DATED 28 NOVEMBER 2023

(1) NHS ENGLAND

and

(2) IQVIA LTD.

CONTRACT
relating to

Privacy Enhancing Technology Services

TABLE OF CONTENTS

THIS CONTRACT is made on 28 November 2023

BETWEEN:

(1) **NHS England** of 7-8 Wellington Place, Leeds LS1 4AP (the **"Authority"**); and

(2) **IQVIA LTD.**, a company registered in England and Wales whose registered office is 3 Forbury Place, 23 Forbury Road, Reading, United Kingdom, RG1 3JH (the **"Supplier"**),

(each a **"Party"** and together the **"Parties"**).

INTRODUCTION

(A) The Authority is an executive non-departmental public body of the Department of Health & Social Care and responsible for the National Health Service in England further to the National Health Service Act 2006, the Health and Social Care Act 2012 and the Health and Care Act 2022. The Authority wishes to procure privacy enhancing technology services in order to deliver its functions.

(B) On 21 June 2023 the Authority published a notice on the Government's Find a Tender service (ref 2023/S 000-017630), inviting prospective suppliers to submit requests to participate in a procurement for privacy enhancing technology services in relation to the Programme.

(C) The Supplier is a leading global provider of advanced analytics, technology solutions, and clinical research services to the life sciences and healthcare industries and has experience in the provision of privacy enhancing technology and associated services.

(D) On the basis of the Supplier's response to the advertisement and a subsequent tender process, the Authority selected the Supplier as its preferred supplier.

(E) The Parties have agreed to contract with each other in accordance with the terms and conditions set out below.

IT IS AGREED as follows:

1. **DEFINITIONS**

1.1 In this Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in these Terms and in particular Schedule 1 (Definitions).

2. **INTERPRETATION**

2.1 In this Contract, unless the context otherwise requires:

2.1.1 the singular includes the plural and vice versa;

2.1.2 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

2.1.3 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

2.1.4 the words "including", "other", "in particular", "for example" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation";

2.1.5 references to "writing" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of

representing or reproducing words in a visible form and expressions referring to writing shall be construed accordingly;

2.1.6 references to "Clauses" and "Schedules" are, unless otherwise provided, references to the clauses and schedules of this Contract and references in any Schedule to paragraphs, parts, annexes and tables are, unless otherwise provided, references to the paragraphs, parts, annexes and tables of the Schedule or the part of the Schedule in which the references appear;

2.1.7 the headings in this Contract are for ease of reference only and shall not affect the interpretation or construction of this Contract; and

2.2 In the event and to the extent only of a conflict between this Contract and the Applicable Supplier Terms, the conflict shall be resolved in accordance with the following descending order of precedence:

2.2.1 this Contract (excluding Schedule 4 (Supplier Solution);

2.2.2 Schedule 4 (Supplier Solution); and

2.2.3 the Applicable Supplier Terms.

3. APPLICABLE SUPPLIER TERMS

Applicable Supplier Terms:

3.1 The only terms applying to use of the Supplier Solution are the Supplier terms which are set out or expressly referred to in Schedule 17 (Applicable Supplier Terms) (the "**Applicable Supplier Terms**") and as may be modified strictly in accordance with the provisions of this Contract.

Modifications to Applicable Supplier Terms:

3.2 The Applicable Supplier Terms cannot be amended during the Term without the Authority's prior written consent.

Hyperlinks:

3.3 Where in:

3.3.1 any Applicable Supplier Terms; and/or

3.3.2 the Supplier Solution,

a standard, policy, list, terms and conditions or any other document ("**Additional Terms**") is incorporated into the relevant Applicable Supplier Terms and/or Supplier Solution by reference to a hyperlink, then such hyperlink shall be deemed ineffective and any Additional Terms shall be deemed unenforceable and shall not apply to this

Contract and this Contract shall apply as if such hyperlink to the Additional Terms was not included.

3.4 The Supplier acknowledges that Services are provided to and for the benefit of Authority Users as well as the Authority and the Parties agree to perform their obligations under Schedule 19 (Authority Users).

4. TERM

4.1 This Contract shall take effect on the Effective Date, and unless terminated earlier under the terms of this Contract, shall expire at the end of the Initial Term.

4.2 Subject to Clause 4.3 & 4.4, the Authority may elect to extend the Term as follows:

4.2.1 for a 24 month period beginning on the third (3rd) anniversary of the Commencement Date and ending on the fifth (5th) anniversary of the Commencement Date ("**First Extension Period**");

4.2.2 if the Authority elects to extend the Term by the First Extension Period, for a 12 month period beginning on the fifth (5th) anniversary of the Commencement Date and ending on the sixth (6th) anniversary of the Commencement Date ("**Second Extension Period**"); and

4.2.3 if the Authority elects to extend the Term by the Second Extension Period, for a further 12 month period beginning on the sixth (6th) anniversary of the Commencement Date and ending on the seventh (7th) anniversary of the Commencement Date ("**Third Extension Period**").

4.3 Where the Authority wishes to trigger an Extension Period, the Authority shall give the Supplier at least fifteen (15) Working Days' notice before the end of the Initial Term or the then current Extension Period (as applicable).

4.4 This Contract will not in any circumstances apply beyond the Maximum Term.

5. PROVISION AND RECEIPT OF THE SERVICES

5.1 The Supplier shall perform the Services in accordance with this Contract.

5.2 The Supplier shall ensure that the Services comply at all times and in all respects with:

5.2.1 the Service Description; and

5.2.2 the Supplier Solution.

5.3 The Supplier shall perform its obligations under this Contract in accordance with:

5.3.1 all applicable Laws; and

5.3.2 Good Industry Practice.

5.4 In its performance of its obligations under this Contract (including provision of the Services) the Supplier shall at all times comply with this Contract including the Schedules.

5.5 In its receipt and use of the Services the Authority shall at all times comply with the provisions of this Contract.

5.6 In their dealings under this Contract the Parties shall at all times behave and act reasonably and in good faith towards each other and in accordance with the collaborative behaviours set out in Clause 29 (Collaborative Behaviour).

5.7 The Authority will 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.

Service Description and Supplier Solution:

5.8 The Supplier warrants that all software described in the Supplier Solution and forming part of the Services shall:

5.8.1 be free from material design and programming errors;

5.8.2 perform in all material respects in accordance with the relevant specifications contained in the Supplier Solution; and

5.8.3 not infringe any Intellectual Property Rights.

5.9 The Service Description and Supplier Solution may only be modified in accordance with the provisions of Clauses 5.12 to 5.16 (Modifications to the Services).

Configuration Services:

5.10 In accordance with the scope of the Service Description, as part of the Services the Authority may request, and the Supplier has agreed to provide, configuration services that link the software and services described in the Supplier Solution to the Other Data Platforms ("**Configuration Services**"). In the event the Authority requires Configuration Services, the Authority shall submit a Service Request to the Supplier in accordance with Clause 5.11.

5.11 Where the Authority submits a Service Request, the Authority shall be committed to purchase and pay for such Configuration Services and the Supplier shall be obliged to provide such Configuration Services in accordance with Schedule 5 (Charges & Invoicing) and as otherwise set out under the terms of this Contract. Service Requests must be submitted in accordance with the agreed process set out in Schedule 12 (Service Request Procedure) (including any restrictions on who is authorised to submit Service Requests if specified in that Schedule).

Modifications to the Services:

5.12 The Authority acknowledges that the Services are provided by the Supplier using hardware and software systems made available to customers on a multi-tenant basis and accordingly the Supplier may need to modify the Services during the Term, for example to introduce new and improved functionality and may also include discontinuing and replacing some elements of the Services.

5.13 Subject to the Authority's right to terminate under Clause 5.15, the Supplier may, from time to time during the Term, propose a modification to the Services ("**Service Modification**") provided in each case the following conditions are satisfied:

5.13.1 subject to Clause 5.14, the Supplier has given the Authority Authorised Representative no less than thirty (30) days' prior written notice via email of the proposed Service Modification, such notice to include a hyperlink directly to a URL setting out in full and in a clear and transparent manner the relevant modified Service Descriptions for the proposed Service Modification;

5.13.2 the proposed Service Modification applies on a uniform basis to all customers in respect of the affected Services; and

5.13.3 the proposed Service Modification does not constitute a substantial modification to this Contract (including the Service Description and Supplier Solution) to the extent that the Regulations would otherwise require a new procurement procedure.

5.14 The Supplier is not required to provide prior written notice of Service Modifications under Clause 5.13.1 where and to the extent a Service Modification is reasonably necessary to enable the Supplier:

5.14.1 to comply with Law and such requirement to comply is imminent and was reasonably unforeseen by the Supplier in the circumstances; or

5.14.2 to maintain the security of the Supplier's technology infrastructure,

(in each case an "**Urgent Service Modification**") provided that as soon as is reasonably possible following completion of any Urgent Service Modification the Supplier gives the Authority Authorised Representative written notice via email of the date on which such Urgent Service Modification was made and includes in such notice brief summary details of the Urgent Service Modification together with a hyperlink directly to a URL setting out in full and in a clear and transparent manner the relevant modified Service Descriptions for that Urgent Service Modification.

5.15 Where the Authority reasonably believes a Service Modification or Urgent Service Modification has, or is likely to have, a materially adverse impact on:

5.15.1 the Authority's or any Authority User's use and enjoyment of the Services under this Contract;

5.15.2 the commercial benefits of this Contract to the Authority (including in relation to pricing and performance of the Services); and/or

5.15.3 the balance of risks under this Contract from the Authority's perspective (including the creation of new or increased potential liabilities and/or new or materially different operational responsibilities for the Authority and/or any Authority Users),

the Authority may, acting reasonably, object to the Supplier's proposed and/or actual modifications to the Services notified under Clause 5.13.1 (Service Modification) or Clause 5.14 (Urgent Service Modification) (as applicable) by notifying the Supplier in writing within 30 (thirty) days of the Authority's receipt of the Supplier's notice of such Service Modification or Urgent Service Modification (as applicable). If the Parties (acting reasonably) are unable within the next ten (10) days to resolve the Authority's objection to its reasonable satisfaction the Authority may terminate this Contract with immediate effect and without any liability (including, for the avoidance of doubt, pursuant to Clause 22.4) by giving notice in writing to the Supplier.

5.16 Where the Authority:

5.16.1 does not object to a Service Modification or Urgent Service Modification within the thirty (30) day period referred to in Clause 5.15 or

5.16.2 having objected the Authority subsequently agrees to the relevant Service Modification or Urgent Service Modification,

and subject to the conditions in Clause 5.13 being satisfied, the relevant Service Descriptions are deemed modified to reflect the relevant modified Service Descriptions notified to the Authority under either (as applicable):

(a) Clause 5.13.1 (Service Modifications), with effect from the effective date set out in the relevant email notice or where no effective date is specified thirty (30) days following the Authority's receipt of the email notice; or

(b) Clause 5.14 (Urgent Service Modifications), with effect from the effective date set out in the relevant email notice or where no effective date is specified immediately upon the Authority's receipt of the email notice,

save where any of the conditions in Clause 5.13 are not satisfied, in which case the relevant Service Modification or Urgent Service Modification is deemed invalid and shall not modify the then current relevant Service Descriptions applying to this Contract.

6. IMPLEMENTATION & MILESTONES

Implementation Plan:

6.1 The Supplier shall be responsible for preparing and maintaining a detailed Implementation Plan. A draft of the Implementation Plan is set out in Schedule 6 (Implementation Plan). The Supplier shall provide a further draft Implementation Plan to the Authority not later than thirty (30) days after the Effective Date.

6.2 The draft Implementation Plan submitted in accordance with Clause 6.1:

6.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively, including each Milestone Date, and as the Authority may otherwise require; and

6.2.2 it shall take account of all dependencies on the Authority or any other third party known to, or which should reasonably be known to, the Supplier.

6.3 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone is Achieved on or before its Milestone Date.

6.4 The Supplier shall monitor its performance against the Implementation Plan and Milestones and report to the Authority on such performance in accordance with the agreed governance processes.

Reviewing and changing the Implementation Plan:

6.5 Subject to Clause 6.3, the Supplier shall keep the Implementation Plan under review and ensure that it is updated on a regular basis.

6.6 The Authority shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

6.7 Changes to any Milestones, Milestone Payments and Delay Payments shall not be permitted unless agreed in writing by the Authority.

6.8 The Supplier shall, as soon as reasonably practicable, notify the Authority if the Supplier: (i) fails to; or (ii) becomes aware of any event or incident that could have a material impact on its ability to, meet a Milestone Date. As soon as reasonably practicable, but in any event within two (2) Working Days of receipt of such notice, the Parties will work together in good faith to agree a rectification plan to include the revised Milestone Date and the actions required to meet it. Each Party shall take such steps as are reasonably practicable to mitigate the impact of any delays to a Milestone Date.

Compliance with the Implementation Plan:

6.9 The Supplier shall:

6.9.1 comply with Implementation Plan; and

6.9.2 ensure that each Milestone is Achieved on or before its Milestone Date.

6.10 Where the Supplier is responsible for the failure to Achieve a Milestone by the relevant Milestone Date this shall constitute a material Default.

6.11 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay:

6.11.1 it shall:

(a) notify the Authority in accordance with Clause 18 (Rectification Plan Process); and

(b) use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay; and

6.11.2 if the Delay or anticipated Delay relates to a Key Milestone, the provisions of Clause 19 (Delay Payments) shall apply.

Testing and Achievement of Milestones:

6.12 The Parties shall work together in good faith to agree the test criteria determining whether or not a Milestone has been Achieved. Notwithstanding this, the Authority shall determine, in its absolute discretion, whether or not a Milestone has been Achieved.

