDP Overall	Architecture Principles	n/a	Relentless Focus on Automation– Apply intelligent automation to replace manual tasks across development, test, deployment and support processes.
[REQ-2.7.2.0.4]	Platform	FDP Overall	Architecture Principles	n/a	Modular and Flexible Architecture- Design services for modularity and re-usability to support independence in components and services.
[REQ-2.7.2.0.5]	Platform	FDP Overall	Architecture Principles	n/a	Lean Operations – Enable shared services that drive scale and operational efficiency without heavy reliance on a central team
[REQ-2.7.2.0.6]	Platform	FDP Overall	Architecture Principles	n/a	Federated Multi-Tenant Architecture–Support multi-tenant deployment model that enables the federation of data services to support NHS England centrally, as well as NHS Bodies.
[REQ-2.7.2.0.7]	Platform	FDP Overall	Architecture Principles	n/a	Frictionless Data and Code Sharing– Data and code sharing across tenants should be seamless and adhere to all security and privacy constructs.
[REQ-2.7.2.0.8]	Platform	FDP Overall	Architecture Principles	n/a	Support Analytical and Operational Workloads–Enable the development and execution of both analytical and operational workloads.
[REQ-2.7.2.0.9]	Platform	FDP Overall	Architecture Principles	n/a	Deliver at pace–Provide established frameworks and services to accelerate innovation and the agile development of products from ideation to productionised services
[REQ-2.7.2.0.10]	Platform	FDP Overall	Architecture Principles	n/a	Comprehensive Integration Patterns– Provide a comprehensive suite of standardized integration patterns/services to allow the optimal integration mechanism to be selected for systems across the NHS landscape.
[REQ-2.7.2.0.11]	Platform	FDP Overall	Architecture Principles	n/a	Intuitive and Accessible Platform Services – The Data Platform should support multiple technical and non-technical user personas by providing both code and low-code services. Platform service should also comply with accessibility standards.

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.7.2.0.12]	Platform	FDP Overall	Architecture Principles	n/a	Establish an Open Platform – Adopt industry standards to enable interoperability and minimise vendor lock-in. The Data Platform will be required to support use cases developed and delivered by other providers.
[REQ-2.1.1.9.1]	Platform	Data Platform	Integration Services	PET Integration	The Data Platform must have the ability to call PET API to invoke a defined privacy treatment on specified data
[REQ-2.1.1.9.2]	Platform	Data Platform	Integration Services	PET Integration	The Data Platform must have the ability To receive treated data from PET
[REQ-2.1.1.9.3]	Platform	Data Platform	Integration Services	PET Integration	The Data Platform must have the ability to call PET API to reidentify and reinsert sensitive data into treated data.
[REQ-2.1.1.9.4]	Platform	Data Platform	Integration Services	PET Integration	FDP must support the secure transfer of data to and from the PET solution. These services must also support structured and semi-structured data in batch, micro batch, and streaming mode.
[REQ-2.5.2.0.1]	Platform	Security and Common Services	Data Protection	n/a	Support Encryption (e.g. 256-bit AES encryption) of Data at-Rest and in-Transit across all services withing the platform.
[REQ-2.5.3.0.1]	Platform	Security and Common Services	Data Control	n/a	Provide fine-grain access control to data across the platform based on PBAC and RBAC attributes and roles maintained by the IDAM solution
[REQ-2.5.5.0.2]	Platform	Security and Common Services	Key Management	n/a	FDP must provide the ability for the NHS Organisations to manage their own cryptographic keys i.e. Customer Managed Keys, using a 3rd party Key Management System (KMS)
[REQ-2.5.7.0.2]	Platform	Security and Common Services	Monitoring and Alerting	n/a	The ability to integrate configurable alerting functionality into orchestration and workflows based on events or thresholds, in order to provide a comprehensive monitoring and alerting service for orchestration and workflows.
[REQ-2.5.8.0.2]	Platform	Security and Common Services	Change Management	n/a	The ability to rollback from released changes across tenants. Various release patterns should be possible (canary, blue-green …).
[REQ-2.5.8.0.3]	Platform	Security and Common Services	Change Management	n/a	The ability to support various release patterns incl. canary, blue-green deployments

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.5.11.0.2]	Platform	Security and Common Services	Disaster Recovery	n/a	The disaster recovery services must be configured to support the RPO and RTO service levels defined in the <<FDP Service Catalogue document>>
[REQ-2.5.12.0.10]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide elastically scalable platform services to support the scale up/down in accordance with workload demands
[REQ-2.5.12.0.11]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide configurable consumption/cost thresholds for each Tenant that will raise alerts when thresholds are broken
[REQ-2.5.12.0.12]	Platform	Security and Common Services	Cost and Capacity Management	n/a	Provide configurable consumption/cost Cap threshold for each Tenant that will prevent cloud spent from excessing a predefined value in order to prevent overspend
[REQ-2.5.12.0.13	Platform	Security and Common Services	Cost and Capacity Management	n/a	The supplier shall provide self-service reporting access to the Authority which provides views of underlying cloud costs by tenant and product.
[REQ-2.5.12.0.14]	Platform	Security and Common Services	Cost and Capacity Management	n/a	The supplier shall provide self-service reporting access to the Authority which provides views of usage by tenant, user and product, which includes but is not limited to when did users last access a product/tenant, how many users are using a product, how many users are logged into a tenant, volume of data within a tenant by product and purpose.
[REQ-2.5.13.0.2]	Platform	Security and Common Services	Patient Opt-Out	n/a	The ability to call a national opt out service to ensure data relating to patients that have opted out is not Ingested into FDP
[REQ-2.7.1.0.13]	Platform	FDP Overall	Standards and Frameworks	n/a	Comply with "Reproducible Analytical Pipelines" (RAP, a set of best practices and training created in GDS and ONS)
[REQ-2.1.1.2.5]	Platform	Data Platform	Integration Services	API Integration	Create and Publish a Suite of Rest API services that enable programmatic interaction with Data Assets, Platform Services and Products (Analytic Solutions and Platform Applications)
[REQ-2.3.11.0.3]	Platform	Platform Applications	n/a	n/a	Platform Applications must be built on top of an API layer that connects to the canonical data model rather that use-case specific data models. This is to maximise the ease of reuse of applications across end user organisations

UUID	Capability Type	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)
[REQ-2.7.1.0.14]	Platform	FDP Overall	Standards and Frameworks	n/a	The FDP will enable, and must apply, secure data environment policy for any use of NHS health and social care beyond direct patient care. Secure data environment for NHS health and social care data - policy guidelines - GOV.UK (www.gov.uk)
[REQ-2.6.4.0.9]	Platform	SDLC	MLOps	n/a	The Data Platform must provide a feature store capability that allows calculated features to persistent in order to support the sharing and reuse of ML models across environments

UUID	Capability Type	Level 1	Requirement (Must / Ability to…)
[REQ-F93FB2]	Information Governance	Common Law Duty of Confidentiality (CLDOC)	Ensure the maintenance of the Common Law Duty Of Confidentiality and apply measures proportionate to the data as defined in the Data Protection Act 2018 / UK GDPR
[REQ-12C35D]	Information Governance	Compliance	Hold, and demonstrate, valid certifications in: •Data Security Protection Toolkit •Cyber Essentials plus •ISO 27001 + 27017
[REQ-8A72F1]	Information Governance	Compliance	Effectively manage information incidents/ breaches in line with the FDP Breach Management Procedure
[REQ-019E3F]	Information Governance	Compliance	Identify and inform the controller, when data is being processed outside the UK, ensuring that any country where data is being processed, is on the approved list and have agreed controls in place to ensure that data is processed in alignment with UK data protection legislation
[REQ-E8124D]	Information Governance	Compliance	Address the following functional, more health specific, lawful requirements: •Subject Access Requests (SARs) •Freedom of Information (FOIs) •National Data Opt Out for secondary use purposes •Right to Object Upheld

UUID	Capability Type	Level 1	Requirement (Must / Ability to…)
	Information Governance	Data Protection Act 2018 / UKGDPR	Follow and adhere to specific processing instructions by the identified Data Controllers. Note: the Supplier will be categorised as a Data Processor. The appropriate basis for processing personal data that is available to statutory health and social care organisations in the delivery of their functions are: •Article 6(1)(c) •Article 6(1)(e) •Article 9(2)(h) •Article 9(2)(i) •Article 9(2)(j) •Data Protection Act 2018, Schedule 1 •Consent may be used as a lawful basis for research when the above lawful bases cannot be applied: oArticle 6(1)(a) oArticle 9(2)(a) This applies to, at least, all activities of the supplier and users, and all components of the platform including (but not limited to): data ingestion, data storage, data processing, data cataloging, data science and advanced analytics, analytical solutions, platform applications, publishing.
[REQ-47DB15]	Information Governance	DPIA	Participate in and support the DPIA process of completing the necessary IG documentation
[REQ-836397]	Information Governance	DPIA	Data is to be held under the explicit instruction of the identified data controller for either the length of the contract or for the period detailed within the DPIA for the individual product. At the end of the contract data should either be returned to the data controller or with the issuing of a destruction certificate, this will be on explicit instruction of the data controller.

UUID	Capability Type	Level 1	Requirement (Must / Ability to…)
[REQ-81AF93]	Information Governance	FDP Overall	Achieve good data governance for all data types within the Data Platform by ensuring the following controls are implemented: •Appropriately defining identifiable, sensitive, special category data for all data types ensuring appropriate access controls can be implemented based on the user's privilege levels. •Data classification for all data types including the use of metadata •Ensuring an understanding of data states with appropriate security (data at rest / data in transit / data in use) •Compliance requirements are met (DPA 18/UKGDPR) •Following the agreed IG approval process for all new data flows which will include completion of DPIA's, approved by all parties
[REQ-675B98]	Information Governance	FDP Overall	Adhere to the Information Governance (IG) approach, guided by the '5 Safes' Framework
[REQ-42C804]	Information Governance	FDP Overall	Suppress small outlying data groups from exported datasets and information made available is analytic reports
[REQ-391CE0]	Information Governance	FDP Overall	Data lineage can be used to show full context of data management, including source of data, full version history of the data, data aggregation rules, quality of datasets and end-to-end transformation.
[REQ-B9AD29]	Information Governance	FDP Overall	Capability for users to provide feedback and comment on suitability, accuracy and usability.
[REQ-C5E07B]	Information Governance	FDP Overall	Data modelling techniques implemented into ingestion processes should include relational techniques, data relationship modelling, hierarchical modelling and object modelling.
[REQ-16CF8F]	Information Governance	FDP Overall	The lifecycle of "Corporate Records" related data and information used in FDP should conform with "NHS England Corporate Records Retention and Disposal Schedule"
[REQ-3F7474]	Information Governance	FDP Overall	The lifecycle of "Primary Care Services" related data and information used in FDP should conform with "NHS England Primary Care Services records retention schedule"

UUID	Capability Type	Level 1	Requirement (Must / Ability to…)
[REQ-B8DBC5]	Information Governance	Technical Security Requirements to meet Data Protection Act 2018/UKGDPR	Ensure PET works across any and all FDP tenancies: (i)all data ingested to the Data Platform would have its metadata captured through PET; (ii)data uses (e.g. direct care, secondary uses) across Tenants would call PET, and; (iii)data uses (e.g. direct care, secondary uses) within a Tenant would call PET, however; (iv)direct care uses within a tenant may have little or no privacy treatments applied (depending on context and purpose, as directed by the Data Controller); (v)it follows that the Data Platform would control treatment of data and audit uses in conjunction with PET, and PET would audit all changes of data usage / purpose; (vi) and that PET will demonstrate which privacy controls have been applied to any dataset in any tenant. For example, the PET solution will understand the source of data, what policies (instructions) have been applied and where data has been sent (ie tenant x). FDP will understand which users have accessed the data. In cohesion, the PET solution and FDP will understand the complete picture.
[REQ-D1A503]	Information Governance	Technical Security Requirements to meet Data Protection Act 2018/UKGDPR	Demonstrate how you will implement, in a secure and compliant way, the following scenario: there may be instances where processing may span multiple sources based on different tenants (data sources in different clouds and on-premises)
[REQ-79C0F5]	Information Governance	Technical Security Requirements to meet Data Protection Act 2018/UKGDPR	Adhere to the established data privacy principles across FDP as a whole, including: 1.Records are protected by encryption 2.Records are joined & associated using a consistent and person-unidentifiable key 3.Technical controls should not compromise data integrity 4.Records are exchanged encrypted 5.Data types might use differing encrypted 6.Summary information & stats are supported by PET 7.Data translation to legacy can break/change crypt protections solely for legacy 8.Decryption happens only at point of uses

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-2849BC]	Encryption Management	Prove your identity to the satisfaction of the certificate authority to obtain digital certificates
[REQ-B9E65D]	Encryption Management	Obtain digital certificates to provide assurance that the communication with data source provides is who they claim to be
[REQ-1C6F17]	Encryption Management	Integrate with or provide a Public Key Infrastructure (PKI) to provide a single mechanism to securely manage and use cryptographic keys.
[REQ-D38E59]	Encryption Management	Have public key infrastructure (PKI) and security governance framework that manages the overall approach to the management of the PKI and information within it. Examples of this governance include: •Clearly identified board representative who are responsible for the security of the PKI service. •A documented framework for security governance, with policies governing key aspects of information security relating to the PKI. •Security and information security should form part of the service provider’s financial and operational risk reporting procedures. •Processes to identify and ensure compliance with applicable legal and regulatory requirements.
[REQ-F6D00A]	Encryption Management	Develop and implement through their whole lifecycle, a policy on the use, protection and lifetime of cryptographic keys.
[REQ-26EBD5]	Encryption Management	Seamlessly and transparently to the user, based on their persona, conduct key management, especially for data encryption within the data stores
[REQ-6ADC22]	Encryption Management	Develop a policy on the use of cryptographic controls for protection of information as part of the your design process, and implement at the start of the programme.
[REQ-84F4A4]	Encryption Management	Carefully protect your own private keys to preserve your trust relationships. Suppliers should align with existing NHS England public key infrastructure (PKI) policies and procedures which may include use of current NHS England Certificate providers
[REQ-8237BB]	Encryption Management	Authenticate all clients to server communications using mutual TLS (mTLS) supported by PKI.
[REQ-0B643C]	Encryption Management	Adhere to strict controls on data confidentiality and must implement ciphers as stipulated by the NHS England Security Operations team

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-DF56B2]	Incident Management	As part of the service, we would expect the successful participant to provide their own capability for logging and monitoring of security events/incidents. We would require the NHSE CSOC to be notified of any high severity incidents to enable our own CSOC to provide incident response support and assess the potential impact of an incident on NHSE systems. The type and severity of incidents we would require notification of can be agreed with the CSOC as part of the FDP service onboarding. There would also be the requirement for a regular cadence of reporting of security incidents and responses to the NHSE FDP Programme. As part of the service we expect the supplier to be responsible for identifying log requirements and creating use cases to deliver their own SOC capability. NCSC provide good guidance on this Building a Security Operations Centre (SOC) - NCSC.GOV.UK The advised log retention period for security logs from NCSC is 6 months.
[REQ-0DD020]	Incident Management	Work closely with NHS England Cyber Security teams to ensure vulnerabilities are managed, compliance is maintained, and risks are appropriately mitigated
[REQ-107BD3]	Incident Management	Report all tier 1 and tier 2 incidents and outages to NHS England service managers with the contractual timescales. All communication shall be via agreed methods
[REQ-E22514]	Incident Management	Establish supplier management teams responsibilities and procedures to ensure an effective and timely response to information security incidents related to NHS England systems and services.
[REQ-9E5835]	Incident Management	Ensure that NHS England Security Operations and Information Governance teams are notified of all breaches that impact their services and data with 2 hours of a breach being identified
[REQ-BF19E7]	Incident Management	Ensure procedures for responding to information security incidents related to NHS England systems and services are documented
[REQ-197C5A]	Incident Management	Ensure information security events are reported through appropriate management channels as defined in Service Level Agreements (SLA's) and the FDP specific, Breach Management Procedure
[REQ-F1E8E6]	Incident Management	Ensure employees and contractors using the supplier's information systems and services note and report any observed or suspected information security weaknesses in systems or services. NHS England Security teams could also identify and raise security weaknesses with the supplier, who is expected to respond and remediate as required
[REQ-A91D64]	Incident Management	Ensure a lessons learnt process is in place to ensure knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents
[REQ-65BCED]	Incident Management	Define and apply procedures for the identification, collection, and preservation of information, which can serve as evidence in the event of a data breach

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-653957]	Incident Management	Assign service managers to NHS England services, who are responsible for engaging with NHS England service managers on services provided
[REQ-2D3274]	Incident Management	Assess information security events and security incidents to decide if they are to be classified as information security incidents. Example security incidents include the following: •Unauthorised attempts to access systems or data •Privilege escalation attack •Insider threat •Malware attack •Denial-of-service (DoS) attack •Man-in-the-middle (MitM) attack
[REQ-2B0A43]	Incident Management	Adhere to the FDP Breach Management Procedure
[REQ-1E8FAA]	Incident Management	Adhere to NHS approved incident Management Policy
[REQ-3353B2]	Incident Management	Adhere to NHS approved incident Management Policy
[REQ-68DF0C]	Information Security Compliance	Ensure the privacy and protection of personally identifiable information and protected health information is safeguarded as required in relevant legislation and regulation
[REQ-35A4DB]	Information Security Compliance	Ensure that the supplier’s approach to managing information security is independently reviewed at planned intervals or when significant changes occur to their systems and services.
[REQ-D511DE]	Information Security Compliance	Ensure that supplier management teams regularly review the compliance of information processing and procedures within their area of responsibility to ensure they are aligned with the appropriate security policies, standards, and any other security requirements
[REQ-8B6BDB]	Information Security Compliance	Ensure that supplier information systems are frequently (minimum annual) reviewed for compliance with their information security policies and standards
[REQ-9A5DD3]	Information Security Compliance	Ensure NHS England records and data are to be protected from loss, destruction, unauthorised access, and unauthorised release, in accordance with contractual obligations and supplier policies
[REQ-C8D28F]	Information Security Compliance	Ensure cryptographic controls are implemented in compliance with all relevant agreements, legislation, and regulations
[REQ-74DC9C]	Information Security Compliance	Ensure appropriate procedures are implemented to ensure intellectual property rights and use of proprietary software products follow legislative, regulatory, and contractual requirements

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-05E168]	Information Security Compliance	Ensure all information system and services storing and processing NHS England data are kept up to date with the relevant legislative, regulatory, contractual requirements and the supplier approach to meet these requirements is identified and documented
[REQ-BAE505]	Information Security Compliance	Manage (create, exchange, store, replace and destroy) cryptographic keys.
[REQ-B1B84A]	Information Security Compliance	The FDP solution should be able to use cryptographic Customer Managed Keys with the use of 3rd party cryptographic Key Management Systems/Services (KMS)
[REQ-45590D]	Infrastructure Security	Use testing automation tools to identify and mitigate against vulnerabilities
[REQ-668596]	Infrastructure Security	Use an NHS England approved scanning tool to conduct monthly vulnerability assessments and monitor by approved personnel
[REQ-742DE8]	Infrastructure Security	Ensure no confidential NHS England information (personal identifiable information/protected health information) is transmitted using electronic messaging (e-mail). Transfer of contractual / financial documents should be password protected, with the password transmitted via an alternative communication channel to the e-mail. All system-to-system communication must adhere to the communication standards outlined in this document
[REQ-4CADC9]	Infrastructure Security	Segregate information services, users, and information systems on their networks services
[REQ-4E80A7]	Infrastructure Security	Run vulnerability assessments on new critical systems before deploying them into the infrastructure network and after any significant changes to the infrastructure

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-5333F2]	Infrastructure Security	Provide threat modelling reports to NHS England CISO and stakeholders 6 monthly or when requested for visibility of threat intelligence, asset identification, risk assessments and threat mapping. Threat modelling should follow the identification of: •key assets •potential threat actors •entry points •components within the kill chain •use cases •trust levels identifying a list of top threats based on vulnerability assessments. For each threat (in order of priority), identify mitigations actions, which may include implementation of specific security control. Create and review a risk matrix to determine if the threat is adequately mitigated. Document the threats and review periodically
[REQ-F642C1]	Infrastructure Security	Provide SOC2 audit reports to NHS England CISO and stakeholders when requested for visibility of Information security audits providing assurance of privacy controls, confidentiality / integrity / availability of data. SOC2 reports must be provided at bidding stage and provided upon change to the report
[REQ-B50D46]	Infrastructure Security	Produce a report from each vulnerability assessment to address: - Vulnerabilities found. - Remediation steps. - Results from mitigation controls or risk acceptance. - Any exceptions, including false positives or vulnerabilities that cannot be fixed, must be explained. Reports and data from vulnerability scans must be treated as confidential
[REQ-1D1BEC]	Infrastructure Security	Ensure their production networks supporting the FDP solution are managed to protect the confidentiality, integrity and availability of NHS England data. Non-production environment will be required to adhere to the same controls as production, with no production data within these environments
[REQ-1AE7F5]	Infrastructure Security	It is expected that access to production data is limited for the FDP-AS supplier using role specific priviledged accounts

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-0E619A]	Infrastructure Security	It is expected that MFA and approved methodologies are enforced for priviledged access to production systems.
[REQ-4BDF04]	Infrastructure Security	Ensure all production and non-production environments must be hosted within the UK region. Development access to non-production environments must be from within the European Economic Area (EEA)/ European Union (EU) regions only. Exceptions to development in these regions must be formally agreed with NHS Corporate IT. These development environments must not contain any NHS England patient data
[REQ-6AA4BA]	Infrastructure Security	Ensure all NHS England systems and services have a fully formed disaster recovery plan to ensure the availability and integrity of data is always maintained. A draft plan must be provided by the bidder for NHS England review
[REQ-0BAC58]	Infrastructure Security	Ensure agreements outline the secure transfer of NHS England information between all parties
[REQ-8FE5AB]	Infrastructure Security	Confirm service levels and management requirements of all network services have been identified and included in network services agreements
[REQ-598A03]	Infrastructure Security	Carry out vulnerability scanning monthly using a suite of automation tools with reports being shared with NHS England upon request
[REQ-0ACC54]	Infrastructure Security	Be in accordance with NCSC best practices for security patch management. These best practices include: •Patches should be tested to ensure they do not impact the system •Processes should be in place for urgent patching, outside of normal patch cycles •Patches should be cryptographically signed by the supplier and verified before application •Mechanisms should be in place to identify vulnerabilities in third party libraries and produce tested security patches
[REQ-859043]	Infrastructure Security	Agree to NHS England non-disclosure agreements for the protection of information within NHS England systems and services and should be regularly reviewed.
[REQ-159E5A]	Infrastructure Security	Adhere to NHS England Information Sharing Policy to protect the confidentiality of information with all types of communication mechanisms
[REQ-9FB76D]	Infrastructure Security	Follow the Change Control Procedure, particularly on occassions where some internal vulnerability scans may require firewalls to allow certain IP addresses to access specific environments
[REQ-1D89D6]	Organisational Factors	Provide a generic phone number and have a monitored mailbox available providing 24/7/365 contact and support
[REQ-B01DE3]	Organisational Factors	Nominate a security liaison team with a designated lead individual (SPOC) for coordinating security activities.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-48082D]	Organisational Factors	Ensure supplier resource teams are not be located on any current hostile environments
[REQ-88FFD7]	Organisational Factors	Ensure production system access is restricted to onshore resource only.
[REQ-67C604]	Organisational Factors	Ensure policies and procedures with supporting security measures are implemented to protect NHS England systems and services being accessed at teleworking sites.
[REQ-A92318]	Organisational Factors	Ensure non-production system access does not contain any production data and can be accessed from near shore and off shore resource.
[REQ-E91DC3]	Organisational Factors	Ensure information security is addressed within the project development life cycle
[REQ-73A6B9]	Organisational Factors	Ensure conflicting duties and areas of responsibility are separated to prevent unauthorised or unintentional modification to NHS England systems and services
[REQ-024B0B]	Organisational Factors	Ensure appropriate contacts with relevant authorities are established and maintained
[REQ-2AD6AB]	Organisational Factors	Ensure appropriate contacts with relevant associations are established and maintained. These include the following: •Information Commissioners Office (ICO) •Law enforcement agencies •National Cyber Security Centre •Any additional organisations as dictated by NHS during the life of the contract NHS England Contact will include: •NHS Information Governance •NHS Cybersecurity •NHS Fraud
[REQ-4DBE93]	Organisational Factors	Ensure all information security responsibilities are defined and allocated to appropriate resource.
[REQ-3CF9C8]	Personnel Management	Requirement for technical staff to meet with NHS security process prior to working on the FDP, and this may vary dependent on the role being fulfilled
[REQ-707AD9]	Personnel Management	Ensure that supplier staff who have access to personal identifiable data (PII) or protected health information (PHI), complete information security and awareness training. The training content is required to be reviewed and approved by NHS Information Governance team, who may also audit training and awareness programmes

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-F61A27]	Personnel Management	Supplier's staff must complete IS and awareness training and have BPSS clearance if they have access to non-production environments.
[REQ-D1EC73]	Personnel Management	Unless otherwise agreed with the Authority, Supplier's staff must complete IS and awareness training and have SC clearance if they have access to production envronments, PID, or PHI.
[REQ-8FE1D8]	Personnel Management	Ensure supplier personnel working on NHS England systems and services have the right to work in the UK, with the appropriate documentation to confirm eligibility (Passport / Visa / Work Permit)
[REQ-74781E]	Personnel Management	Ensure personnel have stipulated their full employment history within the application form and highlighted any employment gaps. References should be verified covering a minimum of 3 years from the current employer and previous employers
[REQ-256EF5]	Personnel Management	Ensure management follow the principle of Least Privileged access in relation to the joiners and movers within the supplier's organisation. This would include scheduled user access audits
[REQ-698230]	Personnel Management	Ensure formal and communicated disciplinary processes are implemented to act against employees who have caused an information security breach
[REQ-144FF9]	Personnel Management	Ensure employees and contractors have their access to NHS England systems and services terminated at the end of their employment and/or reviewed at point of changing responsibilities
[REQ-75CB4A]	Personnel Management	Ensure contractual agreements with suppliers state their responsibilities for information security
[REQ-55EF24]	Personnel Management	Ensure all personnel working on NHS England systems and services are subject to satisfactory disclosure from the Disclosure and Barring Service (DBS check)
[REQ-DED814]	Personnel Management	Ensure all employees and contractors accessing NHS England systems and services adhere to information security controls in accordance with their policies and procedures
[REQ-6213AE]	Personnel Management	Ensure all employees and contractors accessing NHS England systems and services receive appropriate awareness education and training relevant for their job function
[REQ-FAF147]	Personnel Management	Conduct background checks on all applicants for employment who access NHS England systems and services, in accordance with UK regulations and are proportional to the classification of the information being accessed
[REQ-E30629]	Risk Management	Have a mature risk management process with the following activities: •Context establishment •Risk identification •Risk analysis •Risk evaluation •Risk treatment