Issue of Milestone Achievement Certificate

6.13 The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:

6.13.1 Achievement of that Milestone in accordance with Clause 6.12; and

6.13.2 performance by the Supplier to the reasonable satisfaction of the Authority of any other tasks identified in the Implementation Plan as associated with that Milestone.

6.14 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 5 (Charges & Invoicing).

7. WARRANTIES AND STANDARDS

7.1 The Supplier warrants and represents that:

7.1.1 it has full capacity and authority to enter into and to perform this Contract and this Contract is executed by its authorised representative;

7.1.2 it is a legally valid and existing organisation incorporated in the place it was formed;

7.1.3 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might reasonably be anticipated to affect its ability to perform this Contract;

7.1.4 it maintains all necessary rights, authorisations, licences and consents to perform its obligations under this Contract;

7.1.5 it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform this Contract;

7.1.6 it is not impacted by an Insolvency Event; and

7.1.7 all statements made and documents submitted by the Supplier as part of the procurement of the Services under this Contract are true and accurate.

7.2 The Supplier shall at all times during the Term comply with the Standards and maintain, where applicable, accreditation with the relevant Standards' authorisation body.

8. CHARGES, PAYMENT AND INVOICING

8.1 In consideration of the Supplier carrying out its obligations under this Contract, including the provision of the Services, the Authority shall pay the undisputed Charges.

8.2 The Charges for Services consumed or to be consumed by the Authority during the Term shall be calculated using the relevant pricing information (including applicable currency), charging model, payment profile, invoicing procedure and payment method set out or referred to in Schedule 5 (Charges & Invoicing) as these apply to the relevant Services.

8.3 The Supplier warrants that it will calculate Charges due under this Contract accurately in compliance with Schedule 5 (Charges & Invoicing).

8.4 The Supplier shall invoice the Charges to the Authority in accordance with this Clause 8 and the Authority will pay the Supplier within thirty (30) days of receipt of a valid invoice. All Supplier invoices shall be expressed and paid in pounds sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice. The Authority must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

8.5 The Charges are stated exclusive of VAT, which shall be added at the prevailing rate (with visibility of the amount as a separate line item) as applicable and paid by the Authority following delivery of a valid invoice.

8.6 The Authority may retain or set off any amount owed to it by the Supplier (including any Authority's Existing Entitlement) against any amount due to the Supplier under this Contract or under any other agreement between the Supplier and the Authority.

8.7 If the Authority wishes to exercise its right pursuant to Clause 8.6 it shall give notice to the Supplier within thirty (30) days of receipt of the relevant invoice, setting out the Authority's reasons for retaining or setting off the relevant Charges.

8.8 If there's an invoice dispute, the Authority must pay any undisputed amount and return the invoice within 10 Working Days of the invoice date. The Authority will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Authority within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

8.9 Due to the nature of the Services it is not practicable in a static Schedule to agree in detail exactly the quantity and rate of consumption of the Services during the Term. Accordingly, the Charges due under this Contract are calculated (in accordance with the process set out in Schedule 5 (Charges & Invoicing)) by reference to the Authority's actual consumption of Services. Accordingly, the Supplier agrees that the Authority's anticipated quantities and rates of consumption of Services are indicative only.

9. LIABILITIES

Unlimited liability:

9.1 Neither Party limits its liability for:

9.1.1 death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors (as applicable);

9.1.2 fraud or fraudulent misrepresentation by it or its employees;

9.1.3 breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or

9.1.4 any liability to the extent it cannot be limited or excluded by Law.

9.2 The Supplier's liability in respect of the indemnity in Clause 10.7 shall be unlimited.

Financial and other limits:

9.3 Subject to Clauses 9.1 and 9.2 (Unlimited Liability) and Clause 9.6 (Consequential losses):

9.3.1 the Supplier's aggregate liability in respect of loss of or damage to Authority Data or breach of the Data Protection Legislation that is caused by Default of the Supplier occurring in each and any Contract Year shall in no event exceed [Redacted under FOIA s43, Commercial interests];

9.3.2 the Supplier's aggregate liability in respect of all other Losses incurred by the Authority under or in connection with this Contract as a result of Defaults by the Supplier [Redacted under FOIA s43, Commercial interests]; and

9.3.3 the Supplier's aggregate liability in respect of all Service Credits incurred in any rolling period of 12 months [Redacted under FOIA s43, Commercial interests] ("**Service Credit Cap**").

9.4 Deductions from Charges shall not be taken into consideration when calculating the Supplier's liability under Clause 9.3.2. The Supplier hereby expressly agrees that any Losses of any NHS Body incurred in connection with or in relation to this Contract arising in contract, tort (including negligence) or otherwise shall be deemed to be (and shall be) the Losses of the Authority.

9.5 Subject to Clauses 9.1 (Unlimited Liability) and Clause 9.6 (Consequential Losses), and without prejudice to the Authority's obligation to pay the Charges as and when they fall due for payment, the Authority's total aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Contract as a result of Defaults by the Authority [Redacted under FOIA s43, Commercial interests].

Consequential Losses:

9.6 Subject to Clauses 9.1 and 9.2 (Unlimited Liability) and Clause 9.7, neither Party shall be liable to the other Party for:

9.6.1 any indirect, special or consequential Loss; or

9.6.2 any loss of profits, turnover, business opportunities or damage to goodwill (in each case whether direct or indirect).

9.7 Notwithstanding Clause 9.6 but subject to Clause 9.3, the Supplier acknowledges that the Authority may, amongst other things, recover from the Supplier the following Losses incurred by the Authority and any Authority User to the extent that they arise as a result of a Default by the Supplier:

9.7.1 any additional operational and/or administrative costs and expenses incurred by the Authority and any Authority User, including costs relating to time spent by or on behalf of the Authority and any Authority User in dealing with the consequences of the Default;

9.7.2 any wasted expenditure or charges;

9.7.3 the additional cost of procuring Replacement Services for the remainder of the Term and/or replacement Deliverable Items, which shall include any incremental costs associated with such Replacement Services and/or replacement Deliverable Items above those which would have been payable under this Contract;

9.7.4 any compensation or interest paid to a third party by the Authority and/or any Authority User; and

9.7.5 any fine or penalty incurred by the Authority and any Authority User pursuant to Law and any costs incurred by the Authority and any Authority User in defending any proceedings which result in such fine or penalty.

Mitigation:

9.8 Each Party shall use all reasonable endeavours to mitigate any loss or damage suffered arising out of or in connection with this Contract, including any Losses for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Contract.

Notice and conduct of Indemnity Claims:

9.9 If a Beneficiary is notified of a Claim then it must notify the Provider as soon as reasonably practical and no later than 10 Working Days.

9.10 At the Provider's cost and expense the Beneficiary must both:

9.10.1 allow the Provider to conduct all negotiations and proceedings to do with a Claim; and

9.10.2 give the Provider reasonable assistance with the Claim if requested.

9.11 The Beneficiary must not make admissions about the Claim without the prior written consent of the Provider which cannot be unreasonably withheld or delayed.

9.12 The Provider must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

9.13 The Provider must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

9.14 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

9.15 If the Provider pays the Beneficiary money under an indemnity or under Clause 10.5.2 (as applicable) and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Provider the lesser of either:

9.15.1 the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

9.15.2 the amount the Provider paid the Beneficiary for the Claim.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 Save for the licences expressly granted pursuant to Clauses 10.3 and 10.4, neither Party shall acquire any right, title or interest in or to the IPR (whether pre-existing or created during the Term) of the other Party or its licensors.

10.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

10.3 The Authority grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Term to use the Authority's or its relevant licensor's Authority Content and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that:

10.3.1 any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Clause 26 (Confidentiality); and

10.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Authority's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Authority.

10.4 The Supplier grants to:

10.4.1 the Authority; and

10.4.2 the Authority Users,

the licence taken from its Applicable Supplier Terms as set out or expressly referred to in Schedule 4 (Supplier Solution) under the heading 'Licence Terms' which licence shall, as a minimum, grant the Authority and any Authority Users a non-exclusive, non-transferable licence during the Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Contract and subject to the terms of the MoU.

10.5 Subject to the limitation in Clause 9.5, the Authority shall:

10.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Authority and/or Authority Users is in breach of applicable Law;

(b) alleging that the Authority Content violates, infringes or misappropriates any rights of a third party;

(c) alleging that the Authority's and/or Authority User's use of the Services is in material breach of the Applicable Supplier Terms;

(d) arising from the Supplier's use of the Authority Content in accordance with this Contract; and

10.5.2 in addition to defending in accordance with Clause 10.5.1, the Authority will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Authority,

provided that the Authority's obligations under this Clause 10.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

IPR Indemnity:

10.6 The Supplier shall ensure and procure that the availability, provision and use of the Services and the performance of the Supplier's responsibilities and obligations hereunder shall not infringe any Intellectual Property Rights of any third party.

10.7 The Supplier will during and after the Term, on written demand, defend and indemnify and keep the Authority and/or any Authority Users indemnified from and against all Losses incurred by, awarded against or agreed to be paid by the Authority and/or any Authority Users (whether before or after the making of the demand pursuant to the indemnity hereunder) arising from an IPR Claim.

Supplier options:

10.8 If an IPR Claim is made, or the Supplier anticipates that an IPR Claim might be made, the Supplier may, at its own expense and sole option, either:

10.8.1 procure for the Authority the right to continue using the relevant item which is subject to the IPR Claim; or

10.8.2 replace or modify the relevant item with non-infringing substitutes provided that:

(a) the performance and functionality of the replaced or modified item is at least equivalent to the performance and functionality of the original item;

(b) the replaced or modified item does not have an adverse effect on any other Services;

(c) there is no additional cost to the Authority and/or any Authority User; and

(d) the terms and conditions of this Contract shall apply to the replaced or modified Services.

10.9 The indemnity in Clause 10.7 shall not apply where and to the extent an IPR Claim and/or any Losses arising from such an IPR Claim, arise directly from and would not have arisen in the absence of:

10.9.1 the use of any Authority Content provided by the Authority and/or any Authority User; and/or

10.9.2 the Authority's breach of this Contract and/or any Authority User's breach of any of the Applicable Supplier Terms.

10.10 If the Supplier elects to procure a licence in accordance with Clause 10.8.1 or to modify or replace an item pursuant to Clause 10.8.2, but this has not avoided or resolved the IPR Claim, then:

10.10.1 the Authority may terminate this Contract by written notice with immediate effect; and

10.10.2 without prejudice to the indemnity set out in Clause 10.7, the Supplier shall be liable for all reasonable and unavoidable costs of the substitute items and/or services including the additional costs of procuring, implementing and maintaining the substitute items.

11. PUBLICITY AND BRANDING

11.1 The Supplier shall not, and shall take all reasonable steps to ensure the Supplier staff do not, make any press announcements or publicise this Contract or any part of it in any way nor use the Authority's name or brand in any promotion or marketing or announcement of orders, without the Authority's prior written approval (the decision of the Authority to approve or not shall not be unreasonably withheld or delayed).

11.2 Each Party acknowledges to the other that nothing in this Contract either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Services) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

12. AUTHORITY CONTENT AND SECURITY REQUIREMENTS

12.1 The Supplier shall comply with the cyber security and information governance requirements set out in Schedule 3 (Cyber Security and Information Governance).

12.2 The Supplier shall not access, store, copy, disclose or use any of the Authority Content uploaded to the relevant data storage platform(s) other than for the sole purpose and to the extent necessary to provide the Services or as otherwise approved in advance and in writing by the Authority, unless the Supplier is required to do so by Law. If it is so required the Supplier shall promptly notify the Authority before doing so unless prohibited by Law.

12.3 If the Supplier suspects that the Authority Content has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Authority without undue delay and within 72 hours of becoming aware and will (at its own cost if corruption, loss, breach or degradation of the Authority Content was caused by the act or omission of the Supplier) comply with any remedial action reasonably proposed by the Authority.

12.4 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

12.5 If Malicious Software causes loss of operational efficiency or loss or corruption of Authority Content, the Supplier will assist and support the Authority to mitigate any Losses and restore the Services to operating efficiency as soon as possible.

12.6 [Redacted under FOIA s43, Commercial interests]

12.7 The Authority acknowledges it has responsibilities in relation to security where and to the extent described in the relevant Applicable Supplier Terms and applicable Service Descriptions.

13. **KEY PERFORMANCE INDICATORS**

13.1 The Supplier shall:

13.1.1 provide the Services in such a manner so as to meet or exceed the Target Performance Level for each Key Performance Indicator from the Commencement Date; and

13.1.2 comply with the provisions of Schedule 8 (Performance Levels) in relation to the monitoring and reporting of its performance against the Key Performance Indicators.

Performance Failures:

13.2 If in any Service Period:

13.2.1 a KPI Failure occurs in respect of a Critical KPI, Service Points shall be calculated in accordance with Schedule 8 (Performance Levels) and Service Credits deducted from the Service Charges in accordance with Schedule 5 (Charges & Invoicing); and

13.2.2 a Material KPI Failure occurs, the Supplier shall comply with the Rectification Plan Process (in addition to Service Credits accruing in accordance with Clause 13.2.1 where the KPI Failure is in respect of a Critical KPI).

13.3 Service Credits shall not be the Authority's exclusive financial remedy for a KPI Failure in respect of a Critical KPI.

Critical Performance Failure:

13.4 If a Critical Performance Failure occurs, the Authority may exercise its rights to terminate this Contract in whole or in part pursuant to Clause 21.4 (Termination by the Authority).

14. **RECORDS AND AUDIT**

14.1 The Supplier will maintain full and accurate records and accounts, using good industry practice and generally accepted accounting principles, of the:

14.1.1 operation of this Contract and the Services provided under it (including any Sub-Contracts); and

14.1.2 amounts paid by the Authority under this Contract.

14.2 The Supplier's records and accounts will be kept until the latest of the following dates:

14.2.1 7 years after the date of termination or expiry of this Contract; or

14.2.2 another date agreed between the Parties.

14.3 During the timeframes highlighted in Clause 14.2, the Supplier will maintain:

14.3.1 commercial records of the Charges and costs (including Sub-Contractors' costs) and any variations to them, including proposed variations;

14.3.2 books of account for this Contract;

14.3.3 access to its published accounts and trading entity information;

14.3.4 proof of its compliance with its obligations under the Data Protection Legislation and the transparency and data protection provisions under this Contract; and

14.3.5 records of its delivery performance under this Contract, including that of its Sub-Contractors.

14.4 The Supplier will allow representatives of the Authority, the Comptroller and Auditor General and their staff, any appointed representatives of the National Audit Office, HM

Treasury, the Cabinet Office and any successors or assigns of any of the above, access to the records, documents, and account information referred to in Clause 14.3 (including access to online records (including any Security Assessment Documents)) as may be required by them and subject to reasonable and appropriate confidentiality undertakings, to verify and review:

14.4.1 the accuracy of the Charges (and proposed or actual variations to them under this Contract);

14.4.2 any books of accounts kept by the Supplier in connection with the provision of the Services only for the purposes of auditing the Charges under this Contract;

14.4.3 the integrity, confidentiality and security of the Authority Content held or used by the Supplier;

14.4.4 any other aspect of the delivery of the Services including to review compliance with any Law; and

14.4.5 any records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records.

14.5 The Authority acknowledges that the rights of audit or inspection under this Clause 14 shall not include the right to audit or inspect the Supplier's physical infrastructure.

14.6 Notwithstanding any provisions of the DPA and/or any other Applicable Supplier Terms, throughout the Term the Supplier shall appoint external auditors to inspect and verify the continued adequacy and effectiveness of its Protective Measures in respect of the Services (including the security of the physical data centres from which the Supplier provides the Services) ("**Security Audit**"). The Supplier shall ensure:

14.6.1 Security Audits are undertaken at least annually by external auditors appointed by the Supplier and at the Supplier's sole cost and expense;

14.6.2 external auditors appointed to undertake Security Audits are suitably qualified and experienced independent third party organisations, whose identity the Supplier shall disclose to the Authority upon request;

14.6.3 are undertaken in accordance with ISO 27001 (or other substantially equivalent alternative standard(s)); and

14.6.4 any Security Audit results in the independent external auditors providing written summary reports, certifications and/or attestations of compliance (as applicable) in accordance with good industry practice ("**Security Assessment Documents**") capable of being used by the Authority so that it can reasonably assess and assure itself as to the continued adequacy and effectiveness of the Supplier's Protective Measures, the Supplier's compliance with those Protective Measures and its obligations under the Data Protection Legislation in respect of its provision of the Services in accordance with this Contract.

14.7 Upon the Authority's request, and subject to the confidentiality undertakings of this Contract, the Supplier shall at the Authority's option either provide a copy or make available to the Authority for review the Security Assessment Documents. The Security Assessment Documents will be treated as the Supplier's Confidential Information.

14.8 Subject to any confidentiality obligations, the Supplier will use reasonable endeavours to provide all audit information within scope and give auditors access to Supplier Personnel and in each case without undue delay.

14.9 The Authority will use reasonable endeavours to ensure that any audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of audits carried out by the auditors is outside of the Authority's control.

14.10 Each Party is responsible for its own costs incurred in respect of its compliance with the audit obligations in this Clause 14, save that the Supplier will reimburse the Authority its reasonable Audit costs if the Audit reveals a material Default.

15. SUPPLY CHAIN RIGHTS AND PROTECTION

Register of Key Sub-Contractors and Sub-processors:

15.1 The Supplier warrants that the Key Sub-Contractors and Sub-processors as at the Effective Date shall be those set out in Schedule 15 (Key Sub-Contractors) as at that date. Throughout the Term the Supplier shall notify promptly the Authority in writing of any additional or replacement Key Sub-Contractors and Sub-processors (and in the case of any additional or replacement Sub-processors in accordance with the provisions of Clause 17.11) appointed after the Effective Date and maintain at all times throughout the Term an accurate, complete and up to date list of all Key Sub-Contractors and Sub-processors used in the provision of the Services (the "**Supplier's Register**"), such list to contain as a minimum:

15.1.1 the trading name of each Sub-processor and each Key Sub-Contractor and their respective registered company names, if different;

15.1.2 a brief description of each Sub-processor's and each Key Sub-Contractor's role in the provision of the Services;

15.1.3 whether each Key Sub-Contractor should reasonably be categorised as a Sub-processor under Data Protection Legislation; and

15.1.4 details of any third party which is not a Key Sub-Contractor, but which should reasonably be categorised as a Sub-processor under Data Protection Legislation.

15.2 The Supplier's Register is the Supplier's Confidential Information. For the avoidance of doubt, the Confidential Information that the Authority may disclose under Clause 26.7 shall include the Supplier's Register.

Supply Chain Protection:

15.3 Where the Supplier enters into a Sub-Contract wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract the Supplier shall pay any undisputed sums which are due from the Supplier to the relevant Sub-Contractor under that Sub-Contract within thirty (30) days from the receipt of a valid invoice.

15.4 Notwithstanding any provision of Clause 26 (Confidentiality) and 11 (Publicity and Branding) if the Supplier notifies the Authority that the Supplier has failed to pay an undisputed Sub-Contractor's invoice within thirty (30) days of receipt, or the Authority otherwise discovers the same, the Authority shall be entitled to publish the details of the late payment or non-payment (including on Government websites and in the press).

Retention of Legal Obligations:

15.5 The Supplier shall remain responsible for all acts and omissions of its Sub-Contractors and the acts and omissions of those employed or engaged by the Sub-Contractors as if they were its own.

Income Tax and National Insurance Contributions:

15.6 Where the Supplier or any Supplier Personnel are liable to be taxed in the UK or to pay national insurance contributions in respect of consideration received under this Contract, the Supplier shall:

15.6.1 at all times comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, and the Social

Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to national insurance contributions, in respect of that consideration; and

15.6.2 indemnify the Authority against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Supplier Personnel.

16. INSURANCE

The Supplier shall effect and maintain insurances in relation to the performance of this Contract in accordance with Schedule 13 (Insurance Requirements) of this Contract.

17. PROTECTION OF PERSONAL DATA

17.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority or an Authority User is the Controller and the Supplier is the Processor unless otherwise specified in a Schedule of Processing. The only Processing that the Supplier is authorised to do is listed in a Schedule of Processing and may not be determined by the Supplier.

17.2 The Supplier shall notify the relevant Controller immediately if it considers that any Controller's documented instructions infringe the Data Protection Legislation.

17.3 The Supplier shall provide all reasonable assistance to the Authority and an Authority User in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance will include:

17.3.1 a systematic description of the envisaged processing operations and the purpose of the Processing;

17.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

17.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

17.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

17.4 The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

17.4.1 Process that Personal Data only in accordance with any Schedule of Processing, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the relevant Controller before Processing the Personal Data unless prohibited by Law;

17.4.2 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

17.4.3 ensure that:

(a) the Supplier’s personnel do not Process Personal Data except in accordance with this Contract (and in particular any Schedule of Processing);

(b) it takes all reasonable steps to ensure the reliability and integrity of any of the Supplier's personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Supplier's duties under this Clause 17;

(ii) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(iii) 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 Authority or as otherwise permitted by this Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

17.4.4 not transfer Personal Data to a Restricted Country unless the prior written consent of the Authority has been obtained or the Supplier is required to do so by Law. If it is so required the Supplier shall promptly notify the Authority before doing so unless prohibited by Law. Where written consent has been obtained, the following conditions must also be fulfilled before transfer:

(a) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer in accordance with UK GDPR Article 46 as determined by the Authority;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) the Supplier 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 Authority in meeting its obligations); and

(d) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data; and

(e) in respect of any Processing in, or transfer of Personal Data to, any Restricted Country permitted in accordance with this Clause 17.4.4, the Supplier shall, when requested by the Authority, promptly enter into an agreement with the Authority including or on such provisions as the Standard Contractual Clauses and/or such variation as a regulator or the Authority might require which terms shall, in the event of any conflict, take precedence over those in this Clause 17, and the Supplier shall comply with any reasonable instructions notified to it in advance by the Authority with respect to the transfer of the Personal Data; and

17.4.5 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of this Contract unless the Supplier is required by Law to retain the Personal Data.

17.5 Subject to Clause 17.6, the Supplier shall notify the Authority without undue delay:

17.5.1 and in any event within five (5) Working Days of receipt of the request if it:

(a) receives a Data Subject Request (or purported 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; or

(d) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

17.5.2 and, where feasible, not later than 72 hours of:

(a) becoming aware of a Data Loss Event; or

(b) receiving any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract.

17.6 The Supplier's obligation to notify under Clause 17.5 shall include the provision of further information to the Authority in phases, as details become available.

17.7 Taking into account the nature of the Processing, the Supplier shall provide the Authority with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 17.5 (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

17.7.1 the Authority with full details and copies of the complaint, communication or request;

17.7.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

17.7.3 the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

17.7.4 assistance as requested by the Authority following any Data Loss Event;

17.7.5 assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.

17.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Clause 17.

17.9 Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.

17.10 The Supplier shall not provide any third party with access to Personal Data without prior written notice to the Authority and an opportunity for the Authority to object pursuant to Clause 17.11, unless the Supplier is required to provide access by Law. If it is so required the Supplier shall promptly notify the Authority before providing access unless prohibited by Law. The Authority provides general written consent to the Supplier to engage those Sub-processors (including relevant details of such Sub-processor's Processing of Personal Data) as recorded in the Supplier's Register as at the Effective Date provided that before allowing any Sub-processor to process any Personal Data related to this Contract, the Supplier must:

17.10.1 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Clause 17 such that they apply to the Sub-processor; and

17.10.2 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

17.11 Where the Supplier intends to appoint a Sub-processor not identified as a Sub-processor in the Supplier's Register as at the Effective Date, the Supplier shall provide not less

than 30 (thirty) days' prior written notice via email to the Authority Authorised Representative. Where the Authority reasonably believes such proposed Sub-processor has, or is likely to have a materially adverse impact on:

17.11.1 the Authority's use and enjoyment of the Services under this Contract;

17.11.2 the commercial benefits of this Contract to the Authority (including in relation to pricing and performance of the Services); and/or

17.11.3 the balance of risks under this Contract from the Authority's perspective (including the creation of new or increased potential liabilities and/or new or materially different operational responsibilities for the Authority and/or any Authority Users),

the Authority may, acting reasonably, object to such proposed appointment by notifying the Supplier in writing within 30 (thirty) days of the Authority's receipt of the Supplier's email notice of proposed appointment. If the Parties (acting reasonably) are unable within the next 10 (ten) days to resolve the Authority's objection to its reasonable satisfaction the Authority may terminate this Contract with immediate effect and without any liability (including, for the avoidance of doubt, pursuant to Clause 22.4) by giving notice in writing to the Supplier.

17.12 The Supplier shall remain fully liable for all acts or omissions of any of its Sub-processors.

17.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Subject to the Supplier's prior written consent (such consent not to be unreasonably withheld or delayed) the Authority may, at any time on not less than thirty (30) Working Days' notice to the Supplier:

17.13.1 revise this Clause 17 (Protection of Personal Data) by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by Attachment to this Contract); and/or

17.13.2 amend this Contract to ensure that it complies with any guidance, codes of practice, codes of conduct, regulatory guidance, standard clauses or any other related laws arising from the UK GDPR.

17.14 Without prejudice to the foregoing, the Parties acknowledge that in performing its obligations under this Contract, the Supplier will from time to time collect and Process on an incidental basis limited amounts of Personal Data of the Authority and/or Authority Users (for example names and business contact details of points of contact at the Authority and/or Authority Users) ("**CRM Personal Data**") processed in the ordinary course of business. The Supplier shall, when Processing such CRM Personal Data, do so as a Controller and shall ensure that it fully complies with its obligations under the Data Protection Legislation.

17.15 In respect of such CRM Personal Data, the Supplier shall:

17.15.1 Comply with the obligations in clauses 17.4.2, 17.4.3(b), 17.4.4, 17.4.5, 17.5, 17.6, 17.10 and 17.11;

17.15.2 ensure that it has all necessary notices and consents in place to enable it to Process the CRM Personal Data;

17.15.3 provide full information, in the form of a suitable privacy policy, to any Data Subject whose CRM Personal Data may be Processed by the Supplier under this Contract, concerning the nature such Processing;

17.15.4 not, by its acts or omissions, place the Authority and/or any Authority User in breach of the Data Protection Legislation; and

17.15.5 ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, the CRM Personal Data.

17.16 The Supplier shall not Process CRM Personal Data for any purposes other than those set out in this Contract.

18. RECTIFICATION PLAN PROCESS

18.1 In the event that:

18.1.1 there is, or is reasonably likely to be, a Delay;

18.1.2 in any Service Period there has been a Material KPI Failure; and/or

18.1.3 the Supplier commits a material Default that is capable of remedy (and for these purposes a material Default may be a single material Default or a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are remedied) which taken together constitute a material Default),

(each a "**Notifiable Default**"), the Supplier shall notify the Authority of the Notifiable Default as soon as practicable but in any event within 3 Working Days of becoming aware of the Notifiable Default, detailing the actual or anticipated effect of the Notifiable Default and, unless the Notifiable Default also constitutes a Rectification Plan Failure or other Supplier Termination Event, the Authority may not terminate this Contract in whole or in part on the grounds of the Notifiable Default without first following the Rectification Plan Process.