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-179842]	Risk Management	Ensure risks are scored using a defined impact and likelihood matrix, logged in a risk register and reviewed periodically. Critical and High impact risks will be reviewed more frequently
[REQ-BE1D0F]	SDLC	Use and automatically apply threat modelling when designing and deploying applications, including those for the Marketplace.
[REQ-6EE971]	SDLC	Include NCSC 8 Principles of Secure Development & Deployment. (E.G. Secure Development, Secure Environments, and Protect Code repositories) in the secure coding practices of the platform. [https://github.com/ukncsc/secure-development-and-deployment/]
[REQ-A60AE0]	SDLC	Embed Security Controls into the Development and Operations lifecycle, to minimise the risk of security breaches, whilst allowing development to continue at a reasonable pace.
[REQ-28ADF9]	Secure by Design	Adhere to NHS requirements on Secure by Design
[REQ-5BF696]	Security	Retain an audit trail history in a secure environment and with the ability to search and trace events, for 7 years or as long as stated in NHS data retention policies and data disposal schedules (which may vary depending on use cases).
[REQ-2E3556]	Security	Provide CRU(D) event logging for FDP, platform applications and other services in order to provide accountability and traceability of user actions and support complex defect tracing an a multi component environment.
[REQ-64497C]	Security	Have a record of all interactions and events that occur on the platform which includes information on who performed the action and when. The logs cannot be altered or interfered with. This must support governance, auditing (to support SOC2 reports), and forensics needs.
[REQ-8446F7]	Security	Facilitate audit capability to track source database activity to track data usage, user access/authentication for identify security violations and network activity for better configuration of its' resources
[REQ-0E7E2A]	Security	Build-in a full audit trail, for DevOps operations for all system components for each event, including as a minimum; user identification, type of event, date and time, success or failure indication, error details, the origin of the event, and identity or name of affected data, system component or resource.
[REQ-6294ED]	Security	Apply a consistent audit framework and fine-grained security model to safeguard all integrated data from day-one (go-live), whilst minimising custom-code configurations and over-reliant use of proprietary software.
[REQ-31D714]	Security	Create and maintain release notes and known defects within each deployed component
[REQ-2F160C]	Security	Create and maintain a historical record of changes to configuration items deployed into each tenancy
[REQ-4E99AB]	Security	Comprehensively control and manage the development and deployment of coded components (e.g. SDLC) to accommodate the different pace of technology evolution across tenancies.
[REQ-C96E36]	Security	Run SDLC processes that mitigate against OWASP Top 10 vulnerabilities.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-0AEAEA]	Security	Maintain and implement a clear plan for the protection of the FDP platform against malicious cyber attacks from internal and external sources; provide protective measures to counteract and avoid propagation of attack across the estate.
[REQ-ECD5FA]	Security	Enforce the use of encryption and network traffic protocols to ensure data packets are transmitted safely across the NHS IT estate (e.g. AES, SHA, TLS, HTTPS, SFTP, etc).
[REQ-41C1CD]	Security	Design, share and implement a clear plan outlining how to securely configure proxy servers and avoid exposing unencrypted endpoints
[REQ-AEDE53]	Security	Protect computing, network, and storage infrastructure
[REQ-F9D361]	Security	Design, maintain and apply a clear plan outlining Intrusion Detection and Protection (IDS/IPS) at the network and/or host level.
[REQ-C566D6]	Security	Use commercial grade encryption as a minimum when data transmitted across public and cloud infrastructure (TLS)
[REQ-792A08]	Security	Support implementation of easily configurable archiving policies to optimise the amount of data retained on-line and the cost associated with it.
[REQ-120FEC]	Security	Support FOI requests though the ability to uphold the requirements of the Freedom of Information Act 2000
[REQ-869D16]	Security	Support easily configurable data retention policies can comply with NHS Record Management Code of Practice but allow flexibility for the FDP to define extended retention times where historical data is of interest.. (https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/)
[REQ-197E7D]	Security	Store data only in UK locations / availability zones i.e. prevent data being stored outside the UK
[REQ-BF36A4]	Security	Securely segregate NHS FDP data from that of other organisations or customers of the supplier.
[REQ-247F29]	Security	Manage identified data used for secondary use in accordance with the national opt-out requirements.
[REQ-1170AC]	Security	Maintain a clear logical separation between data associated with different Purposes especially when it is governed by UK GDPR / DPA 2018.
[REQ-893713]	Security	Implement data loss prevention measures to ensure data is monitored, classified, protected (rest/motion/use) and accessible during its lifecycle.
[REQ-B8AB34]	Security	Host the solution only in UK locations / availability zones e.g. prevent data being processed outside the UK
[REQ-C90E0A]	Security	Encrypt data at rest. (e.g. 256-bit AES encryption)
[REQ-D59360]	Security	Encrypt at all times any data held on a mobile device within an application developed for the Marketplace.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-EC1D50]	Security	Demonstrate that the FDP and its platform applications and services provide compliance with best practice for security and authorisation of APIs (https://digital.nhs.uk/developer/guides-and-documentation/security-and-authorisation).
[REQ-1E9C2C]	Security	Protect data at rest, in transit and in use.
[REQ-EFDDAA]	Security	Access data only from within UK geographies i.e. prevent data being accessed outside the UK
[REQ-010BA0]	Security	Restore the service within 2 hours (RTO).
[REQ-B6F077]	Security	Plan a maximum of 4 agreed and planned outages per year requiring 2 weeks' notice and 6 short notice emergency changes per year.
[REQ-3B05F1]	Security	Limit the data loss to a maximum of 1 hour data of operation (RPO). Take all reasonable steps to ensure that it is recoverable from cached, mirrored or temporary data stores
[REQ-9CA382]	Security	Provide tooling to support the security management and allow administrators to be alerted, capture and manage operational issues while maintaining system security.
[REQ-C9BF55]	Security	Monitor and uphold the content of data sharing agreements in order to ensure that inappropriate or out of scope data is not transferred to sharing organisations.
[REQ-AAA8D6]	Security	Manage access to data through specific "projects". Projects will embody the intended outcomes, access constraints, DPIA and the data scope of the work. They need to apply to data presented in app access mechanisms enabled by the project whether dashboard, platform app, report and so on
[REQ-0584EE]	Security	Integrate with a separately procured component (PET) to enable access and sharing of special category, identifiable personal data, subject to UK GDPR / DPA2018 within FDP in privacy-preserving manner for data analytics
[REQ-C51D7D]	IDAM	The Successful Supplier must be able to manage multiple approaches to SSO/authentication which differs across the NHS estate, an example of one approach is NHS smartcards. The implementation approach to SSO will be worked through with the Successful Supplier during the mobilisation period.
[REQ-81AC78]	Security	Support dataset level, record-level, field-level and cell-level security through PBAC, so that permission on certain data can be Purpose specific and limited to only those who should see it. It must also be possible to manage and grant authorisations within tenants and across tentants as needed e.g. at a local, regional, or national level. For example the underlying platform data includes linked data for a range of care settings, but a defined Purpose may be restrict access to only allowing access to parts of records for a sub-set of settings.
[REQ-8BE418]	Security	Provide, implement and enforce authentication via Identity & Access Management (IAM) to provide first line access to FDP based on the user's identity

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-666C63]	Security	Provide, implement and enforce Purpose Based Access Controls (PBAC) to provide authorisation to user to access data and functions, providing a scope for data access, time based access and potentially a second level of role based access within the defined Purpose.
[REQ-9B6F91]	Security	Onboard and offboard organisations and federate or delegate the responsibility of managing the on/off boarding process to different NHS organisations
[REQ-6A1F5B]	Security	Manage user authentication and authorisation within and across tenants from a centralised service.
[REQ-202FE9]	Security	Manage Purposes against an FDP user and provide the users with the ability to select one Purpose at a time with which to authorise access to information (PBAC)
[REQ-F675A9]	Security	Ensure that a user can access only one Purpose at a time across all devices and data from a prior Purpose must be cleared from all device sessions before entering the next one.
[REQ-17B732]	Security	Define a Purpose including all mechanisms and constraints by which data can be viewed or interacted with. So, platform apps, dashboards, reports, analytics and exports all need to function within the Purpose and not stray outside of it. Some situations may require the purpose to be time based. Purposes can be established within a single tenant but also need to extend to cover data and access from more than one tenant
[REQ-4A8377]	Security	Follow the principle of Least Privileged Access when setting up and running IAM and PBAC and ensure that the right individuals have appropriate access to resources
[REQ-A8A7E2]	Security	Demonstrate that the FDP and its platform applications and services provide compliance with GPG44 for use of authenticators to protect on-line services and GPG45 to prove an verify identity.
[REQ-726612]	Security	Demonstrate that the FDP and its platform applications and services provide compliance with DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services to provide consistent and standardised user verification authentication across England. (https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3051-identity-verification-and-authentication-standard-for-digital-health-and-care-services)
[REQ-DBB3CE]	Security	Align to NHS authentication standards and to security principles and policies for users and groups. (GPG44, GPG45, NHSD Security and Authorisation (link in Architecture Appendix section 1.2))
[REQ-08319A]	Security	Accept federated identity from multiple (local, national and others) IAM systems into a central FDP IAM control system.
[REQ-1FAD64]	Security	Provide a practical and secure means of authenticating users that may need to use the system but have no means of using one of the established NHS IAM solutions

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-278B6B]	Security	Implement and enforce Role-Based Access Control (RBAC) at different levels of the system, according to context. Once authenticated, the user could be assigned one or more roles at the highest level. These roles provide aggregate access and may provide a basic limitation on data access throughout the system, allowing users access to generally available features and visualisations.
[REQ-0526A1]	Security	Implement and enforce RBAC within a Purpose (PBAC)
[REQ-A3C5D3]	Security	Support incident management processes, raise incidents and be able to integrate with NHSE ITSM tooling that will enable visual monitoring of the FDP Services.
[REQ-EE6264]	Security	Identify system issues when they arrive, mitigate them and solve the root cause. Incidents must be logged, and resolutions shared. Pre-emptive capabilities must also be explored.
[REQ-04055C]	Security	Log user events to measure, analyse and report on system usage, user behaviour, health and performance, and raise alerts when certain criteria are met.
[REQ-51DA1E]	Security	Interpret usage data to inform evolution and tuning the architecture, deployment and resource assignment.
[REQ-DF0567]	Security	Identify inactive users disable accounts automatically but also preserving log integrity.
[REQ-7568C0]	Security Operating Model	Comply with the security requirements for a Critical National Infrastructure (CNI) from the outset. These requirements will include aligning to NCSC Cyber Assessment Framework (CAF) and follow guidelines set out in NCSC CNI Assessment Hub
[REQ-F6FA2E]	Security Operating Model	Adhere to a layered security control model. This is required to ensure appropriate levels of security are implemented at every layer and when combined, provide a more secure environment. These layers must be subject to external audit and frequent review of policy, procedure, and controls
[REQ-190A58]	Security Operations Management	Transfer all NHS England data in useable format at the end of the contract or migration at no additional cost
[REQ-310992]	Security Operations Management	Take and regularly test, in accordance with an agreed backup policy, backups of information, software and system images
[REQ-82076A]	Security Operations Management	Protect logging facilities and log information against tampering and unauthorised access
[REQ-313513]	Security Operations Management	Produce, keep, and regularly review in a tamper proof service, event logs recording user activities, exceptions, faults, and information security events. These log files should be made available for incident investigation, response and forensic purposes. The log files should be retained according to NHS England policy
[REQ-3F852E]	Security Operations Management	Maintain identification of NHS England data assets within their environments to support offboarding processes.
[REQ-1F1F24]	Security Operations Management	Have separated development, testing, and operational environments to reduce the risks of unauthorised access or changes to the operational environment.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-67817C]	Security Operations Management	Ensure vulnerability testing is in alignment with 2D. Security Requirements, Vulnerability Assessments
[REQ-648345]	Security Operations Management	Ensure transactional logs are retained in-line with the DSPT assessment. These shall be implemented from the outset.
[REQ-AEE3DA]	Security Operations Management	Ensure there are procedures implemented to manage the installation of software on operational systems
[REQ-0B2A17]	Security Operations Management	Ensure your security operating procedures are documented and made available to all users who require them
[REQ-0E0336]	Security Operations Management	Ensure the use of resources is monitored and forecasting is carried out for future capacity requirements to ensure the NHS England systems and services performance is maintained. This should be incorporated into the annual service review.
[REQ-27923C]	Security Operations Management	Ensure the clocks of all relevant information processing systems, including all FDP systems, within the supplier's security domain shall be synchronised to a single reference time source, e.g., Stratum 1 servers
[REQ-1BFAE4]	Security Operations Management	Ensure system administrator and operator activities are logged, and the log files are protected against tamper and regularly reviewed. These log files should be made available for incident investigation, response, and forensic purposes.
[REQ-6B3202]	Security Operations Management	Ensure protection against malware for detection, prevention, and recovery, combined with appropriate user awareness
[REQ-805E8C]	Security Operations Management	Ensure penetration testing of environments is carried out at least annually or upon significant change (for example new interfaces). NHS England could request to periodically review these reports. Remediation of identified vulnerabilities must be acted upon by producing and implementing mitigation plans in a timely manner Schedule: •Prior to go-live •Annually thereafter or upon significant change Remediation: •Critical, high, and medium findings to be mitigated prior to go-live •Low and informational findings to be added to backlog for fix within appropriate timescales
[REQ-A331F5]	Security Operations Management	Ensure multiple backups are stored in different locations, based on NCSC guidance. The '3-2-1' rule should be applied: 3 copies, 2 devices, 1 offsite backup held within UK

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-5ADD6C]	Security Operations Management	Ensure information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the supplier's exposure to such vulnerabilities are evaluated and appropriate measures taken to address the associated risk. Suppliers will be required to inform NHS England Cyber teams of critical and high classification technical vulnerabilities
[REQ-88FFAD]	Security Operations Management	Ensure controls governing the installation of software by users shall be implemented
[REQ-8D9E97]	Security Operations Management	Dispose of all NHS England data assets in-line with the exit schedule of the contract.
[REQ-6F72B5]	Security Operations Management	Control and inform to the relevant NHS England stakeholders in a timely manner, changes to the supplier's organisation, business processes, information processing facilities and systems that affect the integrity and availability of NHS England systems and services
[REQ-4B4F06]	Security Operations Management	Carefully plan and agree supplier audit requirements and activities involving verification of operational systems to minimise disruptions to business processes.
[REQ-A08EF2]	Security Operations Management	Be tested for vulnerability to Denial of Service (DoS) and hardened against such attacks when significant software changes are made to production software
[REQ-557664]	Security Operations Management	Allow, enable and support any NHS England audit of the supplier for assurance purposes with sufficient notice. NHS England Cyber Security teams may also conduct external vulnerability scanning on supplier's public facing interfaces and may inform supplies of potential risks identified.
[REQ-326BF4]	Security Operations Management	Achieve Application Security Verification Standard (ASVS) level 2, with the view of Level 3 being achieved as the platform criticality changes or the platform is classified as critical national infrastructure. (Suppliers will be required to be tested against the OWASP top 10 web application vulnerabilities)
[REQ-A925ED]	Security Operations Management	The FDP should have an end point security capability for CSOC monitoring on all tenant services.
[REQ-E3E58A]	Security Operations Management	The Succesful Supplier should have mature and documented framework for undertaking threat modelling, which could leverage industry standard approaches such as STRIDE and DREAD.
[REQ-348E50]	Security Operations Management	The Successful Supplier will be required to implement user activity audit logic to ensure that user activity is appropriate. This should include specific auditing of Privileged Users, providing a mechanism to identify unauthorised change activity.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-49F338]	Security Operations Management	The Successful Supplier will be expected to develop an iterative approach to Use Cases ensuring a level of ongoing development and refinement over time. The Successful Supplier will be expected to work collaboratively with the Authority during this process, to leverage wider business knowledge and technical capability that will inform threat detection. Use-cases should encompass the actual detection logic, along with documentation relating to the rationale, investigative steps, testing and known limitations. In response to an evolving threat landscape the Successful Supplier will be able to adapt existing Use-cases or develop new custom Use-cases on an Ad-hoc basis.
[REQ-05D3EF]	Standards, Frameworks and Principles	Demonstrate that the FDP and its platform applications and services provide compliance with ISO27017 security controls for cloud services
[REQ-2A707A]	Standards, Frameworks and Principles	Comply with NCSC Cloud Security Principles [https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles] 1.Data in Transit Protection 2.Asset Protection and Resilience 3.Separation Between Users 4.Governance Framework 5.Operational Security 6.Personnel Security 7.Secure Development 8.Supply Chain Security 9.Secure User Management 10.Identity and Authentication 11.External interface protection 12.Secure Service Information 13.Audit Information of Users 14.Secure Use of Service (incl. clear articulation of shared responsibility for security)
[REQ-2F6264]	Standards, Frameworks and Principles	Demonstrate that the FDP and its platform applications and services provide compliance with ISO27018 protection of Personal Identity Information

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-8C0B73]	Standards, Frameworks and Principles	Demonstrate that the FDP and its platform applications and services provide compliance with ISO27007 Information Security Management
[REQ-3B793D]	Standards, Frameworks and Principles	Demonstrate that the FDP and its platform applications and services provide compliance with ISO27001 Information Security Management
[REQ-43F762]	Standards, Frameworks and Principles	Demonstrate that the FDP and its platform applications and services provide an acceptable level of compliance with NHS Data Security and Protection Toolkit before entering service (https://www.dsptoolkit.nhs.uk/)
[REQ-8794B3]	Standards, Frameworks and Principles	Comply with NCSC Bulk Data Principles [https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data] 1.Know your data 2.Keep only essential data 3.Unmitigated vulnerabilities 4.User access and privilege 5.Administrator access 6.Know your external dependencies 7.Audit data access 8.No known vulnerable surfaces are exposed at the edges of your service 9.No unsupported software is present in your service and its underlying infrastructure 10.Attacks against the service is proactively monitored and handle through measurable and tested incident response process 11.An automatic alert would be raised in response to an atypical attempt to access bulk data 12.All interfaces are well defined, and none allow for arbitrary queries of data 13.User access to bulk data held by the service is rate-limited 14.A spear-phishing attack against an administrator's email account, or an attack through their web browser, will not yield administrative access to the service using a single exploit 15.All backups or copies of your data are held securely, for the minimum time necessary. These principles must be applied for protecting personal data and must in the shared responsibility model

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-166AE7]	Standards, Frameworks and Principles	The chosen supplier will work to uphold NHS Digital policy, principles, and standards to provide a compliant integration solution. NHS Digital provides a comprehensive source of information on standards, templates, and services available at: Home - NHS Digital Some key references are identified below: •NHS Digital Architecture explain principles, capabilities and support for developers NHS Digital architecture - NHS Digital •Integration patterns: Integration Patterns Book - NHS Digital •NHSE Digital API platform: API platform - NHS Digital •Interoperability Toolkit: Interoperability Toolkit - NHS Digital •NHS Digital explaining NHSD's support for an integration in a box approach: What is 'integration in a box'? - NHS Digital
[REQ-B02975]	Standards, Frameworks and Principles	Produce a current Cyber Essential Plus certificate that is applicable to the scope of the work
[REQ-3C1221]	Standards, Frameworks and Principles	Comply, and demonstrate compliance, with NCSC Cyber Assessment Framework (CAF) and must take steps to comply with the framework from the outset
[REQ-B695F9]	Standards, Frameworks and Principles	Comply with NHS Technology Code of Practice [https://www.gov.uk/guidance/the-technology-code-of-practice]
[REQ-42E195]	Supplier Security Management Plan	Provide named individuals for each of the defined roles: Executive Directors, The Senior Information Risk Owner, Information Asset Owners, Information Governance Team, Procurement Team, Line Managers, All staff
[REQ-90C097]	Supplier Security Management Plan	Processes should be in place for urgent patching, outside of normal patch cycles
[REQ-F561BF]	Supplier Security Management Plan	Patches should be tested to ensure they do not impact the system
[REQ-6CFDF9]	Supplier Security Management Plan	Maintaining the patch status of the system and its components in line with supplier requirements, and ensuring that patches are properly authenticated before applying
[REQ-DFBCD8]	Supplier Security Management Plan	Ensure organisations regularly monitor, review and audit supplier service delivery.
[REQ-CF9EB7]	Supplier Security Management Plan	Ensure NHS England's existing security management plan development guidelines are adhered to

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-A27F17]	Supplier Security Management Plan	Ensure changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks
[REQ-51C4F1]	Supplier Security Management Plan	Ensure all relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation’s information.
[REQ-F997F3]	Supplier Security Management Plan	Ensure agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain
[REQ-2F4D14]	Supplier Security Management Plan	Agree with the Authority, and document, Information security requirements for mitigating the risks associated with your access to the organisation’s assets
[REQ-C2A137]	Supplier Security Management Plan	Agree and adhere to Call-Off Schedule 9 (Security)
[REQ-C51D7D]	IDAM	Use existing solutions in the NHS to authenticate users and provide access into FDP (e.g. CIS2, NHS.net AD, Azure AD or Okta).
[REQ-81AC78]	IDAM	Support dataset level, record-level, field-level and cell-level security through PBAC, so that permission on certain data can be Purpose specific and limited to only those who should see it. It must also be possible to manage and grant authorisations within tenants and across tentants as needed e.g. at a local, regional, or national level. For example the underlying platform data includes linked data for a range of care settings, but a defined Purpose may be restrict access to only allowing access to parts of records for a sub-set of settings.
[REQ-8BE418]	IDAM	Provide, implement and enforce authentication via Identity & Access Management (IAM) to provide first line access to FDP based on the user's identity
[REQ-666C63]	IDAM	Provide, implement and enforce Purpose Based Access Controls (PBAC) to provide authorisation to user to access data and functions, providing a scope for data access, time based access and potentially a second level of role based access within the defined Purpose.
[REQ-9B6F91]	IDAM	Onboard and offboard organisations and federate or delegate the responsibility of managing the on/off boarding process to different NHS organisations
[REQ-6A1F5B]	IDAM	Manage user authentication and authorisation within and across tenants from a centralised service.
[REQ-202FE9]	IDAM	Manage Purposes against an FDP user and provide the users with the ability to select one Purpose at a time with which to authorise access to information (PBAC)
[REQ-F675A9]	IDAM	Ensure that a user can access only one Purpose at a time across all devices and data from a prior Purpose must be cleared from all device sessions before entering the next one.

UUID	Level 1	Requirement (Must / Ability to…)
[REQ-17B732]	IDAM	Define a Purpose including all mechanisms and constraints by which data can be viewed or interacted with. So, platform apps, dashboards, reports, analytics and exports all need to function within the Purpose and not stray outside of it. Some situations may require the purpose to be time based. Purposes can be established within a single tenant but also need to extend to cover data and access from more than one tenant
[REQ-4A8377]	IDAM	Follow the principle of Least Privileged Access when setting up and running IAM and PBAC and ensure that the right individuals have appropriate access to resources
[REQ-A8A7E2]	IDAM	Demonstrate that the FDP and its platform applications and services provide compliance with GPG44 for use of authenticators to protect on-line services and GPG45 to prove an verify identity.
[REQ-726612]	IDAM	Demonstrate that the FDP and its platform applications and services provide compliance with DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services to provide consistent and standardised user verification authentication across England. (https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3051-identity-verification-and-authentication-standard-for-digital-health-and-care-services)
[REQ-DBB3CE]	IDAM	Align to NHS authentication standards and to security principles and policies for users and groups. (GPG44, GPG45, NHSD Security and Authorisation (link in Architecture Appendix section 1.2))
[REQ-08319A]	IDAM	Accept federated identity from multiple (local, national and others) IAM systems into a central FDP IAM control system.
[REQ-1FAD64]	IDAM	Provide a practical and secure means of authenticating users that may need to use the system but have no means of using one of the established NHS IAM solutions
[REQ-278B6B]	IDAM	Implement and enforce Role-Based Access Control (RBAC) at different levels of the system, according to context. Once authenticated, the user could be assigned one or more roles at the highest level. These roles provide aggregate access and may provide a basic limitation on data access throughout the system, allowing users access to generally available features and visualisations.
[REQ-0526A1]	IDAM	Implement and enforce RBAC within a Purpose (PBAC)

UUID	Level 1	Level 2	Level 3	Requirement (Must / Ability to…)	Change Tracking
[REQ-5.5.1.1]	Service Management	Service Management		A federated service model must be delivered that will support Local and Regional Services with National Oversight. Service Management services will need to integrate with multiple ticketing systems while also providing a consolidated monitoring capability that will allow key service performance metrics to be tracked at all levels of the FDP Service. It is expected that some ICB's will have a service desk capability, where this is not available the NHS National Service Desk will provide this functionality. Local trusts service management tool is utilised, this is a standard tooling across service now. It is expected as part of tenant onboarding the Participant, would integrate and agree and methodology to escalate incidents into their own service management processes.	Amended
[REQ-5.5.1.2]	Service Management	Service Management		The responsibility for maintaining adherence to the Data Platform SLAs and KPIs will be withlie only with the Successful Supplier of the platform	
[REQ-6.8.1.1]	Ways of Working	Service Management	Reporting	Operation of the FDP: The Successful Supplier should demonstrate how they will	

[REQ-6.7.1.1]	Ways of Working	Resource Management		In addition to providing the Resourcing requirements set out in Section 4.5 in relation	Amended
[REQ-6.10.1.1]	Ways of Working	Quality Management	Reporting	The supplier will only be accountable for the performance, uptake, and benefits for the	
[REQ-6.5.1.1]	Ways of Working	Product Support		The Successful Supplier will be required to support Use Cases through its role both as	
[REQ-6.12.1.1]	Ways of Working	Product Management	Monitoring	The Successful Supplier is expected design Products with monitoring capability and	
[REQ-6.4.1.1]	Ways of Working	Product Development		Deliver the underlying Products supporting each of the initial Use Cases via the	
[REQ-6.4.2.1]	Ways of Working	Product Development	Transition	As part of its role in delivering the first Use Cases, the Successful Supplier will need to migrate all these Products onto the FDP (see	
[REQ-6.4.2.2]	Ways of Working	Product Development	Transition	In addition to developing new Products throughout the lifecycle of the contract, the	
[REQ-6.4.3.1]	Ways of Working	Product Development	Product Definition	Suppliers are expected to run Pilots to support the definition and delivery of the Product (as set out later in this chapter) and otherwise follow the stages of the Product lifecycle.	
[REQ-6.4.4.1]	Ways of Working	Product Development	Product Delivery	The Successful Supplier is encouraged to utilise agile value stream governance to maximise the efficiency of delivering new Products as part of the FDP-AS.	
[REQ-6.4.5.1]	Ways of Working	Product Development	User Centred Design	suppliers to ensure value for money in development activities and maintaining the	

[REQ-6.4.6.1]	Ways of Working	Product Development	Product Design	the supplier to support the NHS England with defining, scoping, and planning of additional	
[REQ-6.4.7.1]	Ways of Working	Product Development	Product Release	Additionally, the Successful Supplier of the FDP-AS is expected to allow the onboarding	
[REQ-6.4.7.2]	Ways of Working	Product Development	Product Release	Depending on which scale the Product is rolled out at (local or national), there are	Amended
[REQ-6.4.6.2]	Ways of Working	Product Development	Product Design	User Research, UX and UI inc. Accessibility - Supplier shall be responsible for translating business requirements to technical capability and functionality, engaging, and extrapolating the requirements for build out, translating the Use Case user journeys, identifying opportunities for continuous improvements to	
[REQ-6.13.1.1]	Ways of Working	Product Delivery	Product Delivery	The supplier will need to ensure that the solution takes into consideration the complexity of each Use Case.	
[REQ-6.13.1.2]	Ways of Working	Product Delivery	Product Delivery	The successful supplier will be responsible for end-to-end delivery of all three Product	New
[REQ-6.13.1.3]	Ways of Working	Product Delivery	Product Delivery	Products will need to follow a formal acceptance process, both on a National level and on a Local level, called the National Deployment Process. Products must undergo a full technical assessment, a code review, and an assessment of the Product’s readiness before the rollout. This Product	New
[REQ-6.11.1.1]	Ways of Working	Product Decommissioning	End of Life	The Successful Supplier will therefore also need to define a process to support the	

[REQ-5.4.1.1]	Service Management	Platform/Infra DevOps		Platform / Infra DevOps Team - Self-sufficient, autonomous team responsible for the E2E delivery, operation, support and maintenance of the Federated Data Platform, continuously provisioning the tools and services to help the other PODs to solely focus on their delivery objectives	
[REQ-6.3.1.1]	Ways of Working	Platform Management		Provide and operate the federated platform that supports the Use Cases, including for	
[REQ-6.2.1.1]	Ways of Working	Platform Capability		Deliver a set of modular Core Platform Capabilities in the form of data and analytics	
[REQ-6.2.1.2]	Ways of Working	Platform Capability		the Successful Supplier will: 1.be responsible for delivering a set of modular Core Platform Capabilities in the form of data and analytics solutions and	
[REQ-6.2.2.1]	Ways of Working	Platform Capability	Scalability	Additional Use Cases are likely to be approved and created during the lifecycle of the FDP contract, and the supplier should ensure that the FDP is sufficiently scalable to	Amended
[REQ-6.2.3.1]	Platform Capabilities	Platform Capability	Analytical Solutions	In addition to the delivery of the initial Use Case capabilities, the FDP-AS supplier is expected to deliver analytical solutions and platform applications to support NHS England’s Statutory Duty Reporting capability to monitor and improve the quality of care. As part of this, the FDP-AS supplier will be required to produce tools and capabilities for	
[REQ-6.2.2.2]	Ways of Working	Platform Capability	Scalability	ensures that it has the underlying capability to support future Use Cases and associated	

[REQ-5.6.1.1]	Service Management	Performance Management		The responsibility for use case SLAs and KPIs will lie with the organisation that built each use case, which may be the Data Platform supplier (for the use cases scope in Procurements 1 and 2), and may be third-party suppliers or NHS organisations for use	
[REQ-6.9.1.1]	Ways of Working	Performance Management	Reporting	The FDP-AS Supplier Led Delivery Use Cases the FDP-AS Supplier will be expected	
[REQ-6.9.1.2]	Ways of Working	Performance Management	Reporting	The platform should provide the capability for usage reporting, benefits tracking, performance against Product KPI's	
[REQ-5.1.1.1]	Service Management	Partner Services	FDP Overall	Act as a partner to work with them to achieve sustainable outcomes in line with the following principles: •Empowering the NHS through reduced	
[REQ-5.1.1.2]	Service Management	Partner Services	FDP Overall	The expectations and principles for the Successful Supplier relating to Continuous Improvement, Innovation, Measurement and Knowledge Management set out in Schedule	New
[REQ-6.1.1.1]	Ways of Working	Operating Model		The operating model for the Successful Supplier of the FDP-AS should recognise the	
[REQ-6.1.1.2]	Ways of Working	Operating Model		The NHS in England is a complex collection of organisations interacting with each other in constantly evolving ways through Integrated Care Systems (ICS). The Successful	
[REQ-6.1.1.3]	Ways of Working	Operating Model		NHS England envisages to develop a collaborative partnership to work with the Successful Supplier to achieve sustainable outcomes in line with the following principles: •Building Data Capability: enabling the NHS England to have a lasting, improved data	

[REQ-6.1.1.4]	Ways of Working	Operating Model		There will be two different delivery models for Use Cases: FDP-AS Supplier Led Delivery: the FDP-AS Supplier has overall accountability for delivering Platform requirements and Product development for the entire product* if awarded via the Product Development and Supporting Services Contract. Hybrid Delivery: the FDP-AS Supplier is accountable for delivering Platform requirements, but Product development is shared amongst different suppliers or agents (including the FDP-AS Supplier, other suppliers, internal NHS England teams). *in line with the requirements and scope set out as part of this procurement. A Successful Supplier has distinct	Amended
[REQ-6.1.1.5]	Ways of Working	Operating Model		Successful Supplier will need to demonstrate the Business Capabilities set out in Section 4.4, particularly Dev Ops, Platform Solution and Service Management, and Training	
[REQ-6.1.2.1]	Ways of Working	Operating Model	Interoperability	Supplier Collaboration: Suppliers are expected to work within the FDP Programme	Amended
[REQ-6.1.3.1]	Ways of Working	Operating Model	Partner Working	The Successful Supplier will need to engage with and manage diverse groups of	

[REQ-6.1.3.2]	Ways of Working	Operating Model	Partner Working	NHSE has the expectation of the ability to co-locate during the implementation phase and throughout the contract where appropriate	New
[REQ-6.1.4.1]	Ways of Working	Operating Model	Product Development	It is expected that the supplier will build on the NHS England definition of the Product	
[REQ-6.1.4.2]	Ways of Working	Operating Model	Product Development	suppliers are expected to demonstrate an operating model that is flexible enough to	
[REQ-6.1.4.3]	Ways of Working	Operating Model	Product Development	the FDP-AS supplier will be expected to develop and build new Products, which will	
[REQ-6.1.1.6]	Ways of Working	Operating Model		Successful Supplier will balance focus across the provision of the new platform, the transition of existing Products to support the initial Use Cases, and, for the FDP-AS Supplier-Led Use Cases, the build of new Products to deliver business value. The	
[REQ-6.1.5.1]	Ways of Working	Operating Model	Engagement	the supplier is expected to identify new opportunities to optimise, develop and	
[REQ-6.1.5.1]	Ways of Working	Operating Model	Engagement	The NHS England Central Commercial Function has a new vision for how it will work	New
[REQ-6.1.6.1]	Ways of Working	Operating Model	Product Release	Local organisations will be responsible for managing their own Product acceptance, and FDP-AS Suppliers must be considerate of this and are expected to operate in	
[REQ-6.1.7.1]	Ways of Working	Operating Model	Resource Management	The supplier is expected to support NHS England in delivering these FDP Programme	
[REQ-6.1.7.2]	Ways of Working	Operating Model	Resource Management	The Successful Supplier(s) will work with the NHS team during the Mobilisation phase of	Amended
[REQ-6.1.7.3]	Ways of Working	Operating Model	Resource Management	In the list below, the 22 capabilities are split between Delivery Capabilities, Support, and	Amended

[REQ-6.1.7.4]	Ways of Working	Operating Model	Resource Management	Suppliers should demonstrate how their operating model will allow them to deliver the required resource against each business capability at each stage of the FDP Programme.	New
[REQ-5.2.1.1]	Service Management	Incident and Problem Management	Incident Management	Service Management - Act as a single point for monitoring, tracking and communicating P1 and P2 incidents Manage the communication of the service impact with the senior stakeholders across business and technology Manage problem management and continual improvement to improve and manage services effectively.	
[REQ-6.6.1.1]	Ways of Working	Governance	Governance	When providing and operating the federated platform, and delivering on its Core Capabilities, the Successful Supplier will need to adhere to the various Governance models and bodies set out in Section 4.3, particularly with reference to Strategic Governance Forums.	
[REQ-6.6.1.2]	Ways of Working	Governance	Governance	It is expected the FDP-AS supplier will integrate into existing NHS England Governance Forums, as well as NHS technical, delivery, programme management cadence and other relevant governance	Amended
[REQ-6.6.1.3]	Ways of Working	Governance	Governance	The Successful Supplier is expected to report into the following Strategic Level Governance	Amended

[REQ-6.6.1.4]	Ways of Working	Governance	Governance	Suppliers will be expected to integrate with and adhere to Local Governance forums	
[REQ-6.6.2.1]	Ways of Working	Governance	Supplier Management	NHS England and the Successful Supplier will each appoint a dedicated Contract	Amended
[REQ-6.6.2.2]	Ways of Working	Governance	Supplier Management	The Successful Supplier may be required to attend quarterly review meetings with NHS	
[REQ-6.6.2.3]	Ways of Working	Governance	Supplier Management	Due to the strategic importance of the FDP-AS contract the Successful Supplier will be	New
[REQ-6.6.2.4]	Ways of Working	Governance	Supplier Management	All FDP suppliers and NHS England will be expected to sign and adhere to the FDP	New
[REQ-6.6.3.1]	Ways of Working	Governance	Risk Manaagement	Both parties shall pro-actively manage and report on risks that have been attributed to	
[REQ-6.6.4.1]	Ways of Working	Governance	Product Delivery	the FDP-AS supplier is expected to integrate with Local Governance forums, but only on a	
[REQ-5.3.1.1]	Service Management	Application and Data Devops		Application and Data DevOps Team - Hold the E2E accountability for the delivery and	
[REQ-6.5.1.1]	Ways of Working			Account Management - Supplier shall be responsible for technical management,	
[REQ-6.5.1.2]	Ways of Working			DevOps - Supplier shall be responsible for Product development including the	
[REQ-6.5.1.3]	Ways of Working			Data Engineering, Analytics & Dashboards - Supplier shall adhere to, and deliver against,	
[REQ-6.5.1.4]	Ways of Working			Technical Support - Supplier shall be responsible for delivery and management of	
[REQ-6.5.1.5]	Ways of Working			Solution Architecture - Supplier shall propose solutions aligned to standards and approval	
[REQ-6.5.1.6]	Ways of Working			Data Governance and Assurance - Supplier shall adhere to, and deliver against, the	
[REQ-6.5.1.7]	Ways of Working			Security & Privacy Compliance - Supplier shall adhere to, and deliver against, the	
[REQ-6.5.1.8]	Ways of Working			Platform Solution & Service Management - Supplier shall be responsible for operating	

[REQ-6.5.1.9]	Ways of Working			Application & Release Management - Supplier shall be responsible for release,	
[REQ-6.5.1.10]	Ways of Working			Knowledge Management - Supplier shall support Knowledge Management activities	
[REQ-6.5.1.11]	Ways of Working			Marketplace - Out of scope for this procurement, to be considered in	Amended
[REQ-6.5.1.12]	Ways of Working			Innovation - Supplier shall be responsible for identifying and developing industry-led	
[REQ-6.5.1.13]	Ways of Working				
[REQ-6.5.1.14]	Ways of Working			Training - Supplier shall provide Training on the platform and the Use Case solutions.	
[REQ-6.5.1.15]	Ways of Working			Procurement - Supplier shall be responsible for interfacing with and providing input when	
[REQ-6.5.1.16]	Ways of Working			Workforce Deployment - NHS England and Supplier to agree workforce deployment as	
[REQ-6.5.1.17]	Ways of Working			Comms and Engagement - Supplier shall be responsible for supporting comms and	
[REQ-6.5.1.18]	Ways of Working			Portfolio & Change Management - Supplier shall collaborate with NHS England to deliver	
[REQ-6.5.1.19]	Ways of Working			Commercial / Legal / Finance - Supplier shall be responsible for interfacing with and	
[REQ-6.5.1.20]	Ways of Working			Programme / Risk Management & Benefits - Supplier shall be responsible for providing	
[REQ-6.5.1.21]	Ways of Working			Enterprise Architecture - Supplier shall be responsible for adhering to, and delivering	

[REQ-6.5.1.22]	Ways of Working			Use case Business Partner/Product Owner - Supplier shall be responsible for supporting and interfacing with business partners (and other FDP strategy functions) as and when required. Supplier shall act as delegated Product Owner(s) in some circumstances e.g., during early development of the platform or where the NHS England Product owner has not yet been assigned	
[REQ-6.5.1.23]	Ways of Working			This service model will apply across the Product lifecycle, and the FDP-AS Supplier is	
[REQ-6.5.1.24]	Ways of Working			At all stages, the supplier will be expected to meet the NHS England's requirements for	
[REQ-6.5.1.25]	Ways of Working			The supplier is responsible for managing its resource-profile throughout the duration of	Amended

[REQ-6.5.1.26]	Ways of Working			•Onboarding: The supplier will be responsible for a robust Product onboarding process,	
[REQ-6.5.1.27]	Ways of Working			•Delivery: As is set out below, the Successful Supplier will need to be able to rapidly re-	Amended
[REQ-6.5.1.28]	Ways of Working			•Offboarding: The Supplier will manage the offboarding of resources in line with an	
[REQ-6.5.1.29]	Ways of Working			The FDP-AS Supplier will be responsible for continuous improvement and innovation	
[REQ-6.5.1.30]	Ways of Working			Suppliers must ensure that NHS England users of Products at each stage, from vision	Amended
[REQ-6.5.1.31]	Ways of Working			The initial priority for the FDP-AS Supplier will be to configure the new Data Platform and	
[REQ-6.5.1.32]	Ways of Working			the overall Transition Plan will be proposed and owned by the FDP-AS Supplier	
[REQ-6.5.1.33]	Ways of Working			it is expected that the FDP-AS Supplier will take-over the development of In	
[REQ-6.5.1.34]	Ways of Working			the Successful Supplier will also need to define a process for existing Products in the	
[REQ-6.5.1.35]	Ways of Working			The Successful Supplier will be required to provide Monthly Service Incident Reviews,	Amended
[REQ-6.5.1.36]	Ways of Working			Design of the FDP Service Model and supporting catalogue must align to the strategic direction outlined in 'C104091_NHSE_FDPAS_ISFT_Schedule 2_Appendix G_Service Catalogue', covering culture, people, process and technology.	New

[REQ-6.5.1.36]	Ways of Working			Provide the high-level service catalogue, containing the following services: - Service Management - Tenancy Management - Data Quality - MLOps - DataOps - Data Management and Governance - Application Management - Platform Management and Optimisation - Data / Platform Security and Compliance - Cloud and Data Platform Ops	New

O

SCHEDULE 2.2

PERFORMANCE LEVELS

Performance Levels

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

Available has the meaning given in Paragraph 1 of Part II of ANNEX 1: Key Performance Indicators;

Non-Available means in relation to the Supplier System or the Services, that the Supplier System or the Services are not Available;

Performance Monitoring Report has the meaning given in Paragraph 1.1(a) of Part B;

Performance Review Meeting means the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Agreement, as further described in Paragraph 1.5 of Part B;

Repeat KPI Failure has the meaning given in Paragraph 3.1 of Part A;

Service Availability has the meaning given in Paragraph 2 of Part II of ANNEX 1: Key Performance Indicators;

Service Downtime means any period of time during which any of the Services are not Available; and

System Response Time has the meaning given in Paragraph 3.1 of Part II of ANNEX 1: Key Performance Indicators.

PART A: KEY PERFORMANCE INDICATORS AND SERVICE CREDITS

1 KEY PERFORMANCE INDICATORS

1.1 ANNEX 1: Key Performance Indicators sets out the Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

1.2 The Supplier shall monitor its performance against each Key Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B.

1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5.

1.4 As may be further set out in the Implementation SoW, the Authority and the Supplier will agree:

(a) during the process of Achievement of Implementation Milestone 3 (as such Milestone is set out in the Implementation SoW): the application of the Key Performance Indicators to legacy products (as set out in the Inventory) which are identified as having "Platinum", "Gold", "Silver" and "Bronze" (Metals) service requirements in the Inventory (as such Metals are described in the Inventory); and

(b) following load testing during Implementation Milestone 2 (as such Milestone is set out in the Implementation SoW): the baseline levels of Data Platform performance for the purposes of KPI2 and KPI3.

2 SERVICE POINTS

2.1 If the level of performance of the Supplier during a Service Period achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

2.2 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraph 2.3.

2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in ANNEX 1: Key Performance Indicators depending on whether the KPI Failure is a Minor KPI Failure, a Material KPI Failure or a failure to meet the KPI Service Threshold, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 3.2 shall apply.

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES

Repeat KPI Failures

3.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any two or more consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a "**Repeat KPI Failure**".

3.2 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

SP = P + Y

where:

SP = the number of Service Points that shall accrue for the Repeat KPI Failure;

P = the applicable number of Service Points for that KPI Failure as set out in ANNEX 1: Key Performance Indicators depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Material KPI Failure or a failure to meet the KPI Service Threshold; and

Y = P x number of consecutive Measurement Periods in which the Repeat KPI Failure occurs[1].

Worked example based on the following Service Points regime for Total Hours Availability in respect of KPI1.1:

[Redacted under FOIA s43, Commercial interests]

4 PERMITTED MAINTENANCE

4.1 The Supplier shall be allowed to book a maximum of 4 hours Service Downtime for permitted maintenance in any one Service Period which shall take place between the hours and on the day specified in the Maintenance Schedule unless otherwise agreed in writing with the Authority ("**Permitted Maintenance**").

5 SERVICE CREDITS

5.1 Schedule 7.1 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.

5.2 Service Credits accrue during the fourth and subsequent Measurement Periods after the Go Live Date.

5.3 The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

[1] As the KPI Failure is only a *Repeat KPI Failure* in the second or subsequent Measurement Period in which it occurs, the first Measurement Period in which a KPI Failure occurs (before it is a Repeat KPI Failure) is not taken into account for these purposes.

PART B: PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within 10 Working Days of the end of each Service Period, the Supplier shall provide:

(a) a report to the Authority Representative which summarises the performance by the Supplier against each of the Key Performance Indicators as more particularly described in Paragraph 1.2 (the Performance Monitoring Report); and

(b) a report to the Authority's senior responsible officer which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the Balanced Scorecard Report).

Performance Monitoring Report

1.2 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous 3 Measurement Periods;

(b) a summary of all Performance Failures that occurred during the Service Period;

(c) the severity level of each KPI Failure which occurred during the Service Period;

(d) which Performance Failures remain outstanding and progress in resolving them;

(e) for any Material KPI Failures occurring during the Service Period, the cause of the relevant KPI Failure and the action being taken to reduce the likelihood of recurrence;

(f) the status of any outstanding Rectification Plan processes, including:

(i) whether or not a Rectification Plan has been agreed; and

(ii) where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;

(g) for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;

(h) the number of Service Points awarded in respect of each KPI Failure;

(i) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;

(j) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

(k) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

(l) such other details as the Authority may reasonably require from time to time;

Information in respect of previous Service Periods

(m) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;

(n) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;

(o) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan;

Information in respect of the next Quarter

(p) any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter; and

(q) such further information as the Authority requires.

Balanced Scorecard Report

1.3 The Balanced Scorecard Report shall be presented in the form of an online accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:

(a) financial indicators;

(b) the Target Performance Levels achieved;

(c) behavioural indicators;

(d) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;

(e) Milestone trend chart, showing performance of the overall programme; and

(f) sustainability and energy efficiency indicators, for example energy consumption and recycling performance.

1.4 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.5.

1.5 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. The Performance Review Meetings shall (unless otherwise agreed):

(a) take place within 5 Working Days of the Performance Monitoring Report being issued by the Supplier;

(b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and

(c) be attended by the Supplier Representative and the Authority Representative.

1.6 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure.

2 PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and records (including Service Request records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority and/or any Authority Service Recipient online and are capable of being printed.

3 PERFORMANCE VERIFICATION

The Authority reserves the right to verify the Availability of the Supplier System and/or the Services and the Supplier’s performance under this Agreement against the Key Performance Indicators.

ANNEX 1: KEY PERFORMANCE INDICATORS

PART I: KEY PERFORMANCE INDICATORS TABLES

The Key Performance Indicators that shall apply to the Operational Services are set out in the table immediately below (Optional Services being covered by the subsequent table):

Key Performance Indicators: non-Optional Services

[Redacted under FOIA s43, Commercial interests]

Key Performance Indicators: Optional services

The Key Performance Indicators that shall apply to the Optional Services are set out in the relevant Statements of Work.

PART II: DEFINITIONS

1 AVAILABLE

1.1 The Supplier System and/or the Services shall be Available when:

(a) End Users are able to access and utilise all the functions of the Data Platform; and

(b) the Data Platform is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description (as measured on a 24 x 7 basis).

2 SERVICE AVAILABILITY

2.1 Service availability shall be measured as a percentage of the total time (during the Total Hours) in a Service Period, in accordance with the following formula (**Service Availability**):

$$\text{Service Availability \%} = \frac{(MP - SD)\,x\,100}{MP}$$

where:

MP = total number of minutes during the Total Hours, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime during the Total Hours, excluding Permitted Maintenance, in the relevant Service Period.

2.2 When calculating Service Availability in accordance with this Paragraph 2:

(a) Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Paragraph 4.1 of Part A of this Schedule shall be subtracted from the total number of hours in the relevant Service Period; and

(b) Service Points shall accrue if:

(i) any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or

(ii) where maintenance undertaken by the Supplier exceeds 4 hours in any Service Period.

3 RESPONSE TIMES

3.1 The "**System Response Time"** is the round trip time taken to process a message or request of the Data Platform, and shall be measured from the moment the last packet of data which relates to a particular message is received at the external interface of the Data Platform until a response is generated and the first block of data leaves the external interface (including, for the avoidance of doubt, the time taken for any necessary processing).

3.2 The Supplier System Response Time shall be the average System Response Time measured over the course of a Service Period.

4 SERVICE REQUEST RESPONSE TIMES

4.1 Service Request response times will be measured from the time that the Service Request is reported to the Supplier, to the point at which the Supplier provides an initial response to the Service Request.

4.2 A Service Request relating to Severity 1 and Severity 2 Service Incidents must be acknowledged by Supplier Personnel. Other Service Requests (and Severity 1 and Severity 2 Service Incident-related Service Requests, provided they have also been acknowledged by Supplier Personnel) may be acknowledged automatically.

4.3 The Supplier shall monitor the Service Request response times and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

5 FIX TIMES

5.1 The "**Fix Time**" of a Service Incident is the period from the time that the Service Incident has been reported to the Supplier to the point of its Resolution and "**Resolution**" means in relation to a Service Incident either:

(a) the root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Service Levels; or

(b) the Authority has been provided with a workaround in relation to the Service Incident deemed acceptable by the Authority.

5.2 Fix times for Service Incidents shall be measured 24x7.

5.3 The Supplier shall measure Fix Times as part of its service management responsibilities and report periodically to the Authority on Fix Times as part of the Performance Monitoring Report.

5.4 For the purposes of this ANNEX 1: Key Performance Indicators, the following expressions shall have the meanings set opposite them below:

Rolling 12 Months means the relevant Service Period plus the previous 11 Service Periods in the aggregate;

Service Incident means a reported occurrence of a failure to deliver any part of the Services in accordance with the Authority Requirements or the Key Performance Indicators;

Service Request means a report or request from the Authority or Authority Service Recipient in respect of a Service Incident or otherwise related to the performance or operation of the Services;

Severity 1 Service Incident (High)

means a Service Incident which, in the reasonable opinion of the Authority:

(a) constitutes a loss of the Service which acutely disadvantages a large group of End Users or Users or prevents them from working or otherwise delivering outcomes expected of them through use of the Service;

(b) the Service/Data Platform is wholly unavailable or severally degraded for all End Users or Users;

(c) has a critical impact on the activities of the Authority and/or any Authority Service Recipient;

(d) causes significant financial loss and/or disruption to the Authority and/or any Authority Service Recipient;

(e) constitutes a high level of clinical, data security or data protection risk;

(f) is highly likely to cause damage to the reputation of the Authority and/or any Authority Service Recipient; or

(g) results in any material loss or corruption of Authority Data;

[Redacted under FOIA s43, Commercial interests]

Severity 2 Service Incident (Medium)

means a Service Incident which, in the reasonable opinion of the Authority has the potential to:

(a) have a moderate adverse impact on the activities of the Authority and/or any Authority Service Recipient and a workaround is acceptable to the Authority and/or any Authority Service Recipient (as applicable);

(b) have a moderate adverse impact on the activities of the Authority and/or any Authority Service Recipient;

(c) cause a financial loss and/or disruption to the Authority and/or any Authority Service Recipient which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Incident (High);

(d) prevent a moderate group of End Users or Users from working or otherwise properly delivering outcomes expected of them through use of the Service;

(e) moderately degrade the Service/Data Platform for the End Users or Users; or

(f) cause a moderate level of clinical, data security or data protection risk (but no such breach/harm is considered likely);

[Redacted under FOIA s43, Commercial interests]

Severity 3 Service Incident (Low) means a Service Incident which, in the reasonable opinion of the Authority and/or any Authority Service Recipient:

(a) has the potential to have a minor adverse impact on the provision of the Services to End Users or Users;

(b) comprises a flaw which does not undermine the End User's or the User's confidence in the information being displayed;

(c) affects or inconveniences a small group of End Users or Users who are still able to work or otherwise deliver outcomes expected of them through use of the Service but may require extra effort; or

(d) constitutes a low level of, or no, clinical, data security or data protection risk;

[Redacted under FOIA s43, Commercial interests]

Total Hours means all hours in a day, Monday to Sunday.