Notification:

18.2 If:

18.2.1 the Supplier notifies the Authority pursuant to Clause 18.1 that a Notifiable Default has occurred; or

18.2.2 the Authority notifies the Supplier that it considers that a Notifiable Default has occurred (setting out sufficient detail so that it is reasonably clear what the Supplier has to rectify),

then, unless the Notifiable Default also constitutes a Supplier Termination Event and the Authority serves a termination notice, the Supplier shall comply with the Rectification Plan Process.

18.3 The "**Rectification Plan Process**" shall be as set out in Clauses 18.4 (Submission of the draft Rectification Plan) to 18.9 (Agreement of the Rectification Plan).

Submission of the draft Rectification Plan:

18.4 The Supplier shall submit a draft Rectification Plan to the Authority for it to review as soon as possible and in any event within 10 Working Days (or such other period as may be agreed between the Parties) after the original notification pursuant to Clause 18.2 (Notification). The Supplier shall submit a draft Rectification Plan even if the Supplier disputes that it is responsible for the Notifiable Default.

18.5 The draft Rectification Plan shall set out:

18.5.1 full details of the Notifiable Default that has occurred, including a root cause analysis;

18.5.2 the actual or anticipated effect of the Notifiable Default; and

18.5.3 the steps which the Supplier proposes to take to rectify the Notifiable Default (if applicable) and to prevent such Notifiable Default from recurring, including

timescales for such steps and for the rectification of the Notifiable Default (where applicable).

18.6 The Supplier shall promptly provide to the Authority any further documentation that the Authority reasonably requires to assess the Supplier's root cause analysis. If the Parties do not agree on the root cause set out in the draft Rectification Plan, either Party may refer the matter to be determined by an expert in accordance with Schedule 10 (Dispute Resolution Procedure).

Agreement of the Rectification Plan:

18.7 The Authority may reject the draft Rectification Plan by notice to the Supplier if, acting reasonably, it considers that the draft Rectification Plan is inadequate, for example because the draft Rectification Plan:

18.7.1 is insufficiently detailed to be capable of proper evaluation;

18.7.2 will take too long to complete;

18.7.3 will not prevent reoccurrence of the Notifiable Default; and/or

18.7.4 will rectify the Notifiable Default but in a manner which is unacceptable to the Authority.

18.8 The Authority shall notify the Supplier whether it consents to the draft Rectification Plan as soon as reasonably practicable. If the Authority rejects the draft Rectification Plan, the Authority shall give reasons for its decision and the Supplier shall take the reasons into account in the preparation of a revised Rectification Plan. The Supplier shall submit the revised draft of the Rectification Plan to the Authority for review within 5 Working Days (or such other period as agreed between the Parties) of the Authority's notice rejecting the first draft.

18.9 If the Authority consents to the Rectification Plan:

18.9.1 the Supplier shall immediately start work on the actions set out in the Rectification Plan; and

18.9.2 the Authority may no longer terminate this Contract in whole or in part on the grounds of the relevant Notifiable Default,

save in the event of a Rectification Plan Failure or other Supplier Termination Event.

19. SUPPLIER RELIEF DUE TO AUTHORITY CAUSE

19.1 Notwithstanding any other provision of this Contract, if the Supplier has failed to:

19.1.1 Achieve a Milestone by its Milestone Date;

19.1.2 provide the Services in accordance with the Key Performance Indicators; and/or

19.1.3 comply with its obligations under this Contract,

(each a **"Supplier Non-Performance"**),

and can demonstrate that the Supplier Non-Performance would not have occurred but for an Authority Cause, then (subject to the Supplier fulfilling its obligations in this Clause 19):

(a) the Supplier shall not be treated as being in breach of this Contract to the extent the Supplier can demonstrate that the Supplier Non-Performance was caused by the Authority Cause;

(b) the Authority shall not be entitled to exercise any rights that may arise as a result of that Supplier Non-Performance to terminate this Contract pursuant to Clause 21.2 or 21.4;

(c) where the Supplier Non-Performance constitutes the failure to Achieve a Milestone by its Milestone Date:

(i) if the Authority considers it appropriate, will make consequential revisions to the Milestone Dates resulting from the Authority Cause;

(ii) the Supplier shall have no liability to pay any Delay Payments associated with the Key Milestone to the extent that the Supplier can demonstrate that such failure was caused by the Authority Cause;

(d) where the Supplier Non-Performance constitutes a KPI Failure:

(i) the Supplier shall not be liable to accrue Service Credits; and

(ii) the Supplier shall be entitled to invoice for the Service Charges for the relevant Services affected by the Authority Cause,

in each case, to the extent that the Supplier can demonstrate that the KPI Failure was caused by the Authority Cause.

19.2 In order to claim any of the rights and/or relief referred to in Clause 19.1, the Supplier shall as soon as reasonably practicable (and in any event within five (5) Working Days) after becoming aware that an Authority Cause has caused, or is reasonably likely to cause, a Supplier Non-Performance, give the Authority notice (a **"Relief Notice"**) setting out details of:

19.2.1 the Supplier Non-Performance;

19.2.2 the Authority Cause and its effect, or likely effect, on the Supplier's ability to meet its obligations under this Contract;

19.2.3 any steps which the Authority can take to eliminate or mitigate the consequences and impact of such Authority Cause; and

19.2.4 the relief claimed by the Supplier.

19.3 Following the receipt of a Relief Notice, the Authority shall as soon as reasonably practicable consider the nature of the Supplier Non-Performance and the alleged Authority Cause and whether it agrees with the Supplier's assessment set out in the Relief Notice as to the effect of the relevant Authority Cause and its entitlement to relief, consulting with the Supplier where necessary.

19.4 The Supplier shall use all reasonable endeavours to eliminate or mitigate the consequences and impact of an Authority Cause, including any Losses that the Supplier may incur and the duration and consequences of any Delay or anticipated Delay.

19.5 If a Dispute arises as to:

19.5.1 whether a Supplier Non-Performance would not have occurred but for an Authority Cause; and/or

19.5.2 the nature and/or extent of the relief and/or compensation claimed by the Supplier,

either Party may refer the Dispute to the Dispute Resolution Procedure. Pending the resolution of the Dispute, both Parties shall continue to resolve the causes of, and mitigate the effects of, the Supplier Non-Performance.

19.6 Any variation that is required pursuant to this Clause 19 shall be implemented in accordance with Clause 39 (Variation).

20. DELAY PAYMENTS

20.1 Subject to Clause 19 (Supplier Relief Due to Authority Cause), if a Key Milestone (or any interim milestone forming part of that Key Milestone) has not been Achieved by its relevant Milestone Date, the Supplier shall, subject to the Delay Payments Cap, pay to the Authority the Delay Payments as set out in Schedule 5 (Charges & Invoicing).

20.2 Delay Payments shall be the Authority's exclusive financial remedy for the Supplier's failure to Achieve a Key Milestone by its Milestone Date except where the Authority is entitled to or does terminate this Contract pursuant to Clause 21.4 (Termination by the Authority).

21. TERMINATION AND EXPIRY

21.1 During the Initial Term, the Authority may terminate this Contract without reason (and, subject to Clause 22.4, without any liability whatsoever or howsoever arising from the Authority's termination under this Clause 21.1) by issuing a written notice to the Supplier giving at least thirty (30) days' written notice, provided that such termination shall not take effect until the anniversary of the Commencement Date immediately following expiry of the thirty (30) day written notice period.

21.2 The Authority may terminate this Contract at any time with immediate effect for material Default by issuing a written notice to the Supplier where:

21.2.1 the Supplier commits any material Default of this Contract which is not, in the reasonable opinion of the Authority, capable of remedy; and/or

21.2.2 the Supplier commits a Default, including a material Default, which in the opinion of the Authority is remediable but has not remedied such Default to the satisfaction of the Authority within fifteen (15) Working Days of being notified in writing to do so.

21.3 For the purpose of Clause 21.2, a material Default may be a single material Default or a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are remedied) which taken together constitute a material Default.

21.4 The Authority may terminate this Contract at any time with immediate effect by issuing a written notice to the Supplier where a Supplier Termination Event occurs.

21.5 The Supplier may, by issuing a written notice to the Authority, terminate this Contract if the Authority fails to pay an undisputed sum due to the Supplier under this Contract and such sum remains outstanding forty (40) Working Days after the receipt by the Authority of a written notice of non-payment from the Supplier specifying:

21.5.1 the Authority's failure to pay;

21.5.2 the correct overdue and undisputed sum;

21.5.3 the reasons why the undisputed sum is due; and

21.5.4 the requirement on the Authority to remedy the failure to pay,

and this Contract shall then terminate on the date specified in the Supplier's written notice (which shall not be less than twenty (20) Working Days from the date of the issue of that notice).

22. CONSEQUENCES OF TERMINATION AND EXPIRY

22.1 Even if a notice has been served to terminate this Contract, the Supplier must continue to provide ordered Services until the dates set out in the notice and as necessary to comply with this Clause 22.

22.2 Expiry or termination of this Contract will not affect:

22.2.1 any rights, remedies or obligations accrued before its termination or expiry (as applicable); and

22.2.2 the right of either Party to recover any amount outstanding at the time of termination or expiry (as applicable).

22.3 Upon termination or expiry of this Contract and subject always to Clause 22.4.1:

22.3.1 the rights and obligations of the Parties under this Contract will cease immediately (including the Authority's payment obligations under this Contract save where and to the extent any payments are expressly stated in this Contract to be payable by the Authority following termination or expiry of this Contract), except for those continuing provisions identified in Clause 22.5;

22.3.2 the Authority will:

(a) pay any outstanding Charges properly due to the Supplier;

(b) extract and/or destroy all copies of the Authority Content for which it had been using the Services. The Supplier shall retain the Authority Content and allow the Authority to extract the Authority Content for a period of 60 (sixty) days following expiry or termination or such other period as may be specified in the Exit Management Plan and the Supplier shall be entitled to a reasonable charge for continuing to provide the Authority with access to the Services for this purpose during the relevant period;

22.3.3 the Supplier will:

(a) comply with any exit related obligations as specified in the Exit Management Plan;

(b) within 10 Working Days of the termination or expiry date, return to the Authority on a pro rata basis any sums paid in advance for Services due to be provided by the Supplier under this Contract for any period post the termination or expiry date (as applicable);

(c) following the expiry of the period referred to in Clause 22.3.2(b), promptly destroy all copies of the Authority Content when it receives the Authority's written instructions to do so or within 12 calendar months after the termination or expiry date; and

(d) provide the Authority with written confirmation that the Authority Content has been securely destroyed pursuant to Clause 22.3.3(c), except if the retention of any of Authority Content is required by Law; and

22.3.4 each Party will promptly either:

(a) return all copies of the other's Confidential Information in such Party's custody, possession or control unless there is a legal requirement to keep it or this Contract states otherwise; or

(b) (where the other Party has given its prior written consent to its destruction) destroy the other Party's Confidential Information and confirm its destruction to the reasonable satisfaction of the other Party.

22.4 If the Authority terminates this Contract for convenience pursuant to Clause 21.1 (but not, for the avoidance of any doubt, termination pursuant to any other right of termination) before the Milestone Date in respect of Milestone 1, the Authority shall pay

the Supplier an amount equal to the Milestone Payment in respect of Milestone 1. The Supplier may not charge the Authority any fees, costs or expenses relating to:

22.4.1 the Authority's extraction, transfer and/or destruction of Authority Content whenever and howsoever after such termination; or

22.4.2 the Supplier complying with its exit related obligations under this Contract.

22.5 The following Clauses survive the termination or expiry of this Contract: Clauses 1 (Definitions), 2 (Interpretation), 3 (Applicable Supplier Terms), 9 (Liabilities), 10 (Intellectual Property Rights), 11 (Publicity and Branding), 14 (Records and Audit), 17 (Protection of Personal Data), 21 (Termination and Expiry), 22 Consequences of Termination and Expiry), 26 (Confidentiality), 27 (Transparency and FOIA), 42 (Entire Agreement), 43 (Third Party Rights), 44 (Disputes) and 45 (Governing Law and Jurisdiction) and Schedule 1 (Definitions) and without limitation to the foregoing any other provisions of this Contract which are expressly or by implication intended to continue.

23. BUSINESS CONTINUITY, DISASTER RECOVERY AND INCIDENT MANAGEMENT

23.1 The Supplier shall have adequate business continuity, disaster recovery and incident management policies and procedures in place to ensure:

23.1.1 continuity of the processes and operations supported by the Services following any failure or disruption of any element of the Services (including where caused by an Insolvency Event of the Supplier, any Sub-contractor and/or any Supplier group member); and

23.1.2 the recovery of the Services in the event of the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable;

23.1.3 it can comply with the incident management requirements set out in Schedule 3 (Cyber Security and Information Governance).

23.2 Within not less than thirty (30) days of the Effective Date, the Supplier shall provide the Authority with a copy of its current business continuity and disaster recover policies ("**Current BCDR Policies**"). The Supplier shall review and update the Current BCDR Policies (and the risk analysis on which it is based) on a regular basis and as a minimum once every 12 months and provide the Authority with copies of such updated policies upon request.

23.3 The Supplier shall ensure that it (and any Sub-contractor and/or any Supplier group member providing any part of the Services) complies with its obligations: (i) set out in the Current BCDR Policies as updated from time to time in accordance with Clause 23.2; and (ii) in respect of the incident management requirements set out in Schedule 3 (Cyber Security and Information Governance).

24. EXIT MANAGEMENT

24.1 The Supplier shall be responsible for preparing and maintaining a detailed Exit Management Plan. The Supplier shall provide a draft Exit Management Plan to the Authority not later than ninety (90) days after the Effective Date.

24.2 The draft Exit Management Plan submitted in accordance with Clause 24.1:

24.2.1 must contain information at the level of detail necessary to manage the exit management stage effectively; and

24.2.2 it shall take account of all dependencies on the Authority or any other third party known to, or which should reasonably be known to, the Supplier.

24.3 The Supplier shall provide each of the items identified in the Exit Management Plan by the date assigned to that item in the Exit Management Plan.

Reviewing and changing the Exit Management Plan:

24.4 Subject to Clause 24.3, the Supplier shall keep the Exit Management Plan under review and ensure that it is updated on a regular basis.

24.5 The Authority shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Exit Management Plan.

Compliance with the Exit Management Plan:

24.6 Each Party shall comply with its respective obligations as set out in the Exit Management Plan.

25. SUB-CONTRACTING

25.1 The Supplier may sub-contract its obligations under this Contract from time to time provided that any proposed Sub-Contractor is included in the list of Key Sub-Contractors set out in Schedule 15 (Key Sub-Contractors). The Supplier shall, prior to sub-contracting, notify the Authority in writing of the Key Sub-Contractor including relevant details as required by the Authority and ensure the Key Sub-Contractor has been duly registered. The Supplier shall not sub-contract any aspect of the Services to a subcontractor, other than a Key Sub-Contractor, without the Authority's prior written consent.

25.2 The Supplier shall remain responsible for all acts and omissions of its sub-contractors (including all Key Sub-Contractors) and the acts and omissions of those employed or engaged by the sub-contractors (including all Key Sub-Contractors) as if they were its own.

26. CONFIDENTIALITY

26.1 For the purposes of this Clause 26, the term **"Disclosing Party"** shall mean a Party which discloses or makes available directly or indirectly its Confidential Information and **"Recipient"** shall mean the Party which receives or obtains directly or indirectly Confidential Information.

26.2 Except to the extent set out in this Clause 26 or where disclosure is expressly permitted elsewhere in this Contract, the Recipient shall:

26.2.1 treat the Disclosing Party's Confidential Information as confidential and keep it in secure custody (which is appropriate depending upon the form in which such materials are stored and the nature of the Confidential Information contained in those materials); and

26.2.2 not disclose the Disclosing Party's Confidential Information to any other person except as expressly set out in this Contract or without obtaining the owner's prior written consent;

26.2.3 not use or exploit the Disclosing Party's Confidential Information in any way except for the purposes anticipated under this Contract; and

26.2.4 without undue delay and within 72 hours of becoming aware notify the Disclosing Party if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Disclosing Party's Confidential Information.

26.3 The Recipient shall be entitled to disclose the Confidential Information of the Disclosing Party where:

26.3.1 the Recipient is required to disclose the Confidential Information by Law;

26.3.2 the need for such disclosure arises out of or in connection with:

(a) any legal challenge or potential legal challenge against the Authority arising out of or in connection with this Contract;

(b) the purpose of the examination and certification of the Authority's accounts (provided that the disclosure is made on a confidential basis) or for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority is making use of any Services provided under this Contract; or

(c) the conduct of a relevant Central Government Body review in respect of this Contract;

26.3.3 the Recipient has reasonable grounds to believe that the Disclosing Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010 and the disclosure is being made to the Serious Fraud Office.

26.4 If the Recipient is required by Law to make a disclosure of Confidential Information, the Recipient shall as soon as reasonably practicable and to the extent permitted by Law notify the Disclosing Party of the full circumstances of the required disclosure including the relevant Law and/or regulatory body requiring such disclosure and the Confidential Information to which such disclosure would apply.

26.5 Subject to Clauses 26.2 and 26.3, the Supplier may only disclose the Authority's Confidential Information on a confidential basis to:

26.5.1 Supplier Personnel who are directly involved in the provision of the Services and need to know the Confidential Information to enable the performance of the Supplier's obligations under this Contract; and

26.5.2 its professional advisers for the purposes of obtaining advice in relation to this Contract.

26.6 Where the Supplier discloses Confidential Information of the Authority pursuant to this Clause 26, it shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.

26.7 The Authority may disclose the Confidential Information of the Supplier:

26.7.1 To any Central Government Body for any proper purpose of the Authority or of the relevant Central Government Body on the basis that the information may only be further disclosed to Central Government Bodies and other Contracting Bodies to the extent reasonably necessary;

26.7.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

26.7.3 to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

26.7.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by the Authority for any purpose relating to or connected with this Contract;

26.7.5 on a confidential basis for the purpose of the exercise of its rights under this Contract; or

26.7.6 to a proposed transferee, assignee or novatee of, or successor in title to the Authority

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this Clause 26.

26.8 For the avoidance of doubt the Charges are Commercially Sensitive Information and categorised as the Supplier's Confidential Information.

26.9 In the event of a breach by the Supplier of any of the applicable provisions of this Clause 26, the Authority reserves the right to terminate this Contract for material Default.

26.10 Transparency Information is not Confidential Information.

27. TRANSPARENCY AND FOIA

27.1 The Supplier must tell the Authority within 48 hours if it receives a Request For Information.

27.2 Within the required timescales the Supplier must give the Authority full co-operation and information needed so the Authority can:

27.2.1 publish the Transparency Information;

27.2.2 comply with any FOIA request; and

27.2.3 comply with any EIR request.

27.3 The Authority may talk to the Supplier to help it decide whether to publish information under this Clause 27. However, the extent, content and format of the disclosure is the Authority's decision, which does not need to be reasonable.

28. CONTRACT GOVERNANCE

28.1 The Parties shall comply with the provisions of Schedule 9 (Reporting & Governance) in relation to the management and governance of this Contract.

Representatives

28.2 Each Party shall have a representative for the duration of this Contract who shall have the authority to act on behalf of their respective Party on the matters set out in, or in connection with, this Contract.

28.3 The initial Supplier Representative shall be the person named as such in Schedule 9 (Reporting and Governance) and shall be classed as Key Personnel. Any change to the Supplier Representative shall be agreed in accordance with Clause 31 (Supplier Personnel).

28.4 The Authority shall notify the Supplier of the identity of the initial Authority Representative within 5 Working Days of the Effective Date. The Authority may, by written notice to the Supplier, revoke or amend the authority of the Authority Representative or appoint a new Authority Representative.

29. COLLABORATIVE BEHAVIOUR

29.1 Without prejudice to any of the other requirements in this Contract, as part of the Services, the Supplier shall work appropriately with the Authority's other suppliers

engaged as part of the Programme ("**Collaborative Suppliers**"). The Supplier agrees to comply with the following principles of collaborative behaviour at all times:

29.1.1 form and conduct collaborative partnerships with the Collaborative Suppliers in accordance with Good Industry Practice in order to help fulfil (so far as reasonably possible) each Collaborative Supplier's respective obligations to the Supplier;

29.1.2 to work with the Collaborative Suppliers to mitigate any operational friction and ineffectiveness and support the use, when possible, common tooling as well as common reference documents;

29.1.3 to take a collaborative approach to knowledge and skills sharing benefiting the Programme as a whole;

29.1.4 to actively participate in reasonable collaborative governance processes with the Collaborative Suppliers including without limitation, attending weekly, or on request by the Authority, governance meetings with the Collaborative Suppliers and contribute to joint reports with the Collaborative Suppliers for those governance meetings; and

29.1.5 to work with the Collaborative Suppliers to mitigate the effect of any service issue and to assist so that the other Collaborative Supplier is able to solve such service issue as expeditiously and cost effectively as possible with minimal service disruption to the Programme.

29.2 The Supplier shall comply with its Social Value Obligations.

30. DIGITAL & DATA ACADEMY

Each Party shall comply with its respective obligations as set out in Schedule 16 (Digital & Data Academy).

31. SUPPLIER PERSONNEL

31.1 The Supplier shall:

31.1.1 provide in advance of any admission to Authority Premises a list of the names of all Supplier Personnel requiring such admission, specifying the capacity in which they require admission and giving such other particulars as the Authority may reasonably require;

31.1.2 ensure that all Supplier Personnel:

(i) are appropriately qualified, trained and experienced to provide the Services with all reasonable skill, care and diligence;

(ii) are vetted in accordance with Good Industry Practice and, where applicable, the security requirements set out in Schedule 3 (Cyber Security and Information Governance); and

31.1.3 comply with all reasonable requirements of the Authority and Authority Users concerning conduct at the Authority Premises, including the security

requirements as set out in Schedule 3 (Cyber Security and Information Governance);

31.1.4 retain overall control of the Supplier Personnel at all times so that the Supplier Personnel shall not be deemed to be employees, agents or contractors of the Authority;

31.1.5 be liable at all times for all acts or omissions of Supplier Personnel, so that any act or omission of a member of any Supplier Personnel which results in a Default under this Contract shall be a Default by the Supplier;

31.1.6 use all reasonable endeavours to minimise the number of changes in Supplier Personnel;

31.1.7 replace (temporarily or permanently, as appropriate) any Supplier Personnel as soon as practicable if any Supplier Personnel have been removed or are unavailable for any reason whatsoever;

31.1.8 bear the programme familiarisation and other costs associated with any replacement of any Supplier Personnel; and

31.1.9 procure that the Supplier Personnel shall vacate the Authority Premises immediately upon the termination or expiry of this Contract.

31.2 If the Authority reasonably believes that any of the Supplier Personnel are unsuitable to undertake work in respect of this Contract, it may:

31.2.1 refuse admission to the relevant person(s) to the Authority Premises; and/or

31.2.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s).

Key Personnel:

31.3 The Supplier shall ensure that the Key Personnel fulfil the Key Roles at all times during the Term. Schedule 14 (Key Personnel) lists the Key Roles and names of the persons who the Supplier shall appoint to fill those Key Roles at the Effective Date.

31.4 The Authority may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Personnel.

31.5 The Supplier shall not remove or replace any Key Personnel (including when carrying out Exit Management) unless:

31.5.1 requested to do so by the Authority;

31.5.2 the person concerned resigns, retires or dies or is on maternity leave, paternity leave or shared parental leave or long-term sick leave;

31.5.3 the person's employment or contractual arrangement with the Supplier or a Sub-contractor is terminated for material breach of contract by the employee; or

31.5.4 the Supplier obtains the Authority's prior written consent (such consent not to be unreasonably withheld or delayed).

31.6 The Supplier shall:

31.6.1 notify the Authority promptly of the absence of any Key Personnel (other than for short-term sickness or holidays of 2 weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

31.6.2 ensure that any Key Role is not vacant for any longer than 10 Working Days;

31.6.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Personnel and, except in the cases of death, unexpected ill health or a material breach of the Key Personnel's employment contract, this will mean at least 60 Working Days' notice;

31.6.4 ensure that all arrangements for planned changes in Key Personnel provide adequate periods during which incoming and outgoing personnel work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services; and

31.6.5 ensure that any replacement for a Key Role:

(i) has a level of qualifications and experience appropriate to the relevant Key Role; and

(ii) is fully competent to carry out the tasks assigned to the Key Personnel whom he or she has replaced.

32. FORCE MAJEURE

32.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Contract to the extent that such delay or failure is a result of a Force Majeure event.

32.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Contract.

32.3 Each Party will use all reasonable endeavours to continue to perform its obligations under this Contract and to mitigate the effects of Force Majeure.

32.4 If a Force Majeure event prevents a Party from performing its obligations under this Contract for more than twenty (20) Working Days, the other Party may terminate this Contract with immediate effect by written notice.

33. WAIVER

33.1 The rights and remedies under this Contract may be waived only by notice and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Contract or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

33.2 Unless otherwise provided in this Contract, rights and remedies under this Contract are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

34. SEVERANCE

34.1 If any provision of this Contract (or part of any provision) is held to be void or otherwise unenforceable by any court of competent jurisdiction, such provision (or part) shall to the extent necessary to ensure that the remaining provisions of this Contract are not void or unenforceable be deemed to be deleted and the validity and/or enforceability of the remaining provisions of this Contract shall not be affected.

34.2 In the event that any deemed deletion under Clause 34.1 is so fundamental as to prevent the accomplishment of the purpose of this Contract or materially alters the balance of risks and rewards in this Contract, either Party may give notice to the other Party requiring the Parties to commence good faith negotiations to amend this Contract so that, as amended, it is valid and enforceable, preserves the balance of risks and rewards in this Contract and, to the extent that is reasonably possible, achieves the Parties' original commercial intention.

34.3 If the Parties are unable to agree on the revisions to this Contract within 5 Working Days of the date of the notice given pursuant to Clause 34.2, the matter shall be dealt with in accordance with Paragraph 4 (Commercial Negotiation) of Schedule 10 (Dispute Resolution Procedure) except that if the representatives are unable to resolve the dispute within 30 Working Days of the matter being referred to them, this Contract shall automatically terminate with immediate effect. The costs of termination incurred by the Parties shall lie where they fall if this Contract is terminated pursuant to this Clause 34.3.

35. RELATIONSHIP OF THE PARTIES

Except as expressly provided otherwise in this Contract, nothing in this Contract, nor any actions taken by the Parties pursuant to this Contract, shall create a partnership, joint venture or relationship of employer and employee or principal and agent between the Parties, or authorise either Party to make representations or enter into any commitments for or on behalf of any other Party.

36. PREVENTING FRAUD BRIBERY AND CORRUPTION

36.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Supplier Personnel, have at any time prior to the Effective Date:

36.1.1 committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or

36.1.2 been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act.