SCHEDULE 2.3

STANDARDS

Standards

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

NHS Standard Contract means the model commissioning contract or contracts published by NHS England (or any successors to the relevant part of its functions) from time to time pursuant to its powers under regulation 17 of the National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012. For the purposes of this Contract "NHS Standard Contract" shall also refer to any variants of the NHS Standard Contract produced by NHS England from time to time; and

Standards Hub means the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/.

2. GENERAL

2.1 The Supplier shall comply with the Standards to the fullest extent applicable. In addition to the Standards set out in this Schedule 2.3 (*Standards*), all standards referred to in the Services Description (and the documentation referenced therein, including the Authority Requirements) and each Statement of Work shall constitute Standards for the purposes of this Agreement.

2.2 Throughout the term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's and/or any Authority Service Recipient's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

2.3 Where a new or emergent standard is to be developed or introduced by the Authority and/or any Authority Service Recipient, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's and/or any Authority Service Recipient's receipt, of the Services is explained to the Authority and/or any Authority Service Recipient (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.4 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

2.5 Where specific hyperlinks are included in this Schedule, the words "(*or at such other NHS or UK government webpage from time to time)*" shall be deemed to be included after the hyperlink.

3. INTEROPERABILITY STANDARDS

3.1 The Supplier shall be required to provide the Services and Deliverables in accordance with such interoperability standards as may be referenced or published by NHS England from time to time. Standards are anticipated to include, but are not limited to:

(a) information governance and security standards that make clear what data may be shared, for what purpose; and what protections are required to keep that data secure;

(b) clinical standards enabling clinicians to safely exchange data with each other with a common understanding of the meaning of the data;

(c) technical standards that will allow systems to talk reliably and securely with each other using common standards for data and transmission;

(d) use of national services, such as the National Record Locator Service, to enable connection across these Local Care Record Exemplars to enable information to be available at the point of care for an individual as they move across geographical boundaries; and

(e) implementation guidance standards.

3.2 The Supplier shall be required to publish the meta-data including data quality rules, processing rules, and data specifications information to support the Standards' development. Until the emergent standard is approved for national use, the Supplier shall be required to map the data according to mapping rules and meta-data information published or referenced via the Authority and/or any Authority Service Recipient. Where a Standard is to be changed or new or emergent standard is to be developed or introduced by the Authority and/or any Authority Service Recipient, NHS England or any other relevant organisation, the Authority and/or any Authority Service Recipient will engage in relation to such change or new or emergent standard through a competent standards framework management organisation with the intention that the Supplier will be able, through such standards framework management organisation (such as INTEROPen (http://www.interopen.org) to comment and engage with the Authority and/or NHS England or any other relevant organisation (as applicable) on the potential impact on the Supplier's provision, or the Authority's and/or any Authority Service Recipient's receipt, of the Services and Deliverables.

3.3 The Supplier shall provide the Services and Deliverables in accordance with the interoperability standards set out below:

(a) NHS Number to be available at the point of care;

(b) SNOMED CT implemented across all settings of care;

(c) Dictionary of Medicines and Devices (dm+d) implemented across all venues of care;

(d) utilisation of GS1 standards for barcoding;

(e) utilisation of ICD11 for the classification of diseases;

(f) implementation of FHIR based specifications i.e. CareConnect;

(g) utilisation of Unified Codes for Units of Measure (UCUM) to represent all units of measures in clinical systems and across messaging products;

(h) staff and citizen facing identity services adopt use of FIDO and related public key-based specifications;

(i) staff and patient facing services apps support OpenID Connect for single-sign-on; and

(j) Open APIs for access to clinical services and patient records support OAuth2.

4. NATIONAL CONTRACT STANDARDS

4.1 The Supplier shall be required to provide the Services and Deliverables in accordance with any applicable standards set out in the NHS Standard Contract as published or referenced by NHS England from time to time including but not limited to any standards on the interoperability of information technology systems, applications, tools, software and/or hardware.

4.2 The Supplier shall comply with the Authority's Code of Conduct for Suppliers (being the document signed by the Supplier as part of the tender process, as updated by the Authority and provided to the Supplier from time to time).

5. TECHNOLOGY AND DIGITAL SERVICES PRACTICE

The Supplier shall (when designing, implementing and delivering the Services and Deliverables) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

6. INFORMATION STANDARDS COMPLIANCE

6.1 The Supplier shall at all times comply with the NHS Information Standards to the extent that such standards are relevant to the Services and Deliverables provided by the Supplier to the Authority and/or any Authority Service Recipient. The NHS Information Standards are documented online at https://digital.nhs.uk/data-and-information/information-standards as updated from time to time.

6.2 Where relevant to the Services and Deliverables, the Supplier shall ensure that they comply with:

(a) the NHS Clinical Information Standards documented online at https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/nhs-digital-data-and-technology-standards/clinical-information-standards to ensure that information about the health and care of individuals can be securely shared and compared across the health care sector; and

(b) any updates or future revisions of those or equivalent standards published or referenced by NHS England.

6.3 The Supplier shall comply with the Authority's information governance framework document for the Programme ("**FDP IG Framework**") as updated by the Authority and provided to the Supplier from time to time.

6.4 and the Authority's other information governance standards relating to the Federated Data Platform Programme.

7. DIGITAL, DATA AND TECHNOLOGY STANDARDS

7.1 The Supplier shall at all times provide Services in compliance with:

(a) the principles and guidance published by NHS England at https://www.england.nhs.uk/about/protecting-and-safely-using-data-in-the-new-nhs-england/;

(b) the Data and Technology Standards published by NHS Digital as outlined online at https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards; and

(c) any updates or future revisions of those or equivalent standards published or referenced by NHS England.

8. CYBER STANDARDS

8.1 The Suppliers shall provide the Services and Deliverables in accordance with the following standards:

(a) Cyber-Essentials+ across the stack as well as at network level;

(b) The process, people and technology standards from the 10 Data and Cyber Security Standards; and

(c) Design digital services using the NHS Digital service manual (https://beta.nhs.uk/service-manual/).

9. OPEN DATA STANDARDS & STANDARDS HUB

9.1 The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

9.2 The Supplier shall ensure that all documentation published on behalf of the Authority and/or any Authority Service Recipient pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 9.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

9.3 The Supplier shall ensure that all documentation describing the data sourced or utilised within the Authority System that is in scope of the Services, including but not limited to meta-data including data specifications, data quality rules, and processing rules are published and updated regularly to promote bottom-up standards creation process. The Supplier shall also ensure the consistent mapping to national or emergent standards during the standards development phase which will be published on the Standards Hub.

10. TECHNOLOGY ARCHITECTURE STANDARDS

The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. Documentation produced in compliance with TOGAF 9.1 or its equivalent, shall be deemed to have been produced in accordance with Good Industry Practice.

11. ACCESSIBLE DIGITAL STANDARDS

11.1 The Supplier shall comply with (or with equivalents to):

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.0 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

12. SERVICE MANAGEMENT SOFTWARE & STANDARDS

12.1 Subject to Paragraphs 2 to 9 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

(a) ITIL v3 2011;

(b) ISO/IEC 20000-1 2011 "ITSM Specification for Service Management";

(c) ISO/IEC 20000-2 2012 "ITSM Code of Practice for Service Management";

(d) ISO 10007 "Quality management systems – Guidelines for configuration management"; and

(e) BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/IEC 27031:2011, ISO 22301 and ISO/IEC 24762:2008 in the provision of "IT Service Continuity Strategy" or "Disaster Recovery" plans.

12.2 For the purposes of management of the Services (including development and supply of Deliverables) and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

13. ENVIRONMENTAL STANDARDS

13.1 The Supplier warrants that it has obtained ISO 14001 (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout the Term. The Supplier shall follow a sound environmental management policy, ensuring that any Deliverables and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

13.2 The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

13.3 The Supplier shall (when designing, procuring, implementing and delivering the Services and Deliverables) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

13.4 The Supplier shall comply with the EU Code of Conduct on Data Centres’ Energy Efficiency. The Supplier shall ensure that any data centre used in delivering the Services are registered as a participant under such Code of Conduct.

13.5 The Supplier shall comply with the Authority’s and/or any Authority Service Recipient’s and HM Government’s objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document “Greening Government: ICT Strategy issue (March 2011)” at https://www.gov.uk/government/publications/greening-government-ict-strategy.

14. HARDWARE SAFETY STANDARDS

14.1 Not used.

15. STANDARDS FOR PROVIDERS OF ONLINE PRIMARY CARE SERVICES

15.1 Not Used.

16. STANDARDS FOR DATA DRIVEN TECHNOLOGY, MACHINE LEARNING & ARTIFICIAL INTELLIGENCE

16.1 The Supplier shall, where applicable, comply with the principles of the Department of Health Social Care Code of Conduct for data-driven health and care technology dated February 2019, which may be accessed at https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology. The Supplier shall:

(a) understand users, their needs and the context;

(b) define the outcome and how the technology will contribute to it;

(c) use data that is in line with appropriate guidelines for the purpose for which it is being used;

(d) be fair, transparent and accountable about what data is being used;

(e) make use of open standards;

(f) be transparent about the limitations of the data used and algorithms deployed;

(g) show what type of algorithm is being developed or deployed, the ethical examination of how the data is used, how its performance will be validated and how it will be integrated into health and care provision;

(h) generate evidence of effectiveness for the intended use and value for money;

(i) make security integral to the design (keep systems safe by safeguarding data and integrating appropriate levels of security); and

(j) define the commercial strategy (including IP).

17. STANDARDS SPECIFIED BY THE MHRA

17.1 The Supplier shall, where applicable, comply with the standards and guidance set out in the Medicines and Healthcare products Regulatory Agency website which can be accessed at https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency.

18. CLINICAL RISK MANAGEMENT STANDARDS

18.1 The Supplier shall, where applicable, comply with the following standards set out at https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team/clinical-risk-management-standards:

(a) DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems; and

(b) DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems, and any updates or future revisions of those or equivalent standards published or referenced by NHS England.

19. LHCR PROGRAMME TECHNICAL CAPABILITIES

19.1 The Supplier Solutions shall, where applicable, adhere to any technical capabilities that enable the following within a LHCR:

(a) Core Interoperability Services – Open APIs;

(b) Core Interoperability Services – Record Location;

(c) Core Interoperability Services – Event Management;

(d) Core Interoperability Services – Longitudinal Care Record;

(e) Core Interoperability Services – Personal Health Records (PHRs);

(f) Reference Services – Metadata Management;

(g) Reference Services – Reference Data Management;

(h) Reference Services – Information Standards;

(i) Reference Services – Master Patient Index;

(j) Data Services – Data Rules Management;

(k) Data Services – Data Discovery Support;

(l) Data Services – Data Transfer and Dissemination;

(m) Data Services – Data Integration;

(n) Data Services – Data Processing;

(o) Data Services - De-identification/Re-identification;

(p) Information Governance and Security – Patient Choices;

(q) Information Governance and Security - Information Governance Implementation;

(r) Information Governance and Security – Authorisation and Authentication;

(s) Information Governance and Security - Care Record Access Audit;

(t) Information Governance and Security – Cyber Security; and

(u) Analytics – Analytics.

19.2 The references in Paragraph 19.1 above to 'Core Interoperability Services', 'Reference Services', 'Data Services', 'Information Governance and Security' and 'Analytics' are references to the headings and descriptions outlined in the 'LHCRE Funding Agreement' available upon request from NHS England, via email, at england.phmsupport@nhs.net.

20. PRSB COMMON CORE INFORMATION STANDARDS

20.1 The Supplier shall, within 6 months of its endorsed publication date, comply with all of the standards listed in the Professional Record Standard Body (PRSB) – Core Information Standards to be published online at https://theprsb.org/standards/coreinformationstandard/ or such other address as is communicated to the Suppliers by the Authority from time to time.

20.2 Failure to comply with the Standard listed in this Paragraph 20 of this Schedule within the agreed timeframe shall be deemed to constitute a material Default which may result in the Authority terminating this Agreement.

21. INFORMATION GOVERNANCE FRAMEWORK FOR INTEGRATED HEALTH CARE

21.1 The Supplier shall comply with all of the standards listed in the 'Local Health and Care Records – Information Governance Framework for Integrated Health and Care' from time to time, available upon request from NHS England at england.phmsupport@nhs.net.

22. INFORMATION STANDARDS NOTICES

22.1 The Supplier shall at all times, comply with any Information Standards Notices published, from time to time, by the Data Coordination Board (or any successor body to that board) online at https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/information-standards-notices.

SCHEDULE 2.4

SECURITY MANAGEMENT

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"Risk Management Documentation" has the meaning given in Paragraph 6.3;

"Information Management System" means the Core Information Management System and the Wider Information Management System;

"Accreditation" means the assessment of the Core Information Management System in accordance with Paragraph 6 by the Authority or an independent information risk manager/professional appointed by the Authority, which results in an Accreditation Decision;

"Accreditation Decision" is the decision of the Authority, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;

"Accreditation Plan" means the Supplier's plan to attain an Risk Management Approval Statement from the Authority, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.4;

"Breach of Security" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement;

(b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority and/or any Authority Service Recipient, the Supplier or any Sub-contractor in connection with this Agreement; and/or

(c) any part of the Supplier System ceasing to be compliant with the Certification Requirements,

or any material identified risk of, threat or attempt to cause such an occurrence in each case as more particularly set out in the security requirements in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements;

"Certification Requirements" means the requirements set out in Paragraph 7;

"Core Information Management System" means those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources, which the Authority has determined in accordance with Paragraph 4.2 shall be subject to Accreditation;

"IT Health Check" has the meaning given Paragraph 8.1(a);

“Personal Data Processing Statement” sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority and/or any Authority Service Recipient; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority and/or any Authority Service Recipient; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its

Sub-contractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 6.4 of Schedule 2.4 (Security Management) and included in the Risk Management Documentation;

"Process Authority Data" means any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Authority Data;

"Required Changes Register" means a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Authority shall be made to the Core Information System and/or the Risk Management Documentation as a consequence of the occurrence of any of the events set out in Paragraph 6.13(a) to 6.13(h) together with the date on which each such change shall be implemented and the date on which each such change was implemented;

"Risk Management Approval Statement" means a notice issued by the Authority which sets out the information risks associated with using the Core Information Management System and confirms that the Authority is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;

"Risk Management Reject Notice" has the meaning given in Paragraph 6.7(b);

"Security Test" has the meaning given Paragraph 8.1;

"Statement of Information Risk Appetite" has the meaning given in Paragraph 5.1;

"Vulnerability Correction Plan" has the meaning given in Paragraph 8.3(c)(i); and

"Wider Information Management System" means those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data which have not been determined by the Authority to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources.

2 INTRODUCTION

2.1 This Schedule sets out:

(a) the principles which the Supplier shall comply with when performing its obligations under this Agreement in order to ensure the security of the Authority Data, the IT Environment, the Supplier System and the Information Management System;

(b) the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 6;

(c) the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;

(d) the Security Tests which the Supplier shall conduct during the Term in Paragraph 8;

(e) the Security Tests which the Authority may conduct during the Term in Paragraph 8.6;

(f) the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 9;

(g) the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 10; and

(h) each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 11.

3 PRINCIPLES OF SECURITY

3.1 The Supplier acknowledges that the Authority and Authority Service Recipients place great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

(a) the IT Environment;

(b) the Supplier Solution; and

(c) the Information Management System.

3.2 Notwithstanding the involvement of the Authority in the Accreditation of the Core Information Management System, the Supplier shall be and shall remain responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors;

(b) the security of the Supplier Solution; and

(c) the security of the Information Management System.

3.3 The Technical Design Authority shall, in addition to its responsibilities set out in Schedule 8.1 (Governance), monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.

3.4 Each Party shall provide access to members of its information assurance personnel to facilitate the Supplier's design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of the Supplier Solution and Information Management System and otherwise at reasonable times on reasonable notice.

4 INFORMATION MANAGEMENT SYSTEM

4.1 The Information Management System comprises the Core Information Management System and the Wider Information Management System.

4.2 The component parts of the Core Information Management System and its boundary with the Wider Information Management System are shown in the diagram in Annex 2.

4.3 Any proposed change to the component parts of and/or boundary of the Core Information Management System shall be notified and processed in accordance with the Change Control Procedure.

5 STATEMENT OF INFORMATION RISK APPETITE AND BASELINE SECURITY REQUIREMENTS

5.1 The Supplier acknowledges that the Authority has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services (the "**Statement of Information Risk Appetite**").

5.2 The Authority's Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.

5.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Accreditation of the Core Information Management System.

6 ACCREDITATION OF THE CORE INFORMATION MANAGEMENT SYSTEM

6.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 6.

6.2 The Accreditation shall be performed by the Authority or by representatives appointed by the Authority and/or any Authority Service Recipient.

6.3 Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall comply with, and be subject to approval by the Authority in accordance with, this Paragraph 6 (the "**Risk Management Documentation**").

6.4 The Risk Management Documentation shall be structured in accordance with the template as set out in Annex 3 and include:

(a) the Accreditation Plan, which shall include:

(i) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Authority for review and staged approval; and

(ii) the date by which the Supplier is required to have received a Risk Management Approval Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 6.7(a);

(b) a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

(c) a completed ISO 27001:2022 Statement of Applicability for the Core Information Management System;

(d) the process for managing any security risks from Sub-contractors authorised by the Authority and/or any Authority Service Recipient with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) and any system that interfaces or connects to the Services and could directly or indirectly have an impact on that Information, data and/or the Services;

(e) unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority and/or any Authority Service Recipient or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(f) the Required Changes Register;

(g) evidence that the Supplier and each applicable Services Sub-contractor is compliant with the Certification Requirements; and

(h) a Personal Data Processing Statement.

6.5 If the Risk Management Documentation submitted to the Authority pursuant to Paragraph 6.3 (or Paragraph 6.10, as applicable) is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Risk Management Documentation is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 6.4 shall be deemed to be reasonable.

6.6 To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:

(a) access to the Sites (in particular sites in which key hubs of Supplier Personnel working on the Services are located but excluding public cloud data centres), ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

(b) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to enable the Authority to establish that the Core Information Management System is compliant with the Risk Management Documentation.

6.7 The Authority shall, by the relevant date set out in the Accreditation Plan, review the identified risks to the Core Information Management System and issue to the Supplier either:

(a) a Risk Management Approval Statement which will then form part of the Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

(b) a rejection notice stating that the Authority considers that the residual risks to the Core Information Management System have not been reduced to a level acceptable by the Authority and the reasons why ("**Risk Management Rejection Notice**").

6.8 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

(a) address all of the issues raised by the Authority in such notice; and

(b) notify the Authority that the Core Information Management System is ready for an Accreditation Decision.

6.9 If the Authority determines that the Supplier's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Authority may (where it can demonstrate that the risks or deficiencies are material to the Authority or Authority Service Recipients) terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(c).

6.10 The process set out in Paragraph 6.7 and Paragraph 6.8 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Agreement.

6.11 The Supplier acknowledges that it shall not be permitted to use the Core Information Management System to Process Authority Data prior to receiving a Risk Management Approval Statement.

6.12 The Supplier shall keep the Core Information Management System and Risk Management Documentation under review and shall update the Risk Management Documentation annually in accordance with this Paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 6.13.

6.13 The Supplier shall notify the Authority within 2 Working Days after becoming aware of the following, to the extent that it affects (or could reasonably be expected to affect) the Authority, an Authority Service Recipient, Authority Data, or the Services:

(a) a significant change to the components or architecture of the Core Information Management System;

(b) a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

(c) a change in the threat profile;

(d) a Sub-contractor failure to comply with the Core Information Management System code of connection;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Core Information Management System;

(g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns,

update the Required Changes Register and provide the updated Required Changes Register to the Authority for review and approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Authority. The Parties shall agree a definition of 'significant' (for the purposes of this Paragraph 6.13) as part of the Accreditation Plan.

6.14 If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:

(a) immediately cease using the Core Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority's written directions; and

(b) where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(c).

6.15 The Supplier shall review each Change Request against the Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

6.16 The Supplier shall be solely responsible for the costs associated with developing and updating the Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Accreditation process.

7 CERTIFICATION REQUIREMENTS

7.1 The Supplier shall ensure, at all times during the Term, that the Supplier and any Sub-contractor with access to Authority Data or who will Process Authority Data are certified as compliant with:

(a) ISO/IEC 27001:2022 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2022 (the scope of such certification to cover the Services and supporting governance);

(b) ISO 27017;

(c) Data Security and Protection Toolkit (DSPT); and

(d) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Authority Data. Any exceptions to the flow-down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.

7.2 The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2022; and

(b) are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

7.3 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.

7.4 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

(a) immediately ceases using the Authority Data; and

(b) procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.

8 SECURITY TESTING

8.1 The Supplier shall, at its own cost and expense:

(a) procure a CHECK IT Health Check of the Core Information Management System (an "**IT Health Check**") by a NCSC approved member of the CHECK Scheme:

(i) prior to it submitting the Risk Management Documentation to the Authority for an Accreditation Decision;

(ii) if directed to do so by the Authority in accordance with Paragraph 8.2; and

(iii) once every 12 months during the Term.

(b) conduct vulnerability scanning and assessments of the Core Information Management System monthly (and the Supplier shall comply with Cyber Assessment Framework (CAF), including taking steps to comply with the CAF from the commencement of the Contract);

(c) conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a Supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

(d) conduct such other tests as are required by:

(i) any Vulnerability Correction Plans;

(ii) the ISO27001 certification requirements;

(iii) the Risk Management Documentation; and

(iv) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a "**Security Test**").

8.2 The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.3 In relation to each IT Health Check, the Supplier shall:

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

(c) in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(i) prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

- how the vulnerability will be remedied;
- the date by which the vulnerability will be remedied;
- the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(ii) comply with the Vulnerability Correction Plan; and

(iii) conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

8.4 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 8.4, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.5 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.3, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.6 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information System and/or the Supplier's compliance with the Risk Management Documentation ("**Authority Security Tests**"). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test.

8.7 The Authority: (a) shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test; and (b) acknowledges that its representatives witnessing the Security Tests or carrying out Authority Security Tests in accordance with Paragraphs 8.5 or 8.6 shall not be entitled, as part of such tests, to view or access any Confidential Information of any of the Supplier's customers.

8.8 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If an Authority Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.9 Without prejudice to the provisions of Paragraph 8.3(c), where any Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Core Information Management System and/or the Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. To the extent that the actual or potential Breach of Security or weaknesses affects (or could reasonably be expected to affect) the Authority, an Authority Service Recipient, Authority Data, or the Services, and subject to the Authority's prior written approval, the Supplier shall implement such changes to the Core Information Management System and/or the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

8.10 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Risk Management Documentation in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

(a) has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

(b) would have been avoided had the Authority given its approval to the implementation of such proposed changes.

8.11 For the avoidance of doubt, where a change to the Core Information Management System and/or the Risk Management Documentation is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

8.12 If any repeat Security Test carried out pursuant to Paragraph 8.9 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(c).

8.13 The Supplier shall, by 31 March of each year during the Term, provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Agreement; and

(b) the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

9 VULNERABILITIES AND CORRECTIVE ACTION

9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

9.2 The severity of vulnerabilities for Supplier Software and Third Party Software shall be categorised by the Supplier as ‘Critical’, ‘Important’, ‘Medium’ and ‘Low’ by aligning these categories to the vulnerability scoring according to the agreed method in the Risk Management Documentation and using the appropriate vulnerability scoring systems including:

(a) the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

(b) Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.

9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:

(a) 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;

(b) 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’;

(c) 90 days after the public release of patches for those vulnerabilities categorised as ‘Medium’; and

(d) Vulnerabilities categorised as ‘Low’ will be patched as determined by the Supplier’s information security team.

9.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 9.3 shall be extended where:

(a) the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

(b) the application of a ‘Critical’ or ‘Important’ security patch adversely affects the Supplier’s ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Risk Management Documentation.

9.5 The Risk Management Documentation shall include provisions for major version upgrades of all Supplier Software and Third Party Software to be kept up to date such that all Supplier Software and Third Party Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

9.6 The Supplier shall:

(a) implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent NHS Body;

(b) promptly notify NCSC of any actual or sustained attempted Breach of Security;

(c) ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

(d) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;

(e) pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation;

(f) from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 9.3 for applying patches to vulnerabilities in the Core Information Management System;

(g) propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

(h) remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and

(i) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

9.7 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 9.3, the Supplier shall immediately notify the Authority.

9.8 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 9.3, such failure shall (subject to Paragraph 9.4) constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(c).

10 MALICIOUS SOFTWARE

10.1 The Supplier shall install and maintain anti-Malicious Software or procure that latest versions of anti-virus definitions and anti-Malicious Software is installed and maintained on any devices, which may Process Authority Data and ensure that such anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced , to identify, contain the spread of, and minimise the impact of Malicious Software.

10.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

10.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

(b) otherwise by the Authority.

11 BREACH OF SECURITY

11.1 If either Party becomes aware of a Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Risk Management Documentation.

11.2 The security incident management process set out in the Risk Management Documentation shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security to:

(a) immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) necessary to:

(i) minimise the extent of actual or potential harm caused by such Breach of Security;

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;

(iii) apply a tested mitigation against any such Breach of Security or potential Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier’s ability to deliver the Services so as to meet any Key Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Key Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(iv) prevent a further Breach of Security in the future exploiting the same root cause failure;

(b) as soon as reasonably practicable and, in any event, within 2 Working Days (or such other timescale as is be reasonably agreed by the Parties, to reflect the complexity of the Breach of Security) following the Breach of Security, provide to the Authority full details of the Breach of Security (**Incident Report**), including a root cause analysis where required by the Authority; and

(c) promptly deal with any questions raised by the Authority or other matters arising from the Incident Report, and regularly update the Incident Report over the period during which the Breach of Security persists or during which mitigations against the Breach of Security are being executed or implemented.

11.3 In the event that any action is taken in response to a Breach of Security which occurred as a result of non-compliance of the Information System and/or the Risk Management Documentation with the Baseline Security Requirements and/or this Agreement, then such action and any required change to the Information System and/or Risk Management Documentation shall be completed by the Supplier at no cost to the Authority.

11.4 If the Supplier fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(c).

12 DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

12.1 In addition to the obligations on the Supplier set out Clause 23 (Protection of Personal Data) in respect of Processing Personal Data and compliance with the Data Protection Legislation, the Supplier shall:

(a) Process Authority Data only at the Sites and such Sites must not be located outside of the European Union or United Kingdom (the Supplier ensuring that: (a) any production environments (Authority's and Authority Service Recipients' Data Platform tenants) are only located within the United Kingdom; and (b) suitable controls are in place to ensure that those production environments are only accessible from within (and only by Supplier Personnel within) the United Kingdom except where the Authority and the relevant Authority Service Recipient has given its consent to a transfer of the Authority Data to outside of the European Union in accordance with Clause 23;

(b) on demand, provide the Authority and/or any Authority Service Recipient with all Authority Data in an agreed open format;

(c) have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority and/or any Authority Service Recipient; and

(e) securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as directed by the Authority or any Authority Service Recipient.

Annex 1: Baseline Security Requirements

1 SECURITY CLASSIFICATION OF INFORMATION

If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

1.1 OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority and/or any Authority Service Recipient from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

1.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority and/or any Authority Service Recipient prior to receipt of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority and/or any Authority Service Recipient from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 END USER DEVICES

2.1 The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority and/or any Authority Service Recipient except where the Authority and/or any Authority Service Recipient has given its prior written consent to an alternative arrangement.

2.2 The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

3 NETWORKING

The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

4 PERSONNEL SECURITY

4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. Where any Supplier Personnel are based outside of the United Kingdom (subject at all times to Paragraph 12.112.1(a) of Schedule 2.4), the Supplier shall undertake equivalent pre-employment checks to the extent that they are permitted and applicable under local laws.

4.2 The Authority and/or any Authority Service Recipient and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority and/or any Authority Service Recipient to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which is classified as OFFICIAL-SENSITIVE.

4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority and/or any Authority Service Recipient has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

5 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

5.1 The Supplier shall operate an access control regime to ensure:

() all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

(a) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

5.2 The Supplier shall apply the ‘principle of least privilege’ when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

5.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority and/or any Authority Service Recipient on request.

6 AUDIT AND PROTECTIVE MONITORING

6.1 The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

6.2 The Supplier and the Authority and/or any Authority Service Recipient shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

6.3 The retention periods for audit records and event logs must be agreed with the Authority and/or any Authority Service Recipient and documented in the Risk Management Documentation.

7 SECURE ARCHITECTURE

7.1 The Supplier shall design the Core Information Management System in accordance with:

() the NCSC "Secure Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/collection/cyber-security-design-principles;

(a) the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(b) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority and/or any Authority Service Recipient to securely manage the Authority's and/or any Authority Service Recipient’s use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority and/or any Authority Service Recipient with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors;

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

Annex 2

CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

See Schedule 4.1

Annex 3

Risk Management Documentation Template

Author:

Owner:

Date:

Version:

1 EXECUTIVE SUMMARY

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

Change History

Version Number	Date of Change	Change made by	Nature and reason for change

References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

ID	Document Title	Reference	Date
1.			
2.			
3.			

2 SYSTEM DESCRIPTION

2.1 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

< Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2022) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

3 RISK ASSESSMENT

3.1 Accreditation/Assurance Scope

<This section describes the scope of the Accreditation/Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SIRO/SRO and included here.>

3.3 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.>

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4 IN-SERVICE CONTROLS

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include at least:

a) information risk management and timescales and triggers for a review;

b) contractual patching requirements and timescales for the different priorities of patch;

c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;

d) configuration and change management;

e) incident management;

f) vulnerability management;

g) user access management; and

h) data sanitisation and disposal.>

5 SECURITY OPERATING PROCEDURES (SYOPS)

< If needed any SyOps requirements should be included and referenced here.>

6 MAJOR HARDWARE AND SOFTWARE AND END OF SUPPORT DATES

< This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	🟧

7 INCIDENT MANAGEMENT PROCESS

<The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8 SECURITY REQUIREMENTS FOR USER ORGANISATIONS

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 REQUIRED CHANGES REGISTER

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the {●} capability.	Authority name			Open

10 PERSONAL DATA PROCESSING STATEMENT

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority and/or any Authority Service Recipient; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority and/or any Authority Service Recipient; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach.>

11 ANNEX A. ISO27001 AND/OR CYBER ESSENTIAL PLUS CERTIFICATES

<Any certifications relied upon should have their certificates included>

12 ANNEX B. CLOUD SECURITY PRINCIPLES ASSESSMENT

<A spreadsheet may be attached>

13 ANNEX C. PROTECTING BULK DATA ASSESSMENT IF REQUIRED BY THE AUTHORITY/CUSTOMER

<A spreadsheet may be attached>

14 ANNEX E. LATEST ITHC REPORT AND VULNERABILITY CORRECTION PLAN

SCHEDULE 2.5

INSURANCE REQUIREMENTS

Insurance Requirements

1 OBLIGATION TO MAINTAIN INSURANCES

1.1 Without prejudice to its obligations under this Agreement, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in ANNEX 1 and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.

1.2 The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.

1.3 The Insurances shall be taken out and maintained with insurers who are:

(a) of good financial standing;

(b) appropriately regulated;

(c) regulated by the applicable regulatory body and is in good standing with that regulator; and

(d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.

2 GENERAL OBLIGATIONS

Without limiting the other provisions of this Agreement, the Supplier shall:

(a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

(b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

(c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 FAILURE TO INSURE

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority and/or any Authority Service Recipient may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority and/or any Authority Service Recipient shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 EVIDENCE OF INSURANCES

The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Agreement.

5 CANCELLATION

5.1 Subject to Paragraph 5.2, the Supplier shall notify the Authority in writing promptly upon the Supplier's receipt of any proposed, and any notification of, cancellation, suspension, termination or non-renewal of any of the Insurances.

5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 5.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6 INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

6.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services or this Agreement for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services or this Agreement, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

6.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Agreement and shall allow the Authority and/or any Authority Service Recipient to review such register at any time.

6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

ANNEX 1: REQUIRED INSURANCES

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority or any Authority Service Recipient is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of £100,000 relating to or arising out of the provision of the Services or this Agreement on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART B: UNITED KINGDOM COMPULSORY INSURANCES

The Supplier shall meet its insurance obligations under applicable Law in full, including, United Kingdom employers' liability insurance and motor third party liability insurance.

PART C: ADDITIONAL INSURANCES

Policy	**Minimum limit of indemnity**
Public liability	£10m in the aggregate per annum
Professional Indemnity	[Redacted under FOIA s43, Commercial interests] in the aggregate per annum
Cyber Liability Insurance	[Redacted under FOIA s43, Commercial interests] in the aggregate per annum

SCHEDULE 2.6

AUTHORITY SERVICE RECIPIENTS

1 INTRODUCTION

1.1 The Services require the rollout of and use of Services and the Data Platform by Authority Service Recipients.

1.2 The Parties have agreed the terms of this Schedule to regulate the relationship between the Authority, the Supplier and Authority Service Recipients.

2 MEMORANDUM OF UNDERSTANDING

2.1 The Authority will enter into MoUs in a form not materially different from the form set out in the Annex to this Schedule with each Authority Service Recipient provided access to the Data Platform under this Agreement.

2.2 The Authority acknowledges that each MoU requires Authority Service Recipient compliance with the Platform Use Terms.

3 CHARGES FOR SERVICES

3.1 The Supplier acknowledges that

(a) the Authority is the contracting authority for Service provision and is responsible for payment of Charges;

(b) the Authority assumes no liability for the acts or omissions of Authority Service Recipients;

(c) no further charges are payable in respect of Authority Service Recipient's use of the Data Platform or any Services other than those set out in Schedule 7.1 (*Charges and Invoicing*).

3.2 Other than as set out in this Agreement, the Supplier will not (without the prior consent of the Authority or as otherwise agreed by the Parties in writing) approach in relation to or agree the incurring of charges by:

(a) Deployed Authority Service Recipients, in relation to any Services;

(b) NHS Bodies subject to the Authority’s supervision, in relation to the provision of software products operating on top of Palantir Foundry and listed in the Inventory unless the Supplier: (i) notifies the Authority of its intention to bid on a relevant commercial opportunity; and (ii) complies with a mutually agreed policy for such commercial approach.

3.3 The Supplier acknowledges the principles of collaboration and Programme behaviours set out in the Agreement (and in particular in accordance with the Collaborative Behaviours and FDP Relationship and Collaboration Charter) and agrees to apply them to the establishment of Data Platform services and Products at each Tenancy and accordingly acknowledges that Data Connectors should be designed on a "build once, deploy many" basis, reusing Data Connectors between Tenants, using standard interfaces and APIs where possible and where they do not exit, integrating with a component layer using standard interfaces; and that pricing for any Build Services or deployment of the Data Platform to a new Authority Service Recipient is consistent with those principles.

4 DATA PROCESSING

4.1 The Supplier will enter into Data Processing Agreements with Authority Service Recipients.

4.2 The Supplier will engage and discuss with Authority Service Recipients the details required for the completion of annexes to DPAs describing the details of relevant processing.

4.3 The Authority will discuss with and support Authority Service Recipients in the standardisation of processing instructions to the Supplier for the purposes of efficient finalisation of DPAs.

5 USERS BENEFITTING FROM THE AGREEMENT

5.1 The Authority acknowledges that as third party beneficiaries of Services under the Agreement, use by Authority Service Recipient of the Data Platform and the Services is subject to the terms and conditions of the Agreement, including its exclusions and limitations of liability, and compliance with the Platform Use Terms.

5.2 The Authority undertakes not to take or omit to take any action designed to prevent Supplier enforcing an MoU as a third party beneficiary.

5.3 The Authority undertakes to discuss and agree with the Supplier proposed material changes to the form of the MoU where these affect the terms on which Users use the Data Platform.

5.4 The Parties acknowledge that the limits on liability in Clause 25 of the Agreement apply to Supplier's liability to the Authority and any Authority Service Recipient in aggregate for claims in contract, statute, tort (including negligence) or otherwise that relate to or arise in connection with the provision of Services under this Agreement, all DPAs, the Platform Use Terms and any other agreements made between Supplier and the Authority, Authority Service Recipients or other third parties under or in connection with this Agreement.

ANNEX

FORM OF MEMORANDUM OF UNDERSTANDING

MEMORANDUM OF UNDERSTANDING

relating to the

NHS FEDERATED DATA PLATFORM

Title Memorandum of Understanding relating to the Federated Data Platform

Date *[Insert date of signature by last party to sign]*

Parties

(1) **NHS ENGLAND** of 7-8 Wellington Place, Leeds LS1 4AP (**NHS England**);

(2) **[*Insert name of FDP User Organisation*]** of {l} (the **FDP User Organisation**)

A. NHS England has procured the NHS Federated Data Platform (the **Data Platform**) and the NHS-PET Solution (**NHS-PET**) exercising its statutory powers (including under section 270 of the Health and Social Care Act 2012 (**HSCA 2012**) and sections 2(2), 13D, 13K and 1H(2) of the National Health Service Act 2006 (**NHS Act**)) to provide services effectively, efficiently and economically in the promotion of a comprehensive health service.

B. NHS England wishes to provide the Data Platform to NHS Bodies and where applicable, to Commissioned Health Service Organisations, such as the FDP User Organisation, in order that the FDP User Organisation may use the Data Platform to utilise Products in the pursuit of their functions and data analytics techniques and data ontologies developed by NHS England, and deploy analytics tools enabling FDP User Organisation staff to collect, engineer, assure, analyse, manipulate, interpret and display data integrating information from FDP User Organisation systems (**User Organisation Systems**).

C. User Organisation Systems are supported by various third party contractors (**User Organisation System Contractors**).

D. NHS England and FDP User Organisations will use NHS-PET to record data flows into the Data Platform and where required to treat data flows to de-identify them.

E. The Data Platform is supported by Palantir Technologies UK, Ltd. (the **Platform Contractor**) and NHS-PET by IQVIA Limited (the **NHS-PET Contractor**) and together with the User System Contractors, the **Contractors**) (and the Platform Contractor and the NHS-PET Contractor together referred to as the **FDP Contractors**).

F. The Parties agree to comply with and acknowledge the FDP Information Governance Framework in respect of data processing under this Memorandum of Understanding (**MoU**).

G. The purpose of this MoU is to establish funding, technical and information governance arrangements for the use of the Data Platform and to set out the terms on which the FDP User Organisation may use the Data Platform and NHS-PET, entered by the parties as an NHS contract (as referred to in the NHS Act).

Terms This MoU incorporates the terms and conditions (**Terms**), and Schedules, set out below.

SIGNED BY the parties acting by their authorised representatives to show their agreement to the terms of this MoU

SIGNED for and on behalf of **NHS England**

SIGNED for and on behalf of **FDP User Organisation**

Table of contents

Clause heading and number Page number

TERMS AND CONDITIONS

1. DEFINITIONS AND INTERPRETATION

1.1 In these Terms the following words and phrases bear the meanings given to them below and terms defined in the MoU bear the meaning given to them there unless the context otherwise requires.

Affiliate in respect of a person refers to any person they Control, which Controls them, or is under common Control with them;

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 Information all confidential information (however recorded or preserved) disclosed by a Party to another Party and their Representatives whether before or after the date of this agreement in connection with the MoU;

Contractors as described on the front page of the MoU;

Control a person's ability to direct the affairs of another whether through exercise of management control or voting rights, the ability to appoint directors or other officers, ownership of equity interests or any other means;

Data Platform as described on the front page of the MoU;

Data Principles the FDP Data Principles set out in the FDP Information Governance Framework;

Data Processing Agreement as defined in clause 7.6;

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;

EIR as described in clause 17.1;

FDP Contract refers to the Platform Contract and/or the NHS-PET Contract, as the case may be;

FDP Contractor as described on the front page of the MOU;

Data Governance Group a national group established by NHS England to provide oversight to the approach to data processing and sharing across all Instances of the Data Platform and NHS-PET which will include membership from across FDP User Organisations as detailed in the FDP Information Governance Framework;

FDP Information Governance Framework the information governance framework set out in the FDP Information Governance Framework Document V1.0 (as the same may be updated from time to time);

FDP Solutions the Data Platform and the NHS-PET Solution;

FOIA as described in clause 17.1;

Funding Plan as described in clause 5.2;

MoU the memorandum of understanding incorporating these Terms;

NHS Bodies has the meaning given in the NHS Act;

Commissioned Health Service Organisations 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;

NHS-PET Contract the agreement between NHS England and the NHS-PET Contractor in relation to the provision of the NHS-PET Solution;

NHS-PET Solution as described on the front page of the MoU;

Scope Document as defined in clause 4.1;

Platform Contract the agreement between NHS England and the Platform Contractor in relation to the provision of the Data Platform;

Platform Contractor as described on the front page of the MoU;

Product a product providing specific functionality enabling a solution to a business problem of the FDP User Organisation operating on the Data Platform;

Representatives the officers, employees and individual contractors of a Party authorised by it to act in relation to the MoU;

Services services associated with the Data Platform;

Subcontract a contract or agreement between the Platform Contractor and a third party, under which that third party agrees to provide to the Platform Contractor any part of the Services or assist the Platform Contractor in the Platform Contractor's provision of any part of the Services under the Platform Contract;

Subcontractor a third party with whom the Platform Contractor enters into a Subcontract;

Subcontractor Personnel individuals employed or engaged in the performance of a Subcontract;

User Organisation System Contract as described in clause 6.2.1;

User Organisation System Contractors as described on the front page of the MoU; and

User Organisation Systems as described on the front page of the MoU.

1.2 The Schedules to the MoU are an integral part of the MoU and a reference to the MoU includes a reference to the Schedules; words following the words "includes" or "including" are read without limitation; references to the singular include the plural and a reference to a "person" includes any natural or legal person whether incorporated or not.

2. PURPOSE

2.1 The Parties recognise that the deployment of the Data Platform requires them to establish and operate data sharing and information governance arrangements consistent with the Data Principles and complying with Data Protection Legislation.

2.2 The Parties intend to be bound by the terms of the MoU.

2.3 The Parties shall (and shall procure that any of their Representatives involved in the performance of the Parties' obligations under the MoU) comply with the Data Protection Legislation in connection with the MoU.

3. USE OF THE DATA PLATFORM AND THE NHS-PET SOLUTION

3.1 NHS England agrees to procure the use of the Data Platform and the NHS-PET Solution for the FDP User Organisation, without end user or other charges payable by the FDP User Organisation.

3.2 The FDP User Organisation agrees to comply with the authorised user terms applying to the Data Platform set out in **Schedule 1** and those applying to the NHS-PET Solution set out in **Schedule 2**.

3.3 The Parties may agree the FDP User Organisation's access to and use of Products and will record the Products to which the FDP User Organisation has access by means of an addendum in the form set out in **Schedule 4** unless the parties otherwise agree.

4. PERFORMANCE AND REPORTING

4.1 The Parties may agree a project initiation document (a **Scope Document**) detailing the principles and their respective responsibilities in relation to the implementation of Products, including project plans, delivery, resourcing and technical assumptions and dependencies on the FDP User Organisation in relation to Product implementation and funding. Each Party shall perform its obligations and responsibilities set out in a Scope Document.

4.2 The FDP User Organisation agrees to provide to NHS England on request and in such form as it may request information regarding its use of Products in order for NHS England to review and evaluate the Data Platform. Unless a data sharing arrangement as described in clause 7 is agreed, such information will be aggregated and not identify any person and the FDP User Organisation is not required to provide any personal data under such an information request.

5. FUNDING

5.1 NHS England may agree in a Funding Plan to fund certain activities of the FDP User Organisation in order to deploy Products.

5.2 A Funding Plan shall set out:

5.2.1 the activities of the FDP User Organisation to which the funding is to be applied;

5.2.2 the targets and objectives that the funding is intended to achieve;

5.2.3 the arrangements for monitoring and reporting by the FDP User Organisation to NHS England in relation to the funding;

5.2.4 the arrangements for invoicing, transfer or other means of disbursement of the funding to the FDP User Organisation by NHS England;

5.2.5 if applicable, the financial years to which the funding is allocated and the capital or revenue nature of the funding and any associated financial management requirements of NHS England.

5.3 The FDP User Organisation shall apply funding in accordance with and comply with the terms of a Funding Plan.

6. CONTRACTS

6.1 The FDP User Organisation agrees to collaborate with NHS England in relation to the design, contracting and implementation of changes to the User Organisation Systems required in order to enable the use of the FDP Solutions and Products. The parties intend to make arrangements with User Organisation System Contractors centrally in order that such changes are funded once and implemented consistently across all implementations of a particular electronic patient record or other clinical system provider's systems.

6.2 Where a Funding Plan requires activity to be undertaken by a User Organisation System Contractor:

6.2.1 the FDP User Organisation shall obtain the approval of NHS England to the contractual documentation binding the User Organisation System Contractor to the relevant activity (**User Organisation System Contract**) consistently with the objectives described in this clause;

6.2.2 the FDP User Organisation shall notify NHS England of any material failure or delay by the User Organisation System Contractor to comply with a User Organisation System Contract.

6.3 The FDP User Organisation acknowledges that NHS England is responsible for contractual arrangements with each FDP Contractor and the FDP User Organisation will not take any action or make any commitment with or in respect of a FDP Contractor's provision of their services without NHS England's approval.

7. GOVERNANCE, DATA PROCESSING AND DATA SHARING

7.1 NHS England will establish governance arrangements for the FDP Solutions and the FDP User Organisation may input into governance through its regional delivery managers.

7.2 The Parties will comply with the FDP Information Governance Framework.

7.3 The Parties will observe the Data Principles in the performance of the MoU and will in respect of data processing contemplated by the MoU:

7.3.1 collaborate in the preparation and updating of data protection impact assessments under Data Protection Legislation;

7.3.2 discuss and agree the basis of processing of personal data and legal grounds under which, and purposes for which, data is processed;

7.3.3 establish an NHS FDP System IG Group, Data Governance Group, FDP Specialist External IG Advisory Group and such other arrangements as may be desirable to co-ordinate the implementation and operation of the Data Principles and the FDP Information Governance Framework and ensure that the rights and freedoms of data subjects and compliance with Data Protection Legislation and the Common Law Duty of Confidentiality are considered at all times;

7.3.4 agree the terms of the joint controller arrangements setting out their respective responsibilities for compliance with Data Protection Legislation in relation to the design, governance and service management of the Data Platform and reflect this in the FDP Information Governance Framework (**Joint Controller Arrangement**);

7.3.5 not to share any personal data through the Data Platform with the other Party without first agreeing the legal basis for such data to be shared, and unless the personal data is shared by the FDP User Organisation with NHS England under section 259 of the HSCA 2012, to enter into a written data sharing agreement before sharing the personal data;

7.3.6 co-ordinate and collaborate responses to requests from data subjects in relation to the exercise of their rights under Data Protection Legislation and address complaints under such legislation. The parties intend that the FDP User Organisation is responsible for such co-ordination in relation to all and any personal data processed in their Instance of the Data Platform and NHS-PET and that NHS England is responsible for such co-ordination in relation to all personal data processed in the national Instance of the Data Platform and NHS-PET and for responses to data subjects in relation to exercise of their rights in relation to processing carried out further to the Joint Controller Arrangement;

7.3.7 ensure that appropriate information security practices, technological and organisational measures and procedures are applied to keep personal data secure;

7.3.8 except where expressly agreed by NHS England or as permitted by the FDP Information Governance Framework, ensure that any personal data stored in the Data Platform and NHS-PET is not accessible by the parties' own personnel or contractors from outside the UK; and

7.3.9 agree terms with each FDP Contractor setting out the FDP Contractor's processing instructions and the responsibilities of the parties to the relevant data processing agreement in line with the FDP Information Governance Framework.

7.4 NHS England acknowledges that the FDP User Organisation will not share personal data with NHS England unless and until a legal basis and other requirements of Data Protection Legislation have been met and data sharing agreements reflecting those requirements put in place, as described in clause7.3.5.

7.5 The Parties agree to ensure that each FDP Contractor is engaged under data processing agreements meeting the requirements of Data Protection Legislation.

7.6 The FDP User Organisation will enter into data processing agreements with each FDP Contractor (and such other controllers as may be necessary) in the form set out in Schedule 3 (**Data Processing Agreement**). The FDP User Organisation and FDP Contractors will agree annexes to their Data Processing Agreements in relation to any Product or additional or specific dataflows relating to Services provided further to this MoU before any such personal data is processed by the FDP Contractor.

7.7 The Parties will discuss and collaborate on the preparation and maintenance of equalities impact assessments and other assessments or reviews of the effect of the FDP Solutions on their functions and duties as may be required.

8. RELATIONS WITH FDP CONTRACTORS

8.1 NHS England has procured the support of the FDP Contractors for the FDP Solutions.

8.2 NHS England represents to the FDP User Organisation that the FDP User Organisation is entitled to use each FDP Solution as a third party beneficiary of the Platform Contract or, as the case may be, the NHS-PET Contract, on and subject to the terms of the MoU.

8.3 The FDP User Organisation acknowledges that the Platform Contractor is providing support for the Data Platform under the Platform Contract which includes provisions and restrictions regarding the use of the Data Platform and receipt of the Services, terms required by Data Protection Legislation in relation to the processing of personal data, and provisions and limitations on the Platform Contractor's liability for certain matters, all as set out in the Platform Contract and statements of work and other commitments made under it in respect of the Data Platform. The FDP User Organisation's use of the Data Platform and receipt of the Services is subject to all such provisions, restrictions, terms and limitations.

8.4 The FDP User Organisation acknowledges that the NHS-PET Contractor is providing support for the NHS-PET Solution under the NHS-PET Contract which includes provisions and restrictions regarding the use of the NHS-PET Solution, terms required by Data Protection Legislation in relation to the processing of personal data, and provisions and limitations on the NHS-PET Contractor's liability for certain matters, all as set out in the NHS-PET Contract and statements of work and other commitments made under it in respect of the NHS-PET Solution. The FDP User Organisation's use of the NHS-PET Solution is subject to all such provisions, restrictions, terms and limitations and the FDP Information Governance Framework.

8.5 NHS England undertakes to provide the FDP User Organisation with access to the FDP Contracts on its FutureNHS collaboration platform (or such other platform as may replace it from time to time).

8.6 The FDP User Organisation agrees to notify NHS England in the event that any issue or dispute arises in respect of the FDP User Organisation's use of a FDP Solution. NHS England agrees to facilitate the resolution of any such dispute with a FDP Contractor.

8.7 The FDP User Organisation agrees not to make any claim against a FDP Contractor under a Data Processing Agreement where such claim can be made under the relevant FDP Contract as a third party beneficiary and in any case without first notifying NHS England in accordance with clause 8.6 except in an urgent case where action is required to preserve the FDP User Organisation's rights or remedies or in order to comply with Data Protection Legislation and then provided that the FDP User Organisation immediately notifies NHS England of such claim further to clause 8.6.

8.8 Subject to clause 8.9, the FDP User Organisation agrees not to make any claim (and procure that none of its Affiliates make any claim) against any Subcontractor or any Subcontractor Personnel in connection with the Services (a **Subcontractor Claim**).

8.9 A Subcontractor Claim may only be made by NHS England and :

8.9.1 where it is not possible to bring the claim against the Platform Contractor; and

8.9.2 subject to the terms and conditions of the relevant Subcontract, including its exclusions and limitations of liability.

9. DISPUTE RESOLUTION

9.1 If a Party has any issues, concerns or complaints regarding the operation of the MoU that Party shall notify the other Party promptly and the Parties will seek to resolve the issue through discussion between them.