36.2 The Supplier shall not during the Term:

36.2.1 commit a Prohibited Act; and/or

36.2.2 do or suffer anything to be done which would cause the Authority or any of the Authority's employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

36.3 The Supplier shall during the Term:

36.3.1 establish, maintain and enforce, and require that its Sub-contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

36.3.2 have in place reasonable prevention measures (as defined in sections 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

36.3.3 keep appropriate records of its compliance with its obligations under Clause 36.3.1 and make such records available to the Authority on request; and

36.3.4 take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with Section 47 of the Criminal Finances Act 2017.

36.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of Clause 36.1 and/or 36.2, or has reason to believe that it has or any of the Supplier Personnel have:

36.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

36.4.2 been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

36.4.3 received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Contract or otherwise suspects that any person or Party directly or indirectly connected with this Contract has committed or attempted to commit a Prohibited Act.

36.5 If the Supplier makes a notification to the Authority pursuant to Clause 36.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to audit any books, records and/or any other relevant documentation.

36.6 If the Supplier is in Default under Clauses 36.1 and/or 36.2, the Authority may by notice:

36.6.1 require the Supplier to remove from performance of this Contract any Supplier Personnel whose acts or omissions have caused the Default; or

36.6.2 immediately terminate this Contract.

36.7 Any notice served by the Authority under Clause 36.6 shall specify the nature of the Prohibited Act, the identity of the Party who the Authority believes has committed the Prohibited Act and the action that the Authority has elected to take (including, where relevant, the date on which this Contract shall terminate).

37. COMPLIANCE

Health and Safety:

37.1 The Supplier shall perform its obligations under this Contract (including those in relation to the Services) in accordance with:

37.1.1 all applicable Law regarding health and safety; and

37.1.2 the Health and Safety Policy whilst at the Authority Premises.

37.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority Premises of which it becomes aware and which relate to or arise in connection with the performance of this Contract. The Supplier shall instruct the Supplier Personnel to adopt any necessary associated safety measures in order to manage any such material health and safety hazards.

Equality and Diversity:

37.3 The Supplier shall:

37.3.1 perform its obligations under this Contract (including those in relation to the Services) in accordance with:

(d) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy, maternity or otherwise);

(e) the Authority's or any Authority User's equality and diversity policy as provided to the Supplier from time to time;

(f) any other requirements and instructions which the Authority or any Authority User reasonably imposes in connection with any equality obligations imposed on the Authority or any Authority User at any time under applicable equality Law; and

37.3.2 take all necessary steps, and inform the Authority and the Authority Users of the steps taken, to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission or (any successor organisation).

Official Secrets Act and Finance Act:

37.4 The Supplier shall comply with the provisions of:

37.4.1 the Official Secrets Acts 1911 to 1989; and

37.4.2 section 182 of the Finance Act 1989.

Conflicts of Interest:

37.5 The Supplier:

37.5.1 must take action to ensure that neither the Supplier nor the Supplier Personnel are placed in the position of an actual, potential or perceived Conflict of Interest.

37.5.2 must promptly notify and provide details to the Authority if an actual, potential or perceived Conflict of Interest happens or is expected to happen.

37.6 The Authority will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Authority, such measures do not or will not resolve an actual or potential Conflict of Interest, the Authority may terminate this Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest.

Modern Slavery:

37.7 The Supplier:

37.7.1 shall not use, nor allow its sub-contractors to use forced, bonded or involuntary prison labour;

37.7.2 shall not require any Supplier Personnel or the personnel of any sub-contractors to lodge deposits or identity papers with their employer and shall be free to leave their employer after reasonable notice;

37.7.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

37.7.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world;

37.7.5 shall make reasonable enquires to ensure that its officers, employees and sub-contractors have not been convicted of slavery or human trafficking offences anywhere around the world;

37.7.6 shall have and maintain throughout the Term its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and include in its contracts with its sub-contractors anti-slavery and human trafficking provisions;

37.7.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under this Contract;

37.7.8 shall prepare and deliver to the Authority, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business (or a copy of a report under section 54 of the Modern Slavery Act 2015);

37.7.9 shall not use, nor allow its employees or sub-contractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or sub-contractors;

37.7.10 shall not use or allow child or slave labour to be used by its sub-contractors; and

37.7.11 shall report the discovery or suspicion of any slavery or trafficking by it or its sub-contractors to the Authority and the Modern Slavery Helpline.

37.8 If the Supplier notifies the Authority pursuant to Clause 37.10 it shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to audit any books, records and/or any other relevant documentation in accordance with this Contract.

37.9 If the Supplier is in Default under Clause 37.7 the Authority may by notice:

37.9.1 require the Supplier to remove from performance of this Contract any Sub-Contractor, Supplier Personnel or other persons associated with it whose acts or omissions have caused the Default; or

37.9.2 immediately terminate this Contract.

Whistleblowing:

37.10 As soon as it is aware of it the Supplier and Supplier Personnel must report to the Authority any actual or suspected breach of:

37.10.1 Law;

37.10.2 Clauses 37.1 to 37.7 or 37.11; or

37.10.3 Clause 36.

37.11 The Supplier must not retaliate against any of the Supplier Personnel who in good faith reports a breach listed in this Clause to the Authority or a Prescribed Person.

38. ASSIGNMENT

38.1 The Supplier shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Contract without the prior written consent of the Authority.

38.2 The Authority may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Contract and/or any associated licences to:

38.2.1 any NHS Body; or

38.2.2 to a body other than a NHS Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority,

and the Supplier shall, at the Authority's request, enter into a novation agreement in such form as the Authority shall reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 38.2.

38.3 A change in the legal status of the Authority such that it ceases to be a NHS Body shall not affect the validity of this Contract and this Contract shall be binding on any successor body to the Authority.

39. VARIATION

39.1 Subject to the process outlined in Clauses 5.12 to 5.16 (Modifications to the Services), either Party can request any variation to the Contract or a Service Request Form (as detailed in Schedule 12 of the Contract), (the "**Variation**") which is only effective if agreed in writing and signed by both Parties.

39.2 The Supplier must provide an Impact Assessment either:

39.2.1 with the Variation Form, where the Supplier requests the Variation; or

39.2.2 within the time limits included in a Variation Form requested by the Authority.

39.3 If the Variation cannot be agreed or resolved by the Parties, the Authority can either:

39.3.1 agree that the Contract or Service Request Form, as the case may be, continues without the Variation; or

39.3.2 refer the failure to agree or resolve the Variation as a Dispute to be resolved using the Dispute Resolution Procedure.

39.4 The Authority is not required to accept a Variation request made by the Supplier.

39.5 For the purposes of regulation 101(5) of the Regulations, if the court declares any Variation ineffective, the Parties agree that their mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

39.6 In this clause:

Impact Assessment means an assessment of the impact of a Variation request completed in good faith, including:

a) details of the impact of the proposed Variation on the Services, Deliverable Items and the Supplier's ability to meet its other obligations under the Contract;

b) details of the cost of implementing the proposed Variation;

c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;

d) a timetable for the implementation, together with any proposals for the testing of the Variation; and

e) such other information as the Authority may reasonably request in (or in response to) the Variation request; and

Variation Form means the form set out in Schedule 18 (Variation Form).

40. NOTICES

40.1 Any notices sent under this Contract must be in writing.

40.2 The following table sets out the method by which notices may be served under this Contract and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending.	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

40.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Contract:

	Supplier	Authority
Contact	[Redacted under FOIA s40, personal information]	[Redacted under FOIA s40, personal information]
Address	[Redacted under FOIA s40, personal information]	[Redacted under FOIA s40, personal information]
Email	[Redacted under FOIA s40, personal information]	[Redacted under FOIA s40, personal information]

40.4 Failure to send any original notice by personal delivery or recorded delivery in accordance with this Clause 40 shall invalidate the service of the related e-mail transmission. The deemed time of delivery of such notice shall be the deemed time of delivery of the original notice sent by personal delivery or Royal Mail Signed For™ 1st

Class delivery (as set out in the table in Clause 40.2) or, if earlier, the time of response or acknowledgement by the other Party to the email attaching the notice.

40.5 This Clause 40 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution (other than the service of a Dispute Notice under Schedule 10 (Dispute Resolution Procedure)).

41. FURTHER ASSURANCES

Each Party undertakes at the request of the other, and at the cost of the requesting Party to do all acts and execute all documents which may be reasonably necessary to give effect to the meaning of this Contract.

42. ENTIRE AGREEMENT

42.1 This Contract constitutes the entire agreement between the Parties in respect of its subject matter and supersedes and extinguishes all prior negotiations, arrangements, understanding, course of dealings or agreements made between the Parties in relation to its subject matter, whether written or oral.

42.2 Neither Party has been given, nor entered into this Contract in reliance on, any warranty, statement, promise or representation other than those expressly set out in this Contract.

42.3 Nothing in this Clause 42 shall exclude any liability in respect of misrepresentations made fraudulently.

43. THIRD PARTY RIGHTS

43.1 The Supplier acknowledges that the Authority enters into this Contract for its own benefit and for the benefit of each Authority User and the Supplier shall perform its obligations under this Contract for the benefit of the Authority and such Authority Users. Accordingly, a number of the provisions in this Contract confer benefits on Authority Users and/or other persons named or identified in such provisions (together "**Third Party Provisions**") other than the Parties (each such person a "**Third Party Beneficiary**") and are intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

43.2 Subject to Clause 43.1, a person who is not a Party to this Contract has no right under the CRTPA to enforce any term of this Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

43.3 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Authority, which may, if given, be given on and subject to such terms as the Authority may determine.

43.4 Any amendments or modifications to this Contract may be made, and any rights created under Clause 43.1 may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

44. DISPUTES

44.1 The Parties shall resolve Disputes arising out of or in connection with this Contract in accordance with the Dispute Resolution Procedure.

44.2 The Supplier shall continue to provide the Services in accordance with the terms of this Contract until a Dispute has been resolved.

45. GOVERNING LAW AND JURISDICTION

45.1 This Contract and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

45.2 Subject to Clause 44 (Disputes) and Schedule 10 (Dispute Resolution Procedure) (including the Authority's right to refer the dispute to arbitration), the Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Contract or its subject matter or formation.

SIGNATURE PAGE

This Agreement has been duly executed by the Parties on the date which appears at the head of its page 1.

SIGNED for and on behalf of IQVIA LTD. by a director:	)	
	)	
	)	[SIGNATURE]

SIGNED for and on behalf of **NHS ENGLAND**	)	
	)	
	)	[SIGNATURE]

SCHEDULE 1

DEFINITIONS

1. In accordance with Clause 1 (Definitions), in this Contract the following expressions shall have the meanings ascribed in the table below.

Academy Working Group	has the meaning given to it in Paragraph 2.1 of Schedule 16 (Digital & Data Academy);
Achieve	means in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the provisions of Schedule 7 (Milestones), and **"Achieved"** and **"Achievement"** shall be construed accordingly;
Additional Terms	has the meaning given in Clause 3.3;
Affiliate	means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
Applicable Supplier Terms	has the meaning given in Clause 3.1;
Associated Person	has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017;
Authority Authorised Representative	means the person identified as such in Schedule 9 (Reporting and Governance) as at the Effective Date or as subsequently changed by the Authority from time to time;
Authority Cause	any material breach by the Authority of any responsibilities of the Authority agreed in writing between the Parties from time to time in connection with this Contract, except to the extent that such breach is: a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or b) caused by the Supplier, any Sub-Contractor or any Supplier Personnel;
Authority Content	means the data (together with any databases) including any Personal Data, content, materials, information and software which are controlled, uploaded or otherwise transferred by or on behalf of the Authority to the relevant environments hosted by or on behalf of the Supplier pursuant to the Services including any derivative data that is generated in the relevant environments but excluding metadata where and to the extent such metadata: a) is generated by the Supplier's Services under this Contract solely for administrative and/or service maintenance purposes; b) is not under the control of the Authority; and c) does not contain any Personal Data;

Authority Data	means: a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Authority or an Authority User; and/or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or b) any Personal Data for which the Authority or any Authority User is the Controller;
Authority Premises	means premises owned, controlled or occupied by the Authority, any Authority User and/or any NHS Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them);
Authority's Existing Entitlement	means the Authority's funds held on account by the Supplier in respect of another transaction(s) outside of this Contract and to be used as part or whole payment of the Charges;
Authority User	means any NHS Body receiving the Services and "**Authority Users**" shall mean all of them;
Beneficiary	means a person having (or claiming to have) the benefit of an indemnity or a right to be defended (as applicable) under this Contract;
Central Government Body	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
Change of Control	means any change of Control of the Supplier or a Parent Undertaking of the Supplier;
Charges	means the charges payable to the Supplier by the Authority under this Contract in respect of the Services, calculated in accordance with this Contract and as set out or referred to in Schedule 5 (Charges & Invoicing);
Claim	means any claim which it appears that a Beneficiary is, or may become, entitled to indemnification or a right to be defended (as applicable) under this Contract;
Collaborative Suppliers	has the meaning given in Clause 29.1;
Commencement Date	means the date on which Interim Milestone 1B (as set out in Schedule 7 (Milestones)) is Achieved;
Commercially Sensitive Information	means commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if

	disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
Confidential Information	means the Authority's confidential information and/or the Supplier's confidential information, as the context requires;
Conflict of Interest	a conflict between the financial or personal duties of the Supplier or the Supplier's staff and the duties owed to the Authority under this Contract, in the reasonable opinion of the Authority;
Configuration Services	has the meaning given to it in Clause 5.10;
Contract	means the contract between the Authority and the Supplier consisting of: a) these Terms; b) the Schedules to these Terms;
Contract Year	means a period of twelve (12) consecutive months commencing on the Commencement Date or each anniversary thereof and the period between the last such 12 month period and the last day of the Term;
Control	means control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
Controller	has the meaning given to it in the UK GDPR;
Critical KPI	means those Key Performance Indicators indicated as "Critical KPIs" in Annex 1 of Schedule 8 (Performance Levels);
Critical Performance Failure	[Redacted under FOIA s43, Commercial interests]
CRM Personal Data	has the meaning given in Clause 17.14;
CRTPA	means the Contracts (Rights of Third Parties) Act 1999;
Current BCDR Policies	has the meaning given in Clause 23.2;
Data Loss Event	means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
Data Processing Agreement or **DPA**	means the terms and conditions for data processing as set out in Schedule 11 (Data Processing Agreement) or entered into in accordance with a MOU;
Data Protection Impact Assessment	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
Data Protection Legislation	means: (i) the UK GDPR; (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy;
Data Protection Officer	has the meaning given to it in the UK GDPR;
Data Subject	has the meaning given to it in the UK GDPR;

Data Subject Request	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
Default	means any breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) or any other default, act, omission, misrepresentation, negligence or negligent statement of the Supplier or its personnel in connection with or in relation to this Contract or the subject matter of this Contract and in respect of which the Supplier is liable to the Authority;
Delay	means a delay in the Achievement of a Key Milestone (including any interim milestone forming part of such Key Milestone) by its Milestone Date;
Delay Payment Rate	has the meaning given to it in Part C of Schedule 5 (Charges & Invoicing);
Delay Payments	means the amounts payable by the Supplier to the Authority in respect of a Delay in Achieving a Key Milestone as specified in Schedule 7 (Milestones);
Delay Payments Cap	has the meaning given to it in Part C of Schedule 5 (Charges & Invoicing);
Deliverable Item	means an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Contract as set out in the Implementation Plan;
Digital Suppliers	has the meaning given to it in Paragraph 1.1.1 of Schedule 16 (Digital & Data Academy);
Dispute	means any claim, dispute or difference arises out of or in connection with this Contract (whether contractual or non contractual) or in connection with the negotiation, existence, legal validity, enforceability or termination of this Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
Dispute Notice	means a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
Dispute Resolution Procedure	means the dispute resolution procedure set out in Schedule 10 (*Dispute Resolution Procedure*);
DPA 2018	means the Data Protection Act 2018;
EIR	the Environmental Information Regulations 2004;
Effective Date	means 22 November 2023;
Electronic Invoice	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
Exit Management Plan	means an exit management plan prepared in accordance with Clause 24 (Exit Management);
Extension Period	refers to the First Extension Period, the Second Extension Period, or the Third Extension Period, as the case may be (as those terms are defined in Clause 4.2);

Federated Data Platform	means the Federated Data Platform (FDP) software that will sit across NHS trusts and integrated care systems allowing them to connect data they already hold in a secure and safe environment;
FOIA	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
Force Majeure	means any event, occurrence, circumstance, matter or cause affecting the performance by either Party of its obligations arising from: a) acts, events, omissions, happening or non-happenings beyond the reasonable control of the affected Party which prevent or materially delay the affected Party from performing its obligations under this Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of government, local government or regulatory bodies; d) fire, flood or disaster and any failure or shortage of power or fuel; or e) industrial dispute affecting a third party for which a substitute third party is not reasonably available. The following do not constitute a Force Majeure event: (i) any industrial dispute relating to the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain; (ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure; (iii) any failure of delay caused by a lack of funds; (iv) the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Contract was entered into; or (v) any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans;
Good Industry Practice	means standards, practices, methods and procedures conforming to the Law and the exercise of the 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 within the relevant industry or business sector;
Government	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
Health and Safety Policy	means the health and safety policy of the Authority, an Authority User and/or other relevant NHS Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that

	cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
Implementation Plan	means the draft implementation plan as set out in Schedule 6 (Implementation Plan) as amended in accordance with Clause 6 (Implementation & Milestones);
Initial Term	means the period beginning on the Effective Date and ending on the third anniversary of the Commencement Date;
Insolvency Event	means, in respect of the Supplier: a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or b) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or c) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or e) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or g) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or h) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or i) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;
Intellectual Property Rights or **IPR**	means: a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights having equivalent or similar effect in any country or jurisdiction;

IPR Claim	means any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority in the fulfilment of its obligations under this Contract;
Key Milestone	means a Milestone designated as a "Key Milestone" in Schedule 7 (Milestones);
Key Performance Indicator	means the Critical KPIs and Standard KPIs set out in Annex 1 of Schedule 8 (*Performance Levels*);
Key Personnel	means the Supplier Personnel identified as "Key Personnel" in Schedule 14 (Key Personnel) (if any);
Key Role	means the roles to be performed by the Key Personnel as set out in Schedule 14 (Key Personnel) (if any);
Key Sub-Contractor	means a Sub-Contractor which performs a critical role in the provision of all or part of the Services;
KPI Effective Date	means the date from which performance monitoring begins in respect of each KPI on Achieving the Milestone set out against that KPI in Schedule 8 (Performance Levels);
KPI Failure	means a failure to meet the Target Performance Level in respect of a Key Performance Indicator;
KPI Service Threshold	shall be as set out against the relevant Key Performance Indicator in Annex 1 of Schedule 8 (Performance Levels);
Law	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;
Losses or Loss	means all losses, liabilities, damages, costs, fines, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise;
Malicious Software	means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
Material KPI Failure	means: a) a Serious KPI Failure; b) a Severe KPI Failure; or c) a failure by the Supplier to meet a KPI Service Threshold;
Maximum Term	means a period of seven (7) years from the Commencement Date;

Measurement Period	means in relation to a Key Performance Indicator, the period over which the Supplier's performance is measured (for example, a Service Period if measured monthly or a 12 month period if measured annually);
Milestone	means an event or task described in Schedule 7 (Milestones);
Milestone Achievement Certificate	means the certificate to be granted by the Authority when the Supplier has Achieved a Milestone;
Milestone Date	means the date set out against the relevant Milestone in Schedule 7 (Milestones);
Milestone Payment	means the amount set out in Schedule 7 (Milestone Payments) to be paid by the Authority to the Supplier on the Supplier Achieving each Milestone and "**Milestone Payments**" shall be construed accordingly;
MoU	means a memorandum of understanding between the Authority and an Authority User substantially in the form set out in Schedule 19 (Authority Users);
NHS Body	means a health service body within the meaning of section 275 of the National Health Service Act 2006;
Notifiable Default	shall have the meaning given in Clause 18.1(*Rectification Plan Process*);
Other Data Platforms	means those data platforms forming part of the Programme from time to time other than the Federated Data Platform;
Parent Undertaking	has the meaning set out in section 1162 of the Companies Act 2006;
Party	means a party to this Contract, namely either the Authority or the Supplier (together the "**Parties**");
Performance Monitoring Report	has the meaning given to it in Part B of Schedule 8 (Performance Levels);
Personal Data	has the meaning given to it in the UK GDPR;
Personal Data Breach	has the meaning given to it in the UK GDPR;
Prescribed Person	a legal adviser, an MP, or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies—2/whistleblowing-list-of-prescribed-people-and-bodies, as updated from time to time;
Processing	has the meaning given to it in the UK GDPR and "**Process**" and "**Processed**" shall be interpreted accordingly;
Processor	has the meaning given to it in the UK GDPR;
Programme	means the implementation of new data platforms and/or the maintenance of existing data platforms (including but not limited to the Federated Data Platform), by the Authority and NHS Bodies, to understand patterns, solve problems, plan services for local populations and ultimately transform the health and care of the people the Authority and NHS Bodies serve;

Programme Board	means the body described in Paragraph 4 of Schedule 9 (Reporting and Governance);
Prohibited Acts	means: a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or d) defrauding, attempting to defraud or conspiring to defraud the Authority or other public body; or e) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
Protective Measures	means 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 the Supplier including those set out or referred to in Schedule 11 (Data Processing Agreement);
Provider	means a Party from whom an indemnity or a right to be defended (as applicable) is sought under this Contract;
Rectification Plan Failure	means: a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 18.4 (Submission of the draft Rectification Plan) or 18.8 (Agreement of the Rectification Plan); b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 18.7 (Agreement of the Rectification Plan); c) the Supplier failing to rectify a material Default within the later of: i) 30 Working Days of a notification made pursuant to Clause 18.2 (Notification); and ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date

	specified in the Rectification Plan by which the Supplier must rectify the material Default; d) a Material KPI Failure re-occurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any of the 3 Measurement Periods subsequent to the Measurement Period in which the initial Material KPI Failure occurred; e) the Supplier not Achieving a Milestone by the relevant Milestone Date; and/or f) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of 6 months for the same (or substantially the same) root cause as that of the original Notifiable Default;
Rectification Plan	means a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default;
Rectification Plan Process	means the process set out in Clauses 18.4 (Submission of the draft Rectification Plan) to 18.9 (Agreement of the Rectification Plan);
Regulations	means the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
Relevant Requirements	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
Relief Notice	has the meaning given to it in Clause 19.2;
Replacement Services	means such services as the Authority may seek to procure to replace the Services;
Representative	means in respect of a Party its representative from time to time appointed further to Clause 28;
Request for Information	means a request for information or an apparent request relating to this Contract or an apparent request for such information under the FOIA or the EIRs;
Restricted Country	means any country other than: a) a member of the European Economic Area; b) the United Kingdom; or c) deemed adequate by article 45(3) of the UK GDPR;
Schedule of Processing	means a schedule describing processing, personal data and data subjects set out in (or in the form set out in) Schedule 11 (Data Processing Agreement) or annexed to a DPA;
Security Assessment Documents	has the meaning given in Clause 14.6.4;
Security Audit	has the meaning given in Clause 14.6;
Serious KPI Failure	shall be as set out against the relevant Key Performance Indicator in Annex 1 of Schedule 8 (Performance Levels);
Service Charges	means all Charges other than Milestone Payments;

Service Credit Cap	has the meaning given in Clause 9.3.3 (Financial and other limits);
Service Credits	means credits payable by the Supplier due to the occurrence of 1 or more Critical KPI Failures, calculated in accordance with Schedule 8 (Performance Levels);
Service Description	means the description of the Services as set out or referred to in Schedule 2 (Service Description);
Service Modification	has the meaning given in Clause 5.13;
Service Level Agreement or SLA	means the Supplier's relevant service level terms and conditions which apply to a particular service product provided as part of the Services under this Contract, as set out or referred to in Schedule 4 (Supplier Solution);
Service Period	means a calendar month, save that: a) the first service period shall begin on the first KPI Effective Date and shall expire at the end of the calendar month in which the first KPI Effective Date falls; and b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
Service Points	means in relation to a KPI Failure, the points that are set out against the relevant Critical KPIs in Annex 1 of Schedule 8 (Performance Levels);
Service Request	means a request for Services submitted by the Authority for itself and/or on behalf of any NHS Body in accordance with the procedure for requesting Configuration Services set out in Schedule 12 (Service Request Procedure);
Services	means the services which the Supplier shall make available to the Authority and Authority Users under this Contract as set out or referred to in Schedule 2 (Service Description) and Schedule 4 (Supplier Solution);
Severe KPI Failure	shall be as set out against the relevant Key Performance Indicator in Schedule 8 (Performance Levels);
Social Value Obligations	means the social value commitments made by the Supplier in the Supplier Solution;
Standard KPIs	means those Key Performance Indicators indicated as "Standard KPIs in Annex 1 of Schedule 8 (Performance Levels);
Standards	means any standards set out or referred to in this Contract and Schedule 3 (Cyber Security and Information Governance);
Standard Contractual Clauses	means the standard contractual clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of protection as set out in Commission Decision C (2010) 593 and reference to the standard contractual clauses shall be to the clauses as updated, amended, replaced or superseded from time to time by the European Commission;
Sub-Contract	means any contract or agreement or proposed agreement between the Supplier and any third party whereby that third party agrees to provide to the Supplier the Services (or any part thereof) or to provide facilities or services necessary for the provision of the Services (or any part thereof) or

	necessary for the management, direction or control of the provision of the Services or any part thereof;
Sub-Contractor	means any third party engaged by the Supplier from time to time under a Sub-Contract;
Sub-processor	means any third party appointed as at the Effective Date (and any additional third party appointed strictly in accordance with Clause 17.11) to process Personal Data on behalf of the Supplier related to this Contract as recorded in the Supplier's Register, including those Key Sub-Contractors identified as a sub-processor;
Supplier Non-Performance	has the meaning given to it in Clause 19.1;
Supplier Personnel	means all persons employed or engaged by the Supplier together with the Supplier's servants, agents, suppliers, consultants and Sub-Contractors (and all persons employed by any Sub-Contractor together with the Sub-Contractor's servants, consultants, agents, suppliers and sub-contractors) used in the performance of its obligations under this Contract;
Supplier Solution	the Supplier's solution for the Services set out in Schedule 4 (Supplier Solution), including any Annexes to that Schedule;
Supplier Termination Event	means: (a) the Supplier's level of performance constituting a Critical Performance Failure; (b) a Rectification Plan Failure; (c) failure to Achieve a Key Milestone by its Milestone Date; (d) a Change of Control of the Supplier unless: (i) the Authority has given its prior written consent to the particular Change of Control, which subsequently takes place as proposed; or (ii) the Authority has not served its notice of objection within 6 months of the later of the date on which the Change of Control took place or the date on which the Authority was given notice of the Change of Control; (e) a change of Control of a Key Sub-contractor unless, within 6 months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant contract with the Key Sub-contractor and replaces it with a comparable Key Sub-contractor which is approved by the Authority; (f) the occurrence of an Insolvency Event; or (g) the Supplier acquires Control of the third party supplier providing the Federated Data Platform;
Supplier's Register	means the register of Key Sub-Contractors and Sub-processors described in Clause 15.1 effective as of the Effective Date and as updated from time to time by the Supplier in accordance with this Contract and made available to the Authority upon request;
Target Performance Level	means the minimum level of performance for a Key Performance Indicator which is required by the Authority, as set out against the relevant Key Performance Indicator in Schedule 8 (Performance Levels);

Term	means the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Contract;
Terms	means these terms and conditions excluding the Schedules;
Third Party Beneficiary	has the meaning given in Clause 43.1 (*Third Party Rights*);
Third Party Provisions	has the meaning given in Clause 43.1 (*Third Party Rights*);
Transparency Information	means the transparency reports (including information relating to the Services and performance of this Contract which the Supplier is required to provide to the Authority in accordance with Schedule 9 (Reporting and Governance)) and the content of this Contract, including any changes to this Contract agreed from time to time, except for: a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Authority; and b) Commercially Sensitive Information;
Urgent Service Modification	has the meaning given in Clause 5.14;
UK GDPR	has the meaning given to it in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019;
Variation	has the meaning given to it in Clause 39.1;
VAT	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
Working Day	means any day other than a Saturday, Sunday or public holiday in England and Wales.