9.2 Subject as otherwise specifically provided for in the MoU, any dispute arising between the Parties out of or in connection with the MoU will be resolved in accordance with the provisions of this clause.

9.3 If the Parties are unable to resolve a dispute by discussion, they may appoint an independent facilitator to determine the dispute in accordance with clause 9.4.

9.4 The independent facilitator shall act on the following basis:

9.4.1 the independent facilitator shall decide the procedure to be followed in the determination and shall be requested to make their determination within 30 days of their appointment or as soon as reasonably practicable thereafter. The parties shall assist and provide the documentation that the independent facilitator requires for the purpose of the determination;

9.4.2 the determination process shall be conducted in private and shall be confidential;

9.4.3 The independent facilitator shall have its costs and disbursements met by the Parties.

9.5 The Parties recognise that any dispute or operation of this procedure will be without prejudice to and will not affect the statutory duties of each Party.

9.6 Nothing in this clause shall be construed as prohibiting a Party from applying to a court for interim injunctive relief where it considers that such a step is necessary to prevent irreparable harm to its interests.

10. COMPLIANCE

The Parties shall comply with applicable law in the performance of the MoU.

11. DECISION MAKING

Neither Party delegates to the other any decision or action or authorises the other Party to act in its name or as its agent further to the MoU.

12. TERM AND TERMINATION

12.1 The MoU shall commence on the date on which it is executed by the last Party to sign (the **Commencement Date**) and shall continue in force until termination by agreement in writing by the Parties.

12.2 On termination of the MoU:

12.2.1 The use of the FDP Solutions by the FDP User Organisation shall terminate;

12.2.2 The parties shall agree the closure and funding of activities under any uncompleted Funding Plans.

13. VARIATION

The MoU may only be varied by written agreement of the Parties signed by, or on behalf of, each of the Parties.

14. CHARGES AND LIABILITIES

14.1 Except as otherwise provided, the Parties shall each bear their own costs and expenses incurred in complying with their obligations under the MoU, including in respect of any losses or liabilities incurred due to their own or their Representatives' actions.

14.2 No Party intends that any other Party shall be liable for any loss it suffers as a result of the MoU.

15. NO PARTNERSHIP

Nothing in the MoU is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute any Party as the agent of another Party, nor authorise any of the Parties to make or enter into any commitments for or on behalf of the other Parties.

16. CONFIDENTIALITY

16.1 Subject to Clause 16.2, each Party shall keep the other Parties' Confidential Information confidential and shall not:

16.1.1 use such Confidential Information except for the purpose of performing its rights and obligations under or in connection with this agreement; or

16.1.2 disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this Clause.

16.2 The obligation to maintain confidentiality of Confidential Information does not apply to any Confidential Information:

16.2.1 which another Party confirms in writing is not required to be treated as Confidential Information;

16.2.2 which is obtained from a third party who is lawfully authorised to disclose such information without any obligation of confidentiality;

16.2.3 which a Party is required to disclose by judicial, administrative, governmental or regulatory process in connection with any action, suit, proceedings or claim or otherwise by applicable law, including the FOIA or the EIR;

16.2.4 which is in or enters the public domain other than through any disclosure prohibited by this agreement;

16.2.5 which a Party can demonstrate was lawfully in its possession prior to receipt from the another Party; or

16.2.6 which is disclosed by a Party on a confidential basis to any central government or regulatory body.

16.3 A Party may disclose the other party's Confidential Information to those of its Representatives who need to know such Confidential Information for the purposes of performing or advising on the Party's obligations under this agreement, provided that:

16.3.1 it informs such Representatives of the confidential nature of the Confidential Information before disclosure; and

16.3.2 it procures that its Representatives shall, in relation to any Confidential Information disclosed to them, comply with the obligations set out in this clause as if they were a party to this agreement,

16.3.3 and at all times, it is liable for the failure of any Representatives to comply with the obligations set out in this Clause.

17. FREEDOM OF INFORMATION

17.1 The Parties acknowledge that each is a public authority subject to the requirements of the Freedom of Information Act 2000 (**FOIA**) and the Environmental Information Regulations 2004 (**EIR**).

17.2 Each Party shall, in respect of any requests for information which touch on or relate to the MoU:

17.2.1 provide all necessary assistance and cooperation as reasonably requested by the other Parties to enable them to comply with their obligations under FOIA and EIR;

17.2.2 notify the other Parties of requests for information that it receives as soon as practicable and in any event within 5 days of receipt;

17.2.3 provide to the other Parties a copy of any information it holds and which is required in order to respond to a request for information within 5 days (or such other period as the Parties may reasonably specify) of any request for such Information;

17.2.4 not respond directly to a request for information unless without first consulting with the other Parties; and

17.2.5 comply with the working arrangements for handling FOIA and EIR requests for information set out in the FDP Information Governance Framework.

18. GOVERNING LAW AND JURISDICTION

18.1 The MoU shall be governed by and construed in accordance with the laws of England and Wales.

18.2 Subject to the provisions of Clause 9, the Parties agree that the courts of England shall have exclusive jurisdiction to hear and settle any action, suit, proceeding or dispute in connection with the MoU and irrevocably submit to the jurisdiction of those courts.

19. FURTHER ASSURANCE

19.1 Each Party shall do all things and execute all further documents necessary to give full effect to the MoU.

20. THIRD PARTY BENEFIT

20.1 Each FDP Contractor may enforce clauses 3.2, 8.3, 8.4 and 8.7 and Subcontractors and Subcontractor Personnel may enforce clauses 8.8 and 8.9 of these Terms as a third party. Only the consent of the FDP User Organisation and NHS England is required to a variation to the MoU.

SCHEDULE 1

PLATFORM USE TERMS

These Terms of Service (collectively with any attachments, addenda, or exhibits referenced herein, the "**Agreement**") apply to the provision of the Services to the Customer (each as defined below) by Palantir (each a "**Party**" and collectively the "**Parties**") under the Federated Data Platform programme procured and provided by NHS England ("**FDP**") and is effective as of the date of last signature of the relevant MOU binding the Customer and NHS England.

1. Certain Definitions.

1.1 "**Affiliate**" means an entity that, directly or indirectly, owns or controls or is owned or controlled by, or is under common ownership or control with, a Party as of the Effective Date and for as long as such entity remains directly or indirectly owned or controlled by the Party. As used herein, "**control**" means the power to direct, directly or indirectly, the management or affairs of an entity and "**ownership**" means the beneficial ownership of more than fifty percent of the voting equity securities or other equivalent voting interests of an entity.

1.2 "**Customer**" means the party identified in the MOU and which, subject to the terms of the MOU under which these Terms of Service are incorporated, is recipient of the Service.

1.3 "**Customer Data**" means any data (including aggregated or transformed versions thereof and analytical outputs), models, algorithms, analyses, transformation code or other content that is provided by, whether directly or indirectly from a third party, or created by Customer, or Users using the Service or Website, for integration, use, or other processing in or through the Service.

1.4 "**Data Connection Software**" means Palantir software provided for installation locally for Customer to connect Customer Data to the Service.

1.5 "**Documentation**" means any technical documentation for the Service made available in connection with the Service, including the technical documentation relevant to the Service available at the Website, updated from time to time at Palantir's sole discretion.

1.6 "**FDP Agreement**" means the agreement between Palantir and NHS England effective 22 November 2023 for the provision of services for FDP.

1.7 "**Intellectual Property Rights**" means all rights, title, and interest in and to any trade secrets, patents, copyrights, service marks, trademarks, know-how, trade names, rights in trade dress and packaging, moral rights, rights of privacy, rights of publicity, and any similar rights, including any applications, continuations, or registrations with respect to the foregoing, under the laws or regulations of any governmental, regulatory, or judicial authority.

1.8 "**MOU**" means a Memorandum of Understanding between NHS England and the Customer in relation to the Customer's participation in FDP and which specifies the Service and/or Professional Services (if applicable) to be provided by Palantir, including any attachments, addenda, or exhibits thereto.

1.9 "**Palantir**" means Palantir Technologies UK, Ltd.

1.10 "**Palantir Technology**" means the Service, Documentation, Data Connection Software, Sample Materials, Website, models, and application programming interfaces (APIs), provided or made available to Customer as a service in connection with this Agreement, and any improvements, modifications, derivative works, patches, upgrades, and updates thereto.

1.11 "**Sample Materials**" means any technology and materials provided or made available by Palantir to Customer for use with the Service, including sample code, software libraries, command line tools, data integration code, templates, and configuration files.

1.12 "**Service**" means Palantir's proprietary software-as-a-service offering(s) set forth in the FDP Agreement.

1.13 "**Taxes**" means any applicable sales, use, transaction, value added, goods and services tax, harmonized sales tax, withholding tax, excise or similar taxes, and any foreign, provincial, federal, state or local fees or charges, (including but not limited to, environmental or similar fees) duties, costs of compliance with export and import controls and regulations, and other governmental assessments, including any penalties and interest in respect thereof, imposed on, in respect of or otherwise associated with any transaction hereunder.

1.14 "**Term**" means the term for the provision of Palantir's services which shall be from the Effective Date until the earlier of termination or expiry of: (i) the MOU (or the relevant part thereof resulting in the Customer ceasing its participation in FDP or any successor programme); (ii) the FDP Agreement; and (iii) this Agreement.

1.15 "**Third Party Content**" means any third party data, services, or applications that interoperate with the Service which Palantir may, at Customer's sole discretion, facilitate the use of in connection with the Service and subject to an independent agreement between Customer and such third party.

1.16 "**Third Party Services**" means third party services that Palantir may utilize in the provision of the Service as set forth in the Documentation (or as otherwise agreed by the Parties).

1.17 "**Website**" means WWW.PALANTIR.COM or any other Palantir-owned domains, including any subdomains of the foregoing, and all software, applications, products, content, and services provided by Palantir at or through the Website.

2. Provision of Service.

2.1 Service Access. Palantir shall make available the Service to Customer, subject to the condition precedent set forth in Section 8.4, during the applicable Term solely for use by Customer and its Users in accordance with the terms and conditions of this Agreement and the Documentation for Customer's internal business purposes, or as otherwise set forth in an MOU.

2.2 Data Connection Software License. If applicable for use of the Service, and subject to the condition precedent set forth in Section 8.4, Palantir grants to Customer during the applicable Term a non-exclusive, nontransferable, non-sublicenseable, limited license to use the Data Connection Software for the sole purposes of using and connecting to the Service. Customer shall allow Palantir to access the Data Connection Software remotely as necessary to provide the Service.

2.3 Sample Materials License. Palantir may make available Sample Materials for use by Customer during the Term. If applicable, and subject to the condition precedent set forth in Section 8.4, Palantir grants to Customer during the applicable Term a non-exclusive, non-transferable, non-sublicenseable, limited license, to copy, modify, and use the Sample Materials solely to the extent necessary for Customer's use of the Service.

2.4 Usage Data. Palantir may collect and use metrics, analytics, statistics, or other data related to Customer's use of the Service (a) to provide and secure the Service for the benefit of Customer and (b) to analyze, maintain, support, and improve the Service (*provided* that in relation to (b) the data collected shall not include personal data or Customer Data).

2.5 Security. Palantir has established an Information Security Program ("**ISP**") designed to ensure strong practical security controls, and compliance with industry best practice standards and frameworks. A comprehensive list of Palantir's certifications can be found at https://www.palantir.com/information-security/ under "Compliance and Accreditation." The Palantir ISP additionally is aligned with NIST 800-53, TSC (Trust Service Criteria), and CIS (Center for Internet Security) frameworks and management systems. Palantir will make available to Customer upon written request (no more frequently than once per calendar year) Palantir's: (a) ISAE 3000/SSAE18 SOC2 TYPE II Report, (b) Penetration Test Attestation Letter, and (c) ISO 27001 Certificate. Palantir shall provide the above audit reports relating to Palantir's operating practices and procedures to the extent relevant to the Service. Customer acknowledges that Palantir's documentation noted in this Section and other related information are Palantir's Confidential Information hereunder.

2.6 Service Levels and Support. Palantir and NHS England have agreed service levels and support in the FDP Agreement that shall be applicable to the Service**.** This Agreement does not give Customer any rights to any updates or upgrades to the Palantir Technology or to any extensions or enhancements to the Palantir Technology developed by Palantir at any time in the future. Any supplemental software code or related materials that Palantir provides to Customer as part of any support services are to be considered part of the Palantir Technology and are subject to the terms and conditions of this Agreement**.**

2.7 Professional Services. Palantir shall provide Customer with implementation, enablement, training, or other professional services as specified in the MOU and the FDP Agreement ("**Professional Services**"). If the MOU specifies no Professional Services, Palantir may at its discretion (without an obligation to do so absent a separate agreement providing otherwise) provide Customer Professional Services. The performance of any Professional Services shall not affect ownership of the Palantir Technology and other materials provided by Palantir under this Agreement.

3. Customer Use of Service.

3.1 Accounts. Customer may provision accounts to access the Service ("**Accounts**") for its (a) employees, (b) contractors, (c) other users (including its Affiliates' employees or contractors) mutually agreed by the Parties (collectively, "**Users**"). Customer shall be responsible for (i) administering Accounts; (ii) using industry standard security measures to protect Accounts (including, without limitation, using multi-factor authentication); and (iii) any activity on Accounts and the monitoring of such activity on Accounts (only to the extent that such monitoring does not violate any other term of this Agreement or applicable law). Customer shall immediately de-activate any Account upon becoming aware of the compromise or unauthorized use thereof (and in such case promptly notify Palantir of such compromise or unauthorized use), or upon Palantir's reasonable request.

3.2 Data Protection. The Parties shall comply with the Data Processing Agreement entered into on or around the Effective Date of this Agreement ("**DPA**") and which may be supplemented by additional annexes relating to further products provided under the FDP programme. Customer shall be solely responsible for the accuracy, content, and legality of Customer Data and shall ensure that any integration of Customer Data into the Service complies with applicable laws and regulations, including but not limited to data localization requirements.

4. Acceptable Use.

4.1 Applicable Laws. Customer's access and use of the Service and Website, will not violate applicable laws of the United Kingdom or other laws applicable in the jurisdiction in which Customer is located, in which any natural persons who can be identified (directly or indirectly) by reference to the Customer Data (each, a "**Data Subject**") is located, or in which Customer Data is stored and it is solely Customer's responsibility for ensuring such compliance. Palantir may from time to time make available acceptable use policies, community guidelines, or similar policies, which shall become part of this Agreement following incorporation pursuant to the terms of the FDP Agreement.

4.2 Competitive Use. Customer will not use or access the Palantir Technology to develop, create, improve, or inform a product or service similar to or competitive with any product or service offered by Palantir now or in the future.

4.3 Export Controls. NOT USED.

4.4 Use of PII and/or PHI. If Customer uses or anticipates using Personally Identifiable Information ("PII"), Personal Data, Personal Information, or Protected Health Information ("PHI"), as defined under applicable law, in connection with the Service, Customer will follow the relevant guidance and best practices for protecting sensitive data in the Services set out in documentation available at https://www.palantir.com/docs/foundry/security/overview/. For the avoidance of doubt, this Section does not grant Customer permission to use the foregoing information in connection with the Service if an MOU expressly prohibits or restricts such use.

4.5 Use Cases. Customer will comply with the Use Case Restrictions available at https://palantir.pactsafe.io/legal-3791.html#template-wwpssoyww.

5. Proprietary Rights.

5.1 Customer Data Ownership. As between the Parties, Customer owns all rights, title, and interest, including all Intellectual Property Rights, in and to Customer Data and any modifications made thereto. Subject to the Agreement, Customer grants to Palantir a non-exclusive, worldwide, royalty-free right and license during the Term to process Customer Data solely to provide the Service and/or Professional Services. Customer further grants to Palantir a worldwide, perpetual, irrevocable, royalty-free right and license to use, distribute, disclose, and make and incorporate into the Palantir Technology any suggestions, enhancement request, recommendation, or other feedback provided by Customer or Users relating to the Palantir Technology (but this does not grant Palantir any such right and license in respect of any Intellectual Property Rights owned by NHS England or Customer further to the terms of the FDP Agreement or otherwise).

5.2 Palantir Ownership. As between the Parties and unless the terms of the FDP Agreement otherwise provide, Palantir owns all rights, title, and interest, including all Intellectual Property Rights, in and to the Palantir Technology, and any other related documentation or materials provided by Palantir and any derivative works, modifications, or improvements of any of the foregoing (including without limitation all Intellectual Property Rights embodied in any of the foregoing). Except for the express rights granted herein, Palantir does not grant any other licenses or access, whether express or implied, or any ownership rights to any Palantir Technology, software, services, or Intellectual Property Rights.

5.3 Restrictions. Customer will not (and will not allow any third party to): (a) gain or attempt to gain unauthorized access to the Service or Website or infrastructure, or any element thereof, or circumvent or interfere with any authentication or security measures of the Service or Website; (b) interfere with or disrupt the integrity or performance of the Service or Website; (c) access or attempt to gain access to another customer's data; (d) adversely impact the ability of other customers to use the Service; (e) transmit material containing software viruses or other harmful or deleterious computer code, files, scripts, agents, or programs through the Service or Website; (f) decompile, disassemble, scan, reverse engineer, or attempt to discover any source code or underlying ideas or algorithms of any Palantir Technology (except to the extent that applicable law expressly prohibits such a reverse engineering restriction, and in such case only upon prior written notice to Palantir); (g) provide, lease, lend, use for timesharing or service bureau purposes, or otherwise use or allow others to use the Service for the benefit of any third party; (h) use the Service or Website for any purpose that is not expressly permitted by this Agreement; (i) list or otherwise display or copy any code of any Palantir Technology, except for Sample Materials to the extent necessary for Customer's use of the Service; (j) copy any Palantir Technology (or component thereof) or develop any improvement, modification, or derivative work thereof, except for Sample Materials to the extent necessary for Customer's use of the Service; (k) include any portion of any Palantir Technology in any other service, equipment, or item; (l) perform penetration tests on the Service unless authorized by Palantir; (m) use, evaluate, or view the Palantir Technology for the purpose of designing, modifying, or otherwise creating any environment, software, models, algorithms, products, program, or infrastructure or any portion thereof, which performs functions similar to the functions of the Palantir Technology; (n) remove, obscure, or alter, or otherwise violate the terms of any copyright notice, trademarks, logos, and trade names and any other notices (including third party open source or similar licenses) or identifications that appear on or in any Palantir Technology and any associated media; (o) use the Website or Palantir Technology to engage in or advance any fraud or misrepresentation (including but not limited to providing fraudulent or misleading information in response to the MOU); or (q) use or access the Service for the purposes of engaging in or supporting spamming activities or communications, or marketing activities or communications in violation of the applicable laws prohibiting spam or otherwise governing transmission of marketing materials and/or communications. Notwithstanding the foregoing, or any statement to the contrary herein, Third Party Content may be made available with notices and open source or similar licenses from such communities and third parties that govern the use of those portions, and Customer hereby agrees to be bound by and fully comply with all such licenses; *however*, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all such Third Party Content.

6. Confidentiality. Each Party (the "**Receiving Party**") shall keep strictly confidential all Confidential Information of the other Party (the "**Disclosing Party**"), and shall not use such Confidential Information except for the purposes of this Agreement, and shall not disclose such Confidential Information to any third party other than disclosure on a need-to-know basis to the Receiving Party's directors, employees, agents, attorneys, accountants, subcontractors, or other representatives who are each subject to obligations of confidentiality at least as restrictive as those herein ("**Authorized Representatives**"). The Receiving Party shall use at least the same degree of care as it uses to prevent disclosure of its own confidential information, but in no event less than reasonable care. The Receiving Party may, without violating the obligations of the Agreement, disclose Confidential Information to the extent required by law (including freedom of information legislation), a valid court or government order, *provided* that in relation to a valid court or government order, the Receiving Party: (a) provides the Disclosing Party with reasonable prior written notice of such disclosure and (b) uses reasonable efforts to limit disclosure and to obtain, or to assist the Disclosing Party in obtaining, confidential treatment or a protective order preventing or limiting the disclosure, while allowing the Disclosing Party to participate in the proceeding. "**Confidential Information**" means (i) in the case of Palantir, Palantir Technology (including any information relating thereto); (ii) in the case of Customer, Customer Data; and (iii) any other information which by the nature of the information disclosed or the manner of its disclosure would be understood by a reasonable person to be confidential, in each case, in any form (including without limitation electronic or oral) and whether furnished before, on, or after the Effective Date; *provided*, *however*, that Confidential Information shall not include any information that (1) is or becomes part of the public domain through no act or omission of the Receiving Party or its Authorized Representatives; (2) is known to the Receiving Party at the earlier of the Effective Date or the time of disclosure by the Disclosing Party (as evidenced by written records) without an obligation to keep it confidential; (3) was rightfully disclosed to the Receiving Party prior to the Effective Date from another source without any breach of confidentiality by the third party discloser and without restriction on disclosure or use; or (4) the Receiving Party can document by written evidence that such information was independently developed without any use of or reference to Confidential Information. The Receiving Party shall be liable for any breaches of this Section by any person or entity to which the Receiving Party is permitted to disclose Confidential Information pursuant to this Section. The Receiving Party's obligations with respect to Confidential Information shall survive termination of this Agreement for five (5) years; *provided*, that the Receiving Party's obligations hereunder shall survive termination and continue in perpetuity, or as long as permitted by applicable law, with respect to any Confidential Information that is a trade secret under applicable law.

7. Fees and Payment; Taxes. The Service is deemed delivered upon the provision of access to Customer or for

Customer's benefit. Unless otherwise agreed by the Parties in writing, all fees will be invoiced to NHS England. The Customer is responsible for ensuring that it has a valid agreement with NHS England for incurring such fees whether in the MOU or elsewhere.

8. Term and Termination; Suspension.

8.1 Term. Unless specified otherwise in the MOU, this Agreement is effective for the Term.

8.2 Termination for Cause. Without limiting either Party's other rights, either Party may terminate this Agreement for cause (a) in the event of any material breach by the other Party of any provision of this Agreement and failure to remedy the breach (and provide reasonable written notice of such remedy to the non-breaching Party) within thirty (30) days following written notice of such breach from the non-breaching Party or (b) if the other Party seeks protection under any bankruptcy, receivership or similar proceeding or such proceeding is instituted against that Party and not dismissed within ninety (90) days. Except where an exclusive remedy is specified in this Agreement, the exercise by either Party of the right to terminate under this provision shall be without prejudice to any other remedies it may have under this Agreement or by law.

8.3 Effect of Termination. Upon any termination or expiration of this Agreement, except as specifically set forth below, all Customer's rights, access, and licenses granted to Palantir Technology shall immediately cease and Customer shall promptly return or destroy all Data Connection Software, Sample Materials, and Documentation, and all other Palantir Confidential Information, and, upon written request, certify its compliance with the foregoing to Palantir in writing within ten (10) days of such request. Upon termination or expiration of this Agreement, if requested by Customer, Customer shall, subject to the terms of this Agreement, FDP Agreement and the MOU, have access to the Service for thirty (30) days solely for the purpose of retrieving Customer Data. Palantir shall retain, subject to the other terms of this Agreement, and solely for security purposes, usage information and metadata related to the security of the Service, excluding Customer Data (except for security-related information such as IP addresses, usernames, log-in attempts, and search queries), for a period of two (2) years following the last event logged or such other period specified in the FDP Agreement. No termination or expiration of this Agreement shall limit or affect rights or obligations that accrued prior to the effective date of termination or expiration (including without limitation payment obligations) or the rights and obligations of the Parties and NHS England under the FDP Agreement. Sections 1, 4 (excluding Section 4.5), 5, 6, 7, 8, 9, 10, 12, 13, and 14 shall survive any termination or expiration of this Agreement.

8.4 Suspension of Services. If instructed or required to do so by NHS England under the FDP Agreement or any connected agreement or if Palantir reasonably determines that: (a) Customer's use of the Service or Website violates applicable law or otherwise violates a material term of this Agreement, Section 4 (Acceptable Use), and Section 5.3 (Restrictions); or (b) Customer's use of or access to the Service or Website poses a risk of material harm to Palantir or its other customers, Palantir reserves the right to disable or suspend Customer's access to all or any part of the Website and/or the Palantir Technology, subject to Palantir providing Customer notice of such suspension concurrent or prior to such suspension.

9. Indemnification.

9.1 Palantir Indemnification. Palantir shall defend Customer against any claim of infringement or violation of any Intellectual Property Rights asserted against Customer by a third party based upon Customer's use of Palantir Technology in accordance with the terms of this Agreement and indemnify and hold harmless Customer from and against reasonable costs, attorneys' fees, and damages, if any, finally awarded against Customer pursuant to a non-appealable order by a court of competent jurisdiction in such claim or settlement entered into by Palantir. If Customer's use of any of the Palantir Technology is, or in Palantir's opinion is likely to be, enjoined by a court of competent jurisdiction due to the type of infringement specified above, or if required by settlement approved by Palantir in writing, Palantir may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for Customer the right to continue using the Palantir Technology; or (c) if Palantir reasonably determines that options (a) and (b) are commercially impracticable, terminate this Agreement. The foregoing indemnification obligations of Palantir shall not apply: (i) if Palantir Technology is modified by or at the direction of Customer or Users, but only to the extent the alleged infringement would not have occurred but for such modification; (ii) if Palantir Technology is combined with non-Palantir products not authorized by Palantir, but only to the extent the alleged infringement would not have occurred but for such combination; (iii) to any unauthorized use of Palantir Technology, any use that is not consistent with the Documentation, any use that violates Section 4 (Acceptable Use), or use during any period of suspension (as set forth in Section 8.4); (iv) to any Customer Data; or (v) to any non-Palantir products or services.

9.2 Customer Indemnification. Customer shall defend Palantir against any third party claim asserted against Palantir arising from or relating to (a) Customer's violation of applicable law, (b) Customer Data, (c) Customer's breach of Section 4 (Acceptable Use), (d) Customer's breach of Section 5.3 (Restrictions), or (e) any Customer-offered product or service (except if such claim is attributable to the Service as offered by Palantir) and indemnify and hold harmless Palantir from and against related costs, attorneys' fees, and damages, if any, issued by a competent authority or finally awarded pursuant to a non-appealable order.