SCHEDULE 2

SERVICE DESCRIPTION

NHS Privacy Enhancing Technology (NHS-PET)

Schedule 2, Appendix 2A: Technical Specification

Name of Contracting Authority	**NHS England**
Procurement for	**NHS - Privacy Enhancing Technology (NHS-PET)**
Project reference	**C177577**
Find a Tender Service Contract Notice reference	**FTS-007743**
Date of Publication	**21 June 2023**
Tender Submission Response Deadline	**26 July 2023**

Contents

1 Scope

1.1 What is “NHS Privacy Enhancing Technology” (NHS-PET)?

We are committed to keeping patient information safe and being transparent about how it is used. NHS Privacy Enhancing Technology (NHS-PET) must provide cohesive protection and deliver a standard mechanism to support safe data use including data privacy treatments and ensuring appropriate data access.

A Data Controller is the organisation with legal ownership and responsibility for a specific set of personal identifiable data. Where that Data Controller wishes to share elements of that data with another party, controls are required to ensure that it is only available to those with an approved purpose and that de-identification required for that purpose is applied. The Data Controller, as owner, determines the controls that are required to maintain and ensure privacy. The level of de-identification applied to data may vary based on user roles and requirements for accessing the data. This is in line with Information Commissioner’s Office guidance. NHS-PET is the component in the overall architecture that must implement both those controls and the de-identification.

NHS-PET will be used across NHS, in conjunction with various data platforms, including FDP-AS, which will be the first use case, but also other data platforms in use within NHS. As such, many of the use cases below will refer to FDP-AS, but the NHS-PET capability will be applied in similar ways to other data platforms.

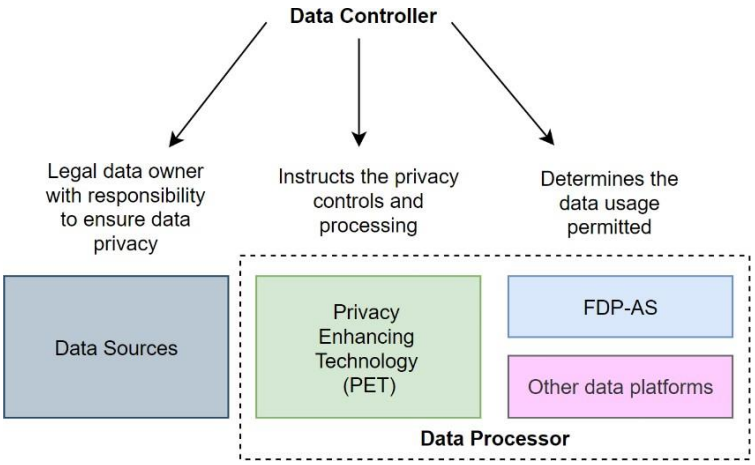


Figure 1 - Data Responsibilities

The NHS-PET solution will need to protect data without compromising the functionality of the underlying data platforms (e.g., FDP-AS), and the modes of interaction between NHS-PET and data platforms are described in the following sections. It is critical that NHS-PET is flexible enough to handle both traditional data protection scenarios, as well as being extensible to new and emerging data trends (e.g., homomorphic encryption, secure multi-party computation, zero-trust proofs).

1.2 High Level Scope

The NHS-PET solution will ensure a clear and transparent process for applying controls to data, to ensure that data is used safely and lawfully across appropriate parts of the NHS. The NHS-PET platform will deliver key capabilities: classification, protection, audit & management in support of secondary and direct-care use-cases across the range of data platforms and FDP-AS tenancies.

The high-level scope can be summarised as:

a) NHS-PET applies controls to datasets protecting NHS data elements to support the use of data by individuals and organisations with a legitimate need to process data.

b) Provides a control point for NHS datasets as they are transferred between source systems to data platforms (including FDP-AS), and between FDP-AS tenants.

c) Applies privacy controls as mandated by the relevant Data Controller to ensure that data can be made available to the correct systems as and when is required, for a legitimate purpose.

d) Audits the movement and treatment of NHS data in support of enterprise-wide, end-to-end auditing. Audit logs are made available to enterprise-wide tooling for collation and advanced analysis.

e) Provides a catalogue of data assets and associated data controls.

f) Offers automated discovery techniques to identify PII and PID attributes in processed datasets (such as special category data elements).

g) Provides an administration console for configuration and management tasks including registering datasets, managing existing datasets, setting privacy policies, and applying privacy controls.

A DPIA process, overseen by the Data Controller, determines the access restrictions required for a given dataset. Access control rules will be associated with processed datasets for implementation by the data platform in question (e.g., a receiving FDP-AS tenant). The FDP-AS, or other data-consuming platform, is responsible for use-case specific data modelling, lineage and applying auditable access level controls.

1.3 System Context

The NHS-PET system exists within the wider data platforms ecosystem (including FDP-AS). NHS-PET provides a data privacy and control point for data ingress to and egress from data platforms, and between those data platforms and associated products and services which consume the treated data.

Data platforms (including the FDP-AS solution) will ingest data via NHS-PET from local and National systems. NHS-PET will process data to apply deidentification privacy mechanisms including anonymisation, pseudonymisation and/or re-identification. It will treat ingress data in transit to ensure a high level of privacy as the data enters data platforms. NHS-PET will implement the governance and privacy controls agreed in advance of any use of data. NHS-PET will be a separate concern from data platforms such as FDP-AS to enhance data governance and enable the long-term ambition to become an enterprise-wide solution for data privacy for the NHS.

The diagram below describes at a high level the scope of planned procurements to support the FDP ecosystem, and wider data platform ecosystem.

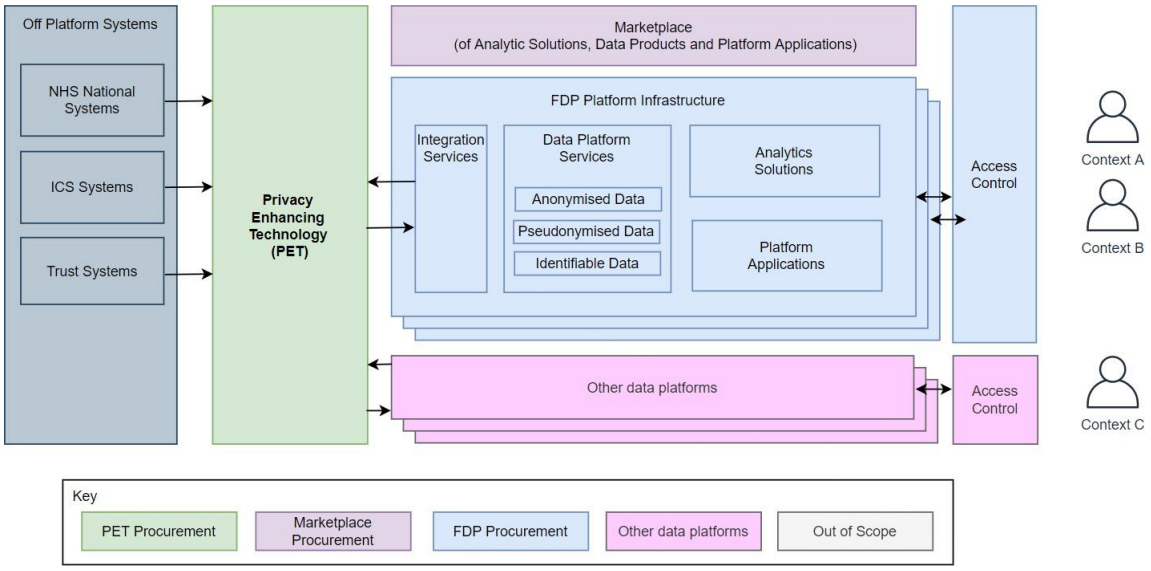


Figure 2 - Ecosystem Components

1.4 Interdependencies of the FDP Programme

For the purpose of this document, interdependencies between the NHS-PET Procurement, FDP-AS and Marketplace are used for illustrative purposes only. Participants should ensure their solution is designed around open standards to support future integration requirements as defined in these separate contracts.

1.5 Wider Ecosystem Components

The diagram above describes the key components which make up the FDP Programme and wider ecosystem.

In addition to NHS-PET the other major components in the Programme architecture include:

1. **Off-Platform Systems:** existing and future applications, data warehouses and data platforms used by the ecosystems of NHS organisations and providers to run their day-to-day healthcare operations. Unlike Platform Applications, Off-Platform Systems are not hosted on the FDP-AS infrastructure and will not be in the future.
2. **FDP-AS - Platform Infrastructure:** an elastically scalable infrastructure capability that will host the Data Platform, Analytical Solutions and Platform Applications.
3. **FDP-AS - Data Platform Services:** the core data platform which will process structured, semi-structured (e.g., JSON), unstructured (e.g., PDF), and binary data (e.g., Images). It will host the data models, data engineering pipelines, data privacy workflows and orchestration.

4. **FDP-AS - Integration Services:** components to support ingress and egress of data in a secure and adaptable way. The solution must support queue-based messaging services that support different policies according to the type of data to ensure appropriate processing and protect data from loss.
5. **FDP-AS - Analytics Solutions:** solutions built upon the Data Platform fulfilling analytics and reporting use cases.
6. **FDP-AS - Platform Applications:** solutions built upon the Data Platform fulfilling operational business use cases.
7. **Marketplace**: a discrete solution for the publishing, sharing, discovery and download of curated FDP solutions. The Marketplace is intended to promote innovation, collaboration, and efficiency, while encouraging adoption and openness of the FDP itself.
8. **Other Data Platforms:** other data platforms which will process structured and semi-structured (e.g., JSON) data. These will host their own data models, data engineering pipelines, data privacy workflows and orchestration.

1.6 FDP-AS Data Platform Multi-tenancy

Data is expected to be held by the FDP-AS in discrete logical ‘Tenancies’. A Tenancy is a means of providing a partition to support a separate set of access controls and potentially separate ownership. The FDP-AS can be considered a collection of discrete Tenants with data being passed from the Data Controllers’ (e.g., Trust) Tenants to ICS/ICB and National level Tenants through strict controls under the explicit instruction of the relevant Data Controller.

In some cases, Local Tenants will use the FDP-AS to process patient identifiable data for direct care. These have enhanced levels of privacy applied to them as a condition of data moving out of the Local Tenant and into National Tenants. There are also expected to be Tenants at the ICS/ICB organisation level which may deliver direct care or coordination of care. National Tenants will serve national use cases and will typically have much higher volumes of data that are anonymised, pseudonymised, aggregated and are outside the scope of UK GDPR / DPA 2018.

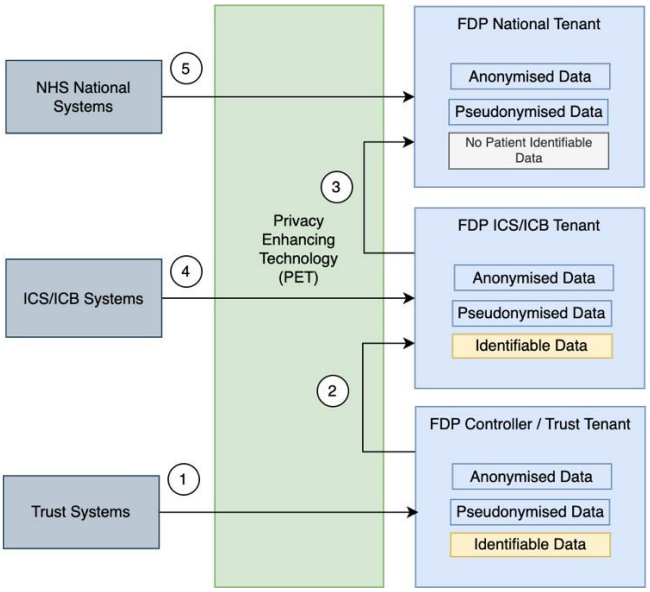


Figure 3 – FDP Multi-Tenancy Model

1. Trust Data is processed by NHS-PET and privacy controls are applied and is made available to the local Tenant, in this case a Trust. Both identifiable and deidentified data will be provided to FDP-AS.
2. Data is processed at a Trust Tenant level and provided for use at an ICS/ICB level again via NHS-PET which may reapply or add further privacy controls. The ICS/ICB Tenant requires non-identifiable data for secondary care-use cases and potentially will also require patient identifiable data in support of direct care use-cases.
3. Data may be aggregated and provided for use within the National tenant and is again re-processed via NHS-PET, which may reapply or add further privacy controls.
4. Non-trust patient data will be processed by NHS-PET and is consumed by ICS/ICB Tenants.
5. Data from NHS systems is privacy