9.3 Indemnification Procedure. The obligations of the indemnifying Party shall be conditioned upon the indemnified Party providing the indemnifying Party with: (a) prompt written notice (in no event to exceed twenty (20) days) of any claim, suit, or demand of which it becomes aware; (b) the right to assume the exclusive defense and control of any matter that is subject to indemnification (*provided* that the indemnifying Party will not settle any claim unless it unconditionally releases the indemnified Party of all liability and does not admit fault or wrongdoing by the indemnified Party); and (c) cooperation with any reasonable requests assisting the indemnifying Party's defense and settlement (at the indemnifying Party's expense). This Section sets forth each Party's sole liability and obligation and the sole and exclusive remedy with respect to any claim of Intellectual Property Rights infringement.

10. Palantir Warranty and Disclaimer.

10.1 Palantir Warranty. Palantir warrants that during the Term (a) the Service will be provided substantially in accordance with the applicable Documentation and (b) the Professional Services will be provided in a professional and workmanlike manner. In the event of a breach of an above warranty, Customer may give Palantir written notice of termination of this Agreement, which termination will be effective thirty (30) days after Palantir's receipt of the notice, unless Palantir is able to remedy the breach prior to the effective date of termination. This warranty shall not apply to the extent such breach is caused by Customer Data or misuse or unauthorized modification of the Service (including but not limited to Customer's violation of Section 4 (Acceptable Use)) or any Customer selected hardware used in connection with the Service.

10.2 Disclaimer. NO AMOUNTS PAID HEREUNDER ARE REFUNDABLE OR OFFSETTABLE EXCEPT AS OTHERWISE EXPLICITLY SET FORTH HEREIN. EXCEPT AS EXPRESSLY SET FORTH HEREIN, THE PALANTIR TECHNOLOGY AND PROFESSIONAL SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY OTHER WARRANTIES OF ANY KIND AND PALANTIR AND ITS SUPPLIERS AND SERVICE PROVIDERS HEREBY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, RELATING TO THE PALANTIR TECHNOLOGY AND PROFESSIONAL SERVICES PROVIDED HEREUNDER OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING LIMITATION, PALANTIR DOES NOT WARRANT THAT THE PALANTIR TECHNOLOGY AND PROFESSIONAL SERVICES WILL MEET CUSTOMER REQUIREMENTS OR GUARANTEE ANY RESULTS, OUTCOMES, OR CONCLUSIONS OR THAT OPERATION OF THE SERVICE WILL BE UNINTERRUPTED OR ERROR FREE. PALANTIR IS NOT RESPONSIBLE OR LIABLE FOR ANY THIRD PARTY SERVICES (INCLUDING WITHOUT LIMITATION, UPTIME GUARANTEES, OUTAGES, OR FAILURES), CUSTOMER DATA, OR ANY THIRD PARTY CONTENT. PALANTIR DOES NOT CONTROL THE TRANSFER OF INFORMATION OR CUSTOMER DATA OVER COMMUNICATIONS FACILITIES, THE INTERNET, OR THIRD PARTY SERVICES, AND THE SERVICE MAY BE SUBJECT TO DELAYS AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. PALANTIR IS NOT RESPONSIBLE FOR ANY DELAYS, FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. PALANTIR SHALL NOT BE RESPONSIBLE OR LIABLE FOR ANY ACTIONS TAKEN OR CONCLUSIONS DRAWN BY CUSTOMER BASED ON CUSTOMER'S USE OF THE SERVICE. NOTHING IN THIS CLAUSE LIMITS ANY RIGHTS OF THE CUSTOMER OR NHS ENGLAND UNDER THE FDP AGREEMENT.

11. Customer Warranty. Customer warrants that (a) Customer has provided all necessary notifications and obtained all necessary consents, authorizations, approvals, and/or agreements as required by any applicable laws or policies, and has informed Palantir of any obligations applicable to Palantir's processing of Customer Data, in order to enable Palantir to process Customer Data, including personal data, according to the scope, purpose, and instructions specified by Customer and that Customer will not direct the processing of Customer Data by Palantir in violation any laws or regulations (including localization requirements) or rights of third parties; (b) it will not use the Service for any unauthorized or illegal purposes; and (c) it will not upload or import Customer Data to the Service requiring additional documentation without first executing such documentation.

12. Limitations of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES FOR ANY (A) COST OF PROCUREMENT OF ANY SUBSTITUTE PRODUCTS OR SERVICES, OR COST OF REPLACEMENT OR RESTORATION OF ANY CUSTOMER DATA, (B) ECONOMIC LOSSES, EXPECTED OR LOST PROFITS, REVENUE, OR ANTICIPATED SAVINGS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF OR DAMAGE TO GOODWILL OR REPUTATION, AND/OR (C) INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL LOSS OR DAMAGE, WHETHER ARISING OUT OF PERFORMANCE OR BREACH OF THIS AGREEMENT OR THE USE OR INABILITY TO USE THE PALANTIR TECHNOLOGY, EVEN IF THE PARTY HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH LOSS OR DAMAGES. EXCEPT FOR THE PARTIES' OBLIGATIONS SET FORTH IN SECTIONS 5 AND 9.2 OF THIS AGREEMENT AND CUSTOMER'S PAYMENT OBLIGATIONS HEREUNDER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY AGREES THAT THE MAXIMUM AGGREGATE LIABILITY OF EITHER PARTY AND ITS AFFILIATES TO THE OTHER PARTY AND ITS AFFILIATES FOR ALL CLAIMS OF ANY KIND SHALL NOT EXCEED FIFTY THOUSAND POUNDS STERLING (GBP 50,000), AND THAT SUCH REMEDY IS FAIR AND ADEQUATE. THE LIMITATIONS SET FORTH IN THIS SECTION 12 SHALL APPLY REGARDLESS OF WHETHER AN ACTION IS BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY AND DO NOT AFFECT OR LIMIT ANY LIABILITY OF PALANTIR, CUSTOMER OR NHS ENGLAND UNDER THE FDP AGREEMENT.

13. Dispute Resolution. Any dispute, controversy, or claim arising from or relating to this Agreement shall first be raised by the Parties in accordance with the provisions of the MOU. The Parties reserve the right that should the dispute be incapable of resolution in accordance with the MOU or if such dispute cannot be resolved following good faith discussions within sixty (60) days after notice of a dispute, it shall be finally settled by arbitration. The governing law shall be the substantive laws of England and Wales, without regard to conflicts of law provisions thereof, and without regard to the United Nations Convention on Contracts for the International Sale of Goods, and arbitration shall be administered in London, United Kingdom under the Rules of Arbitration of the International Chamber of Commerce ("**ICC Rules**"). Notwithstanding the foregoing, each Party shall have the right to institute an action at any time in a court of proper jurisdiction for preliminary injunctive relief pending a final decision by the arbitrator(s), *provided* that (a) the Party instituting the action shall seek an order to file the action under seal (or at a minimum do so for any filings containing Confidential Information or trade secrets) in order to limit disclosure as provided in Section 6 of this Agreement; and (b) a permanent injunction and damages shall only be awarded by the arbitrator(s).

14. Miscellaneous. Palantir shall provide the Service and Professional Services consistent with laws and regulations applicable to Palantir's provision of such Service and Professional Services generally, including but not limited to, regarding data protection and international transfers of personal data, without regard to Customer's specific utilization of the Service except to the extent set forth in the MOU, and subject to Customer's compliance with this Agreement. The Parties shall comply with the Palantir AIP Addendum available at https://palantir.pactsafe.io/aip-legal-3791.html, which is hereby incorporated by reference. Except with Palantir's prior written consent, neither this Agreement nor the access or licenses granted hereunder may be assigned, transferred, or sublicensed by Customer, including, without limitation, pursuant to a direct or indirect change of control of Customer, a merger involving Customer where Customer is not the surviving entity, or a sale of all or substantially all of the assets of Customer (collectively, a "Change of Control"); any attempt to do so shall be void. Customer must provide written notice to Palantir prior to a Change of Control, and Palantir may terminate this Agreement in the event of a Change of Control. Palantir may use subcontractors to deliver Professional Services under this Agreement, provided that Palantir shall remain fully responsible for such subcontractors. Any notice required or permitted hereunder shall be in writing to the Customer at the address set forth in the applicable MOU; notifications to Palantir shall be sent to legalnotices@palantir.com. If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and be enforceable. Any and all modifications, waivers, or amendments must be made by mutual agreement and shall be effective only if made in writing and signed by each Party. No waiver of any breach shall be deemed a waiver of any subsequent breach. Except for the obligation to pay money, neither Party will be liable for any failure or delay under this Agreement due to any cause beyond its reasonable control, including without limitation acts of war, acts of God, earthquake, flood, embargo, riot, sabotage, labor shortage or dispute, governmental act, or failure of the Internet, telecommunications, or hosting service provider, computer attacks, or malicious acts;

provided that the delayed Party: (a) gives the other Party prompt notice of such cause; and (b) uses commercially reasonable efforts promptly to correct such failure or delay in performance. There are no third party beneficiaries under this Agreement, whether express or implied. For the avoidance of doubt, nothing in this Agreement shall be construed to create a joint venture, employment, partnership, strategic alliance, formal alliance, or strategic partnership relationship between the Parties. This Agreement is the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement.. Palantir is in no way affiliated with, or endorsed or sponsored by, The Saul Zaentz Company d.b.a. Tolkien Enterprises or the Estate of J.R.R. Tolkien.

SCHEDULE 2

NHS-PET USE TERMS

1. **INTRODUCTION:** This NHS-PET Software-as-a-Service Addendum ("SaaS Addendum") supplements the agreement between NHS ENGLAND (**Authority**) and IQVIA LTD (**Supplier**) of 28 November 2023 (**Contract**) for the provision by Supplier of its NHS-PET solution as defined in the Contract (as **Services** as there defined, such solution the **SaaS**) with additional terms and conditions that apply to the use of the Services by the Authority and the Authority Users (the Authority and the Authority Users referred to as **User Organisations** in this SaaS Addendum). This SaaS Addendum binds the Authority Users by virtue of a memorandum of understanding (**MoU**) entered into between the Authority and the Authority User.

2. **ACCESS AND USE:**

   a. During the term specified under the MoU (**Term**), the User Organisation may access and use the SaaS solely in accordance with the terms of the Contract. The User Organisation agrees not to access or use the SaaS outside the scope of the rights that are expressly granted by the Supplier in the Contract.

   b. The Supplier will provide to the User Organisation the necessary network links or other access protocols to enable the users who have completed any applicable registration process or who otherwise receive a valid user ID or other access credentials (**Authorised Users**) to access the SaaS during the Term. A User Organisation shall undertake reasonable efforts to make all respective Authorised Users aware of the terms and conditions of this SaaS Addendum that are applicable to their use of the SaaS and shall cause their respective Authorised Users to comply with such terms and conditions.

   c. The Authorised User Obligations: A User Organisation is responsible for its respective Authorised Users' compliance with the provisions of this SaaS Addendum, including for the avoidance of doubt ensuring that Authorised Users do not attempt to access or manipulate in any way the source code of any software used by or on behalf of the Supplier to provide the Services. The Supplier is not responsible for any harm caused by Authorised Users, including individuals who were not authorised to have access to the SaaS but who were able to gain access because usernames, passwords or accounts were not terminated on a timely basis in a User Organisation's local identity management infrastructure or User Organisation local computers. A User Organisation agrees, if and to the extent applicable with respect to the SaaS: (i) to provide the technology and facilities, including access to the internet and an up-to-date and fully supported browser, as required to use them; (ii) to complete the implementation and set-up process as required by the Supplier to access them; (iii) that it is responsible for maintaining the confidentiality of passwords and account information required for access to them; (iv) to notify the Supplier as soon as reasonably practicable of any unauthorised use of the User Organisation's account, breach of security, or loss or theft of user names or passwords; (v) that use of the SaaS is limited to use by Authorised Users and that such use does not include the right to resell or sublicense such SaaS; (vi) to abide by all applicable local, state, national and international law and regulations, and not to use the SaaS for any purpose that is unlawful, not contemplated or prohibited under this SaaS Addendum and/or the Contract; (vii) to use commercially reasonable efforts to prevent unauthorised access to, or use of the SaaS; and (viii) to submit data to the Services (**User Content**) only in accordance with the Contract and applicable laws and government regulations. A User Organisation will not frame or mirror any part of the SaaS, other than copying or framing on the User Organisation's own intranets or otherwise for its own internal business purposes, nor access the SaaS in order to build a competitive product or service, or reverse engineer the SaaS. The User Organisation further agrees not to use or permit use of the SaaS, including by uploading, emailing, posting, publishing or otherwise transmitting any material, for any purpose that may (a) menace or harass any person or cause damage or injury to any person or property, (b) involve the publication of any material that is false, defamatory, harassing or obscene, (c) violate privacy rights, (d) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (e) constitute an infringement of intellectual property or other proprietary rights, or (f) otherwise violate applicable laws, ordinances or regulations.

3. **SECURITY VULNERABILITIES:** The User Organisation shall use all reasonable endeavours to ensure that security vulnerabilities, and the consequences of such vulnerabilities, do not arise as a result of transmission of User Content from the User Organisation's systems to the SaaS, and any interoperating computer applications, including any viruses, Trojan horses, worms or other programming routines contained in User Content or interoperating applications that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data. Nothing in this clause 3 shall limit or override the Supplier's obligations as set out elsewhere in the Contract.

4. **THIRD PARTY SOFTWARE:** Where Supplier provides access to third party software in relation to use of the SaaS, and in accordance with the requirements of the Contract, the User Organisation acknowledges that use of such software may be subject to separate license agreements directly between the User Organisation and the third party licensor. The User Organisation is responsible for complying with the terms of such license agreements in relation to the use of the Services. For third party software embedded in the SaaS, the Supplier grants to the User Organisation a sublicense of such third party software on the terms available through the SaaS which shall enable the User Organisation to use the SaaS in accordance with the Contract. The User Organisation agrees that such embedded third party software shall only be utilized in conjunction with the SaaS.

SCHEDULE 3

FORM OF DATA PROCESSING AGREEMENT

Controller	
Processor	
(together the **Parties** and each a Party)	
Date	
Relating to	The NHS Federated Data Platform

A. This is an agreement (**Agreement**) between the Parties (as defined above) relating to the processing of personal data, made further to the terms of an agreement for the provision of certain software services between NHS England and the Processor in relation to the NHS Federated Data Platform dated *[22][Data Platform][28][NHS_PET]* November 2023 (as may be amended from time to time in accordance with its terms) (the **Services Agreement**). Under the terms of the Services Agreement, the Controller is beneficiary of certain software and data processing services which this Agreement governs in relation to Personal Data.

B. This Agreement is entered into on the date first appearing above.

C. Capitalised terms used in this Agreement have the meanings given to them in the Data Protection Legislation or the definitions schedule.

1) The Parties acknowledge that for the purposes of the Data Protection Legislation, the Processor is a processor and the Controller is the controller (or processor in relation to another controller, if so designated above).

2) The only processing that the Processor is authorised to carry on, whether the Controller acts as a controller or processor, is listed in the Data Processing Schedule, relevant Annexes and paragraph 14, and may not be determined by the Processor. The Parties may agree Annexes describing Processing covered by the terms of this Agreement in relation to specific dataflows or data processing activities from time to time.

3) The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe Data Protection Legislation.

4) The Processor shall provide all reasonable assistance to the Controller in the preparation of any DPIA prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

   a) a systematic description of the envisaged Processing and the purpose of the Processing;

   b) provision of information to assist the Controller with an assessment of the necessity and proportionality of the Processing in relation to the provision of services under the Services Agreement;

   c) provision of information to assist the Controller with an assessment of the risks to the rights and freedoms of Data Subjects; and

   d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5) The Processor shall, in relation to any Personal Data Processed in connection with its obligations under this Agreement:

a) Process that Personal Data only in accordance with the Data Processing Schedule, relevant Annex and paragraph 14, unless the Processor is required to do otherwise by applicable law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by applicable law;

b) ensure that it maintains physical and IT security that follows Good Industry Practice appropriate to prevent a Data Loss Event and has in place appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of such measures) having taken account of the:

    i) nature of the data to be protected;

    ii) harm that might result from a Data Loss Event;

    iii) state of technological development; and

    iv) cost of implementing any measures;

c) ensure that:

    i) the Processor Personnel do not Process Personal Data except in accordance with this Agreement (and in particular the Data Processing Schedule and each Annex);

    ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

        (1) are aware of and comply with the Processor's duties under this Agreement and the obligations to process Personal Data in accordance with the terms of the Services Agreement including in relation to data protection, confidentiality and matters relating to the Freedom of Information Act 2000);

        (2) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

        (3) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

        (4) have undergone adequate training in the use, care, protection and handling of Personal Data;

d) subject to paragraph 14, not transfer Personal Data outside of the UK or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

    i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer under Data Protection Legislation as determined by the Controller;

    ii) the Data Subject has enforceable rights and effective legal remedies;

    iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations);

    iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; or

v) the Processor on the Controller's request promptly enters into an agreement with the Controller including or on such standard terms as the Information Commissioner or the Controller may require;

e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by law to retain the Personal Data.

6) Subject to paragraph 7) of this Agreement, the Processor shall notify the Controller as soon as practically possible (and in any event within 24 hours) if in relation to it Processing Personal Data under or in connection with this Agreement it:

a) receives a Data Subject Request;

b) receives a request to rectify, block or erase any Personal Data;

c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Agreement;

e) receives a request from any third Party for disclosure of Personal Data, processed pursuant to this Agreement, where compliance with such request is required or purported to be required by Law; or

f) becomes aware of a Data Loss Event.

7)

a) The Processor's obligation to notify under paragraph 6) of this Agreement shall include the provision of further information to the Controller in phases, as details become available.

b) The Controller shall notify the Processor as soon as practically possible (and in any event within 24 hours) if it becomes aware of a Data Loss Event affecting Personal Data Processed under this Agreement.

8) Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6) of this Agreement (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

a) the Controller with full details and copies of the complaint, communication or request;

b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

d) assistance as requested by the Controller following any Data Loss Event; and/or

e) assistance as requested by the Controller with respect to any request from the Information Commissioner, or any consultation by the Controller with the Information Commissioner.

9) The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement.

10) The Processor shall allow for audits of its Processing activity by the Controller or the Controller's designated auditor as set out in the Services Agreement.

11) The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12) Before allowing any Subprocessor to Process any Personal Data related to the Agreement, the

Processor must:

a) notify the Controller in writing of the intended Subprocessor and Processing;

b) obtain the written consent of the Controller;

c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Agreement such that they apply to the Subprocessor; and

d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13) The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

14) The Processor will not process or transfer any Personal Data outside the UK except in accordance with the FDP Information Governance Framework.

15) For the purposes of paragraph 5)d) and without prejudice to the other terms of this Agreement the Processor undertakes to:

a) provide appropriate safeguards in relation to transfers of personal data between its group entities for the purpose of performing the Services Agreement; and

b) ensure that transfers of personal data between the Processor and the Subprocessor, are subject to contractual terms between the Processor and the Subprocessor providing appropriate safeguards and containing clauses equivalent to the clauses in this Agreement.

16) The Parties agree to take account of any guidance issued by the Information Commissioner.

17) The Processor is not liable for loss or damage suffered by the Controller resulting from the Processor's breach of any obligation under this Agreement to the extent that such loss or damage results from an act, omission or instruction of the Controller.

18) For the purposes of paragraph 12), the Controller consents to the use by Processor of the following Subprocessors:

[list]

SIGNED BY the parties acting by their authorised representatives to show their agreement to the terms of this Agreement

SIGNED by

....

for and on behalf of **[*Controller*]** (Signature)

....

(Date)

SIGNED by

....

for and on behalf of **[*Processor*]** (Signature)

....

(Date)

DEFINITIONS SCHEDULE

Annex an annex to this Agreement in the form of Part 2 of the Data Processing Schedule;

Data Loss Event any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;

Data Processing Schedule the data processing schedule to this Agreement;

Data Protection Legislation the Data Protection Act 2018, UK GDPR, and all applicable data protection and privacy legislation, legally binding guidance and codes of practice issued by the Information Commissioner in force from time to time;

Data Subject Request a request made by or on behalf of a Data Subject in accordance with rights granted under the Data Protection Legislation to access their Personal Data;

DPIA an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;

FDP Information Governance Framework the information governance framework set out in the FDP Information Governance Framework Document V1.0 (as the same may be updated from time to time);

Good Industry Practice standards, practices, methods and process conforming to the applicable law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking under the same or similar circumstances;

Processor Personnel includes all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under this Agreement;

Subprocessor any third party appointed to process Personal Data on behalf of the Processor in relation to this Agreement;

UK GDPR UK GDPR as defined in and read in accordance with the Data Protection Act 2018; and

Use Terms the authorised use terms applying to the use under the Services Agreement by the Controller's personnel of the Processor's services.

FORM OF DATA PROCESSING SCHEDULE

PROCESSING PERSONAL DATA

PART 1 – GENERAL AND CONTRACT DETAILS

Capitalised terms used in this Schedule have the meaning given to them in the Agreement.

1) The contact details of the Controller:

   a) Data Protection Officer are: [*Insert Contact details*]

   b) Caldicott Guardian are: [*Insert Contact details*]

   c) Chief Information Security Officer are: *[Insert Contact details]*

   d) Senior Information Risk Officer are: *[Insert Contact details]*

2) The contact details of the Processor:

   a) Data Protection Officer are:

   b) Caldicott Guardian are: [*Insert Contact details*]

   c) Chief Information Security Officer are: [*Insert Contact details*]

   d) Senior Information Risk Officer are: [*Insert Contact details*]

3) The Processor shall comply with any further written instructions with respect to Processing by the Controller.

4) Any such further instructions shall be incorporated into Part 2 of this Annex or another Part 2 Annex issued by the Controller describing the relevant Processing in the form of Part 2 of this Annex.

Description	**Details**[1]
Controller for each Category of Personal Data	Is the Controller referred to in the Agreement for all Personal Data categories
Duration of the Processing	Duration of the Services Agreement or, if shorter, the Controller's use of Processor's software or an approved Product.
Nature and purposes of the Processing	Use of the Data Platform [and NHS-PET Solution] to deliver and fulfil Controller's health care provision, health system administration and other management, data analytics and reporting functions through Products approved by the FDP Data Governance Group, which will be subject to separate processing instructions for each Product in the form of Part 2 to this Annex.

[1] Update as appropriate.

Description	**Details**[1]
	Administration of user (staff) data in order to administer use of the Data Platform [and NHS-PET Solution] and for the purposes above. Training in the use of the NHS-PET Solution and Data Platform, and configuration of data analytics functionality in the Data Platform (for which purposes Subprocessor's services may be utilised). Processor complies with obligations in Services Agreement and in the configuration of its software approved by Controller in relation to access to all Personal Data. Processor's instructions are to provide [the Data Platform/NHS-PET Solutions] under the Services Agreement for the above purposes, which will be subject to separate processing instructions for each Product in the form of Part 2 to this Annex]
Type of Personal Data	Personal data and special category data as identified in a separate processing instructions for each Product in the form of Part 2 to this Annex
Categories of Data Subject	Staff, patients, service users and other categories as identified in a separate processing instructions for each Product in the form of Part 2 to this Annex
Plan for return and destruction of the data once the Processing is complete **UNLESS requirement under Union or Member State law to preserve that type of data**	Processor's [*Data Platform/NHS-PET Solution*] is configured only to retain data for defined periods that can be configured by Controller. Processor will delete or provide access for Controller to remove data from the Processor's services at the end of duration of processing.
Transfers of data outside the UK	All personal data is stored in the UK and is not to be accessible or processed from outside the UK.

PART 2 – FORM OF ANNEX: SPECIFIC PROCESSING INSTRUCTIONS

This is an Annex to the Data Processing Agreement between the Controller and the Processor dated *[ ]*. Capitalised terms used in this Schedule have the meaning given to them in the Agreement.

Description	**Details**[2]
Controller for each Category of Personal	Is the Controller referred to in the Agreement for all Personal Data categories

[2] Update as appropriate.

Description	Details[2]
Data	
Processor	
Subprocessors	
Commencement of Processing	
Product Name	
Duration of the Processing	Duration of the Services Agreement or, if shorter, the Controller's use of the Product.
Nature and purposes of the Processing	[ ] [*To be completed in accordance with the Templates issued under the FDP IG Framework Document for each Product]*
Type of Personal Data	{I}
Categories of Data Subject	{I} .
Plan for return and destruction of the data once the Processing is complete **UNLESS requirement under Union or Member State law to preserve that type of data**	Processor's [Data Platform] [NHSE-PET Solution] is configured only to retain data for defined periods that can be configured by Controller. Processor will delete or provide access for Controller to remove data from the Processor's services at the end of duration of processing.
Transfers of data outside the UK	All personal data is stored in the UK and is not to be accessible or processed from outside the UK.
Issued on behalf of the Controller by	[*Insert Name, Job title, Organisation Name, Email address*]
Date of Issue	[ ]

SCHEDULE 4

FORM OF ADDENDUM

Addendum to Memorandum of Understanding relating to the NHS Federated Data Platform	
Date of MoU	
Parties	NHS England [NHS Body]
Product	*Describe Product*
Additional authorised user terms	*Add additional user terms, if any*
Funding Plan	*Describe or refer to any funding arrangements and the matters described in clause 5.2*
Relevant Trust System Contracts	
Additional governance arrangements	
Additional data processing annex	*Add, in the form set out in Part 2 of the Data Processing Schedule in Schedule 4*
Other matters	

SCHEDULE 2.7

DIGITAL & DATA ACADEMY

1. INTRODUCTION

1.1 The Parties agree to collaborate in order to achieve the following objectives:

(a) The co-ordination of their training and recruitment efforts having regard to the workforce profile desirable for NHS Bodies using the Data Platform, including co-ordination with other relevant suppliers of services to the Authority ("**Digital Suppliers**");

(b) The creation of an apprenticeship scheme, or the alignment of the existing apprenticeship programmes of the Parties, aligned with Data Platform usage; and

(c) The creation of a "**Digital & Data Academy**" being a centre of excellence promoted by the Authority, the Supplier and Digital Suppliers, and co-ordinating the matters described in this Schedule.

1.2 The Authority intends to agree terms similar to those in this Schedule with Digital Suppliers.

2. GOVERNANCE

2.1 The Parties will establish a joint committee (the "**Academy Working Group**") for the purposes of managing delivery of the objectives described in this Schedule.

2.2 The Parties will discuss and agree the terms of reference, meeting cadence and attendance of the Academy Working Group (which may include representatives of Digital Suppliers) by analogy with the arrangements for Boards in Schedule 8.1 (*Governance*).

3. APPRENTICESHIP SCHEMES

3.1 The Parties intend to co-ordinate their respective apprenticeship programmes in order to:

(a) Align and jointly plan apprentice recruitment;

(b) Co-ordinate and collaborate on apprentice programmes, including secondment and other learning arrangements;

(c) Collaborate on the procurement and management of training and education providers supporting apprenticeship programmes;

(d) Collaborate on setting up an infrastructure for training and development of apprentices;

(e) Establish ways of working and joint arrangements allowing for the HR management of apprentices on their apprenticeship programmes;

(f) Promote school and college engagement outside of the apprenticeship programmes; and

(g) Seek to procure for the wider benefit of communities served by NHS services, and embed social value objectives.

3.2 The Parties further agree to:

(a) Collaborate on establishing requirements for the apprenticeship framework, based on occupational and professional standards, where necessary;

(b) Clearly define the roles and responsibilities of employers and apprentices;

(c) Develop training plans describing the required learning content and methods of learning and assessment;

(d) Identify or create appropriate academic, vocational or skills-related qualifications associated with relevant apprenticeship programmes;

(e) Invite the Supplier's subcontractors, as agreed with the Authority, to participate in achieving the objectives set out in this Schedule;

(f) Engage in conversations around funding arrangements of the apprenticeship programmes including co-ordination of the deployment of funds derived from each party's apprenticeship levy; and

(g) Engage in discussions and collaborate with Digital Suppliers in pursuit of the purpose of the objectives set out above.

SCHEDULE 2.9

SOCIAL VALUE COMMITMENTS

Social Value Commitments

1. DEFINITIONS

In this Schedule, **Workforce** refers to the Supplier employees and contractors (as applicable) dedicating at least 50% of their working hours to the delivery and operation of the Programme and Associated Services

2. GENERAL

2.1 This Schedule 2.9 sets out the Supplier's commitments to the social value requirements of the Programme, and details the projects, measures and enterprises that the Supplier will participate in, establish or contribute to, as part of meeting the Authority's objectives in this area.

3. FIGHTING CLIMATE CHANGE COMMITMENTS

3.1 Green Cloud Computing

3.1.1 The Supplier will commit to working with its hyperscaler supply chain in order to reduce the carbon emissions generated as a result of and relating to the cloud hosting computing during Service delivery. The Supplier is targeting that all the underlying Data Platform cloud hosting will be powered by renewable energy from 2025 and it will work with its hyperscalers to implement methods to achieve these targets.

3.2 Establishing Northern UK Hub and regional travel

3.2.1 As part of the Supplier's commitments to reduce travel emissions:

(a) The Supplier will establish a Northern England office hub by 2025.

(b) In delivery of the Optional Services, Sub-contractors Accenture and PwC will leverage their regional offices to reduce the travel required by their Workforce to NHS Bodies during delivery. Sub-contractors PwC and Accenture shall also promote the use of more varied sustainable travel-options like cycling.

3.3 Green Travel Plan

3.3.1 The Supplier commits to engage with Zellar within first 2 (two) months of the Effective Date, to develop during the mobilisation phase a green plan to help the Supplier's Workforce take sustainable travel options during delivery of the Services. The plan will be updated annually to ensure effectiveness.

3.4 Reducing technology waste

3.4.1 The Supplier commits to implement a system within the first Contract Year under which it will work with an accredited technology recycling organisation to recycle those computers and mobile phones used as part of Service delivery, as appropriate, and subject to ownership rights.

3.5 Jump Sustainability behavioural change platform

3.5.1 The Supplier commits that within first 5 months of the Effective Date it will develop a behavioural change platform with the organisation, Jump, and will start to enrol its Workforce on the platform. The Supplier will use the platform to provide sustainability training to the Workforce and to encourage them to make sustainable choices.

3.6 Reducing Food Waste & Associated Emissions

3.6.1 As part of the Supplier's commitments, The Supplier will, for the Term, work with its catering team to reduce food waste and identify what surplus food can be sent to OLIO for distribution to the community each week. OLIO will collect this food from the Supplier's London office.

3.7 Offset emissions

3.7.1 The Supplier commits to work with accredited offset NGOs and organisations to purchase and deliver high quality business travel emissions offsets each year. The Supplier will endeavour to offset all emissions resulting from the delivery of the Services by the expiry of the Initial Term and/or any Extension Periods.

3.8 Nature and Wellbeing

3.8.1 The Supplier will endeavour to engage relevant partners including ‘Trees for Cities’, ‘Greener NHS and NHS Forest’, for the purpose of building one wellbeing garden each year of the Term on or near an NHS Trust across the UK. The size and placement of these gardens will be agreed with the relevant Trust at the time. Subject to enlisting relevant partners and willing NHS Trusts, the Supplier aims to build the first wellbeing garden by the end of the first Contract Year.

The following 1.9 to 1.11 are proposed ways of working with the Supplier Sub-contractors, NHSE and NHS Bodies:

3.9 Working with NHSE

3.9.1 As part of the Supplier’s commitments, the Supplier will work with the Authority to scope how Foundry Sustainability can enable a Service sustainability innovation use case. The Supplier will incubate this use case at a NHS Trust and ICS to help ensure it is impactful upon wider rollout.

3.9.2 Investment will be made available for an incubation period of 6-8 weeks for Foundry Sustainability at one Trust and one ICS to configure it to suit the NHS’s specific sustainability needs. The Authority can then decide whether to adopt the customised version of Foundry Sustainability as an application within the Service offering for the Authority and NHS Bodies to add to their Service tenants if they wish.

3.9.3 The Supplier will provide the Authority leadership with ten sustainability training sessions on how technology can be used to reduce carbon footprints across the NHS.

3.10 Food waste

3.10.1 The Supplier will engage the third party, Wrap, in order to configure an application within Foundry Sustainability for the purpose of food waste tracking and reduction. The application can be incubated and tested at the same NHS Trusts and ICSs where the wider Foundry Sustainability application will be tested.

3.11 Decarbonising Supply Chains & Reducing Clinical Waste (Aligning with NHS Clinical Waste Strategy)

3.11.1 The Supplier will configure a supply chain emissions application within Foundry Sustainability. The application has already been proactively trialled with Unipart at East Lancashire Trust and during the first Contract Year, can form part of a further incubation period of 6-8 weeks at an ICS or a second Trust.

Further commitments:

3.12 Sustainability Charter

3.12.1 As part of the Supplier's commitments, the Supplier, PwC and Accenture will sign a sustainability charter to contractually agree to fulfilling the commitments set out herein annually.

3.13 Green Cloud Computing Training

3.13.1 As part of the Supplier's commitments, AWS and the Supplier will provide a virtual, 'Green FDP Training' course to all Service users and NHS Digital and Data Academy apprentices. Learners can complete the course at their own pace to gain a 'Green Cloud Skilled' badge. This training will be delivered as part of our standard Service onboarding training in the period of the first 2 (two) Contract Years, alongside being virtually available to Academy learners. Training will be designed by AWS's green software experts and the Supplier's learning and development team.

Monitoring and governance:

3.14 Establish robust commitment governance and accountability model to identify and empower owners for each commitment

3.14.1 The Supplier will put in place a governance structure to ensure the commitments set out in this Schedule are adhered to and followed. The structure will include: (i) Social Value Lead runs quarterly meetings with sustainability leads from each of the Supplier's organisation to drive progress; and (ii) Social Value Lead reports on decarbonisation progress to the Authority and is accountable for delivering all fighting climate change commitments.

3.15 Feedback, transparency and improvement, applied against the timed action plan

3.15.1 The Supplier's Social Value Lead will meet each quarter with sustainability leads from each organisation within the Supplier to review effectiveness of approach and decarbonisation pathways, discussing how to continuously improve the Supplier's approach to reducing emissions.

3.15.2 The Supplier will update its decarbonisation roadmap each year and have it verified by sustainable business experts [Redacted under FOIA s43, Commercial interests].

3.15.3 The Supplier will review its green travel plan each year for effectiveness.

3.15.4 The Supplier will ensure there is an open transparent dialogue with the Authority, providing accurate quarterly progress reports and emission reduction information. The Supplier will arrange progress meetings each quarter (or as frequently as the Authority wishes) with the Authority to discuss actions taken. The Supplier's Social Value Lead will be a consistent point of contact for the Authority to communicate with.

3.15.5 The Supplier's Social Value Lead will provide progress reports to the Authority (including our emissions reporting) which will be verified for their impact twice a year by Social Value Business (experts on designing and delivering social activities that have true impact across the UK).

4. EQUAL OPPORTUNITY COMMITMENTS

4.1 Digital and Data Academy Commitments

4.1.1 If there is any conflict, inconsistency or ambiguity between this section 2 of Schedule 2.9 and Schedule 2.7 (Digital Data Academy) then Schedule 2.7 (Digital Data Academy) shall take precedent.

4.2 Recruitment Plan

4.2.1 The Supplier commits to providing a team with recruitment expertise to help the Authority generate an Academy recruitment plan, model development & network building with our recruitment and charity partners. This will include the Supplier facilitating 6 workshops with the Authority to aid the plan development.

4.3 Academy Promotion Initiatives

4.3.1 The Supplier commits to allocating a reasonable amount of funding and to provide resources to deliver annual Academy Promotion Initiatives at UK schools and colleges in collaboration with the Authority.

4.4 Governance and Planning

4.4.1 The Supplier will provide ongoing senior representatives for the Academy Working Group during the Term. The Supplier will support the Authority to design an Academy governance model – including facilitating 2 workshops within the first 6 months of delivery between the Authority and the Supplier's recruitment partners to aid model development.

4.5 Technology-enabled-learning*

4.5.1 As part of the Supplier's commitments, the Supplier will provide Academy apprentices with access to a Foundry learning environment during their apprenticeship to power their learning. Working practices and principles, including sharing of code, will be aligned to the Authority's data academy principles (as set out or referred to in Schedule 2.7 (Digital Data Academy)), including how Jupiter and Pyspark can be used within Foundry.

4.6 Apprenticeships Training Plans

4.6.1 The Supplier commits to making available a dedicated resource and data expertise for the purpose of training plan development; providing shorter data-skills and accreditation programmes for the Academy; and to develop new innovation focused modules for Academy apprenticeships.

4.7 Varied learning

4.7.1 The Supplier will support the Authority to arrange apprenticeship secondments across the NHS and industry.

4.8 Inclusive culture

4.8.1 The Supplier will make available: (i) resources to collaborate with learning providers on inclusive by-design training development; (ii) funding and planning /delivery resource for annual ‘Hackathon for Good’ to support communities; and (iii) funding and planning / delivery resource for Academy Community Programme initiatives.

4.9 Management Technology

4.9.1 The Supplier will provide the Authority with up to 20 hours of engineering time configure the Services to the Authority’s needs for the purpose of supporting the Academy’s management. The Supplier has provided Credits for Academy management purposes.

Wider Equal Opportunity Commitments:

4.10 Driving Employment Equality

4.10.1 The Supplier commits to establishing, during the first 2 (two) months from the Effective Date, a joint working group with senior representation from each of the Supplier's organisations. The group will work together as a collective to develop a timed action plan which will drive progress on positive action schemes and senior / mid-level representation diversity targets. The Supplier will endeavour to use the expertise from Diversity, Equity and Inclusion partners where needed. The Supplier reviews plan with the Authority during Mobilisation.

4.10.2 The timed-action-plan will be developed during the first 4 (four) months from the Effective Date, and the Supplier will monitor progress quarterly and review and update annually. The joint working group will meet quarterly throughout the Term.

4.11 Apprenticeships

4.11.1 As part of the Supplier’s commitments, the Supplier will work with an apprenticeship learning provider to run annual apprenticeship schemes - with particular preference for individuals from minority or disadvantaged groups the Supplier aims for **3-5%** of its Workforce to be enrolled onto Level 3+ apprenticeships from 2024 onwards.

4.12 Influencing NHSE

4.12.1 The Supplier commits to work with the Authority Service leadership to design 10 hours of inclusion-focused training, which the Supplier will then deliver to wider

NHSE leadership. Following the training the Supplier can work with the Authority to develop joint equal opportunity targets for the Service programme, which can be developed with the Authority during the Academy Working Group sessions listed in Schedule 2.7. It is anticipated that the training will be provided during first 6 months of the Effective Date.

4.13 Influencing NHS Bodies

4.13.1 In partnership with the Authority and Sub-contractor NECS, the Supplier will provide reasonable funding and co-deliver an annual uplift programme at a NHS Trust – reviewing equal opportunities issues affecting that Trust, providing leadership and digital skills training to approx. 25 BME staff. The training will be geared towards supporting the individuals gain a promotion or move to a new, higher paying role. As part of this the Supplier will also provide education to Trust leadership on how to support in-work progression for BME staff. It is anticipated that the final programme will be delivered in the final year of the Initial Term.

4.14 Inclusive and accessible Service skills development

4.14.1 The Supplier will provide flexible working pattern options, accessibility accommodations and varied learning options to its Workforce throughout the Contract. The Supplier will provide 6 hours of coaching sessions to new parents returning to work.

4.14.2 During the mobilisation phase of the contract, the Supplier will work with DEI charity partners and the minority group communities they work with to review the Supplier's Service adoption and training materials and approach to ensure these are as accessible and inclusive as possible e.g. inclusive language used in training examples. The Supplier will gather feedback quarterly from Service learners via anonymous surveys shared through Foundry's survey function to continuously improve the inclusivity and accessibility of the training during Service rollout. The review will be completed during the mobilisation phase and feedback will be collected quarterly through implementation phase.

4.14.3 As part of the Supplier's commitments, the Supplier will allocate dedicated resources during the transition phase to refactor products to improve their accessibility. The Supplier will create accessibility guidelines within the Service platform for all users, including apprentices, and Service marketplace developers to follow – e.g. developing with inclusive code and how to configure the Service to suit accessibility needs. Where relevant we will review these guidelines with an accessibility focused charity partner and the disabled communities they serve. Completion time: Product development and accessibility guidelines completed during first year of contract.

4.14.4 During our annual Service innovation hackathon the Supplier will work with Service users to develop data driven solution(s) that support inclusivity and accessibility.

4.15 Retention through Inclusion

4.15.1 The Supplier will provide its Workforce with annual inclusivity initiatives. The Supplier aims to have its team feature [Redacted under FOIA s43, Commercial interests]% Black and minority ethnic, female and disabled representation in year one of the contract and throughout the contract at a proportional level as the contract workforce gets smaller as delivery progresses.

4.16 Development Opportunities for All

4.16.1 The Supplier will work with learning partners to run skills development programmes for its Workforce annually. These will be a mixture of online, self-paced learning accreditation or skills programme courses, alongside in-person training courses. Completion time: skills development courses offered and run throughout the Term.

4.16.2 From the Effective Date the Supplier Programme leadership will develop clear progression pathways.

4.16.3 Managers will use these pathways to develop individual progression plans for their direct reports – reviewing progress against these plans bi-annually and encouraging their teams to meet their upskilling and progression goals. Managers to update the plan with their direct reports in Q1 of each year. Completion time: pathways developed during mobilisation phase and used by managers to develop progression plans for their direct reports on the programme on a rolling basis.

4.16.4 The Supplier will deliver an annual ‘Data for Good’ project with a chosen charity over a project period time that suits each project’s requirements. The Supplier will aim to support the charity by helping them develop data driven solutions.

4.16.5 In addition to the commitments above, the Supplier will also provide significant financial investment to help the Authority successfully deliver the Academy.

SCHEDULE 2.10

COLLABORATION

Collaboration

1. COLLABORATION WITH OTHER SUPPLIERS

The Supplier shall co-operate with any Other Supplier notified to the Supplier by the Authority from time to time by providing:

(a) reasonable information (including any Documentation);

(b) advice; and

(c) reasonable assistance,

in connection with the Services, to any such Other Supplier to enable such Other Supplier to create and maintain technical or organisational interfaces with the Data Platform.

2. COLLABORATIVE BEHAVIOURS

2.1 The Supplier and the Authority acknowledge the importance of working together in a partnership spirit towards the objectives of the Programme. Accordingly, the Supplier agrees in the performance of the Services to execute and demonstrate the following behaviours:

(i) proactively leading on, mitigating and contributing to the resolution of problems or issues, acting in accordance with the principle of "fix first, settle later";

(ii) being open, transparent and responsive in sharing relevant and accurate information with the Authority and Other Suppliers;

(iii) where reasonable, adopting common working practices, terminology, standards and technology and a collaborative approach to service development and resourcing with such Other Suppliers;

(iv) providing reasonable cooperation, support, information and assistance to Other Suppliers in a proactive, transparent and open way and in a spirit of trust and mutual confidence; and

(v) identifying, implementing and capitalising on opportunities to improve deliverables and deliver better solutions and performance throughout the relationship lifecycle,

(the **Collaborative Behaviours**).

2.2 The Authority acknowledges that the Supplier's scope and responsibility for Service performance is that set out in the Agreement.

2.3 The Supplier agrees that it shall raise promptly in writing with the Authority any material impact on the time or cost of performance of the Services caused by its following the provisions of this Schedule 2.10 (Collaboration) and the Authority and the Supplier shall agree appropriate Change through the Change Control Process.

2.4 The Supplier and the Authority agree to collaborate on the finalisation of the FDP Relationship and Collaboration Charter having regard to the Collaborative Behaviours.

2.5 The Supplier acknowledges that the Authority's intention is to create a commercial structure and approach (whether through letting of a framework agreement under the Public Contracts Regulations 2015 or otherwise) (**Product Framework**). The Authority acknowledges that the operation of the Product Framework may require consultation with and input from the Supplier including in relation to the implications for Data Platform operations of the Product Framework strategy, the basis on which suppliers to the Product Framework would use the Data Platform including applicable terms and conditions, the approval of applications and applicable fair use policies.

3. NHS LIVE SERVICE INTEGRATION

3.1 In order to facilitate Service provision, the Authority may ask Supplier to make certain arrangements for the connection of Services with other systems provided by NHS England (as successor to the functions of NHS Digital) ("**NHS Live Services**"). Connection and other arrangements and associated rights and obligations for integration of Services with NHS Live Services are set out in a connection agreement between the Authority (as successor to the functions of NHS Digital) and Supplier ("**Connection Agreement**") substantially in the form attached at Annex 1.

3.2 The Authority may by notice to the Supplier confirm that in respect of a NHS Live Service (the "**Designated NHS Live Service**") the terms set out in paragraph 3.3 have effect with effect from such date as the notice may set out.

3.3 The terms referred to in paragraph 3.2 are that in respect of the Designated NHS Live Service:

a. Supplier's performance of, and assumption of obligations under, the Connection Agreement is Service provision;

b. Supplier's liability for Service provision is limited by the applicable provisions of the Agreement ("**Limitation Terms**");

c. Notwithstanding anything to the contrary in the Connection Agreement, the Limitation Terms apply to limit Supplier's liability to the Authority (as counterparty under the Agreement and as successor to the functions of NHS Digital as counterparty under the Connection Agreement) for Service provision (whether (in the case of the Connection Agreement) for performance of the obligations in the Connection Agreement or under the indemnities it contains);

d. where the integration of Services with the Designated NHS Live Service is agreed further to the Agreement ("**Supplier Product Integration**"), performance by Supplier of any conditions or requirements of the Authority recorded further to the agreement of a Supplier Product Integration will be accepted by the Authority as performance of the obligations of the Supplier under the Connection Agreement in relation to that Supplier Product Integration.

3.4 The Authority acknowledges that (i) Service provision in order to meet Authority Requirements may require connection of Services with an NHS Live Service and the giving of the notice referred to in this paragraph may therefore be an Authority Responsibility; and (ii) the connection to such NHS Live Service may necessitate a Change under the Agreement.

Annex 1

As set out at https://digital.nhs.uk/services/nhs-app/partners-and-developers/example-documents/the-connection-agreement

SCHEDULE 3

AUTHORITY RESPONSIBILITIES

Authority Responsibilities

1 INTRODUCTION

1.1 The responsibilities of the Authority and/or any Authority Service Recipient set out in this Schedule shall constitute the Authority Responsibilities under this Agreement. Any obligations of the Authority and/or any Authority Service Recipient in Schedule 2.1 (*Services Description*) and Schedule 4.1 (*Supplier Solution*) shall not be Authority Responsibilities and the Authority and/or any Authority Service Recipient shall have no obligation to perform any such obligations unless they are specifically stated to be “Authority Responsibilities” and cross referenced in the table in Paragraph 3.

1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

The Authority and/or any Authority Service Recipient (where applicable) shall:

(a) perform those obligations of the Authority and/or any Authority Service Recipient which are set out in the Clauses of this Agreement and the Paragraphs of the Schedules (except Schedule 2.1 (*Services Description*) and Schedule 4.1 (*Supplier Solution*));

(b) provide the Supplier in a timely manner with access to, and assistance from, appropriate members of the Authority’s and/or any Authority Service Recipient’s staff and (where reasonably necessary and to the extent within Authority's or Authority Service Recipient's control) Other Suppliers, as such access or assistance is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;

(c) provide in a timely manner sufficient and suitably skilled and qualified staff to fulfil the Authority’s and/or any Authority Service Recipient’s roles and duties under this Agreement as defined in the Implementation Plan and the Ways of Working document to be defined during Implementation and Transition;

(d) provide in a timely manner such documentation, data and/or other information within the Authority's or Authority Service Recipients' possession or control and (where reasonably necessary and to the extent within Authority's or Authority Service Recipient's control) Other Suppliers that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Agreement ; and

(e) procure in a timely manner for the Supplier such agreed access and use of the Authority Premises (as a licensee only) and facilities (including relevant IT systems and network components) as is reasonably required for the Supplier to comply with its obligations under this Agreement, such access to be provided during the Authority's and/or any Authority Service Recipient’s (as applicable) normal working hours on each Working Day or as otherwise agreed by the Authority and/or any Authority Service Recipient (such agreement not to be unreasonably withheld or delayed).

3 SPECIFIC OBLIGATIONS

The Authority and/or any Authority Service Recipient (as applicable) shall, in relation to this Agreement perform the Authority's and/or any Authority Service Recipient's responsibilities identified as such in this Agreement the details of which are set out below:

Document	Location (Paragraph)
Annex 1 to this Schedule 3 (Overall Specific Authority Obligations)	All of Annex 1 to this Schedule 3
SOW	Authority Responsibilities section of the relevant SOW (such Authority Responsibilities to only apply to the relevant SOW)

Annex 1: Overall Specific Authority Obligations

Where an Authority Service Recipient requires onboarding, including access to the Data Platform these responsibilities apply to the Authority and/or such ASR as applicable. The Parties acknowledge that in order to provide certain parts of the Services, the Supplier may require access or assistance from persons who are not the Authority's employees or contractors, where necessary. For the avoidance of doubt, the Authority assumes no liability for the acts or omissions of Authority Service Recipients as per clause 3(b) of Schedule 2.6 (Authority Service Recipients), but non-performance of Authority Responsibilities by the Authority Service Recipients would (subject to the provisions of Clause 31 of the Agreement) still entitle the Supplier to relief under Clause 31 (Authority Cause) of the Agreement.

1. Authority will make its resources available as specified in the document entitled 'ISFT Schedule 4 Commercial Envelope – NHS England Staffing Model' issued as part of the Authority's tender (and 'Guidance/Assumptions' within this) until the 'Ways of Working' document is defined and agreed during Implementation and Transition (at which point Authority will make its resources available as specified in the 'Ways of Working' document shall apply)

2. Authority and/or Authority Service Recipients will run a service desk (NHS England's Service Desk and Authority Service Recipients' Service Desks)

Data Access

3. Timely access to or provisioning of Authority Data within the Authority's or Authority Service Recipients' possession or control which is necessary to provide the Services

4. Timely access to or provisioning of necessary Authority and Authority Service Recipients network components and associated necessary Authority and Authority Service Recipients infrastructure for the purposes of data ingestion and integration as required for the Supplier to provide the Services

5. Timely Authority and Authority Service Recipient information governance approvals required for the use of Authority Data by the Supplier in accordance with the Agreement.

6. Anonymising or pseudonymising personal data, or procuring the anonymisation or pseudonymising of, where required by Authority or relevant Authority Service Recipient prior to sharing with the Supplier

7. Reasonable modifications to existing Authority systems to expose Authority Data which is required by Authority or an Authority Service Recipient in order for the Supplier to provide the Services, where connectors do not exist

Support

8. Provision of L1 response and triage service for support of Foundry issues, as provided in Schedule 2.2 (Performance Levels)

9. Provision of technical personnel, including business change personnel and trainers to receive 'train the trainer' training from the Supplier as the result of the Supplier's provision of training in accordance with its responsibilities in REQ-

2.6.5.0.2 in Appendix 1B to Schedule 2.1 (Services Description), the rest of this Agreement, or an applicable SOW

Further general Authority Responsibilities

10. Promptly inform the Supplier if there is any proposed change of its Key Personnel & for the Programme

11. The Authority will provide the information/documentation to inform what the third party system data structure, format, and possible data values are so that the Supplier can generate synthetic data in the Data Platform

12. Provide adequate access to the internet and desk facilities for the Supplier team deployed at the Authority's site

13. Provide feedback, information, review and sign-off as reasonably required by the Supplier for the Supplier to develop an integrated work plan for the Programme

14. Responsible for all interfaces or data migration for Other Supplier objects outside the Supplier's scope under this Agreement

15. Responsible for (itself or for procuring from an Other Supplier) application maintenance of those legacy applications which are not required by the Authority to be transitioned to the Data Platform

16. Timely management of internal Authority communications

17. Timely and appropriate management of external PR/media enquires (with prior engagement/notification to Supplier) in accordance with the FOI Policy and FOIA and publicity provisions in the Agreement, where such enquiries include reference to the Supplier and/ or the Services

18. Take such steps, and/or furnish such documentation, as are necessary to require Other Suppliers with which the Supplier Solution or any Deliverable interfaces: to (a) engage in collaborative behaviours similar to those set out in Schedule 2.10 (Collaboration) regarding Supplier's own behaviour; and (b) provide timely patches and updates to their own systems to support resolving any regression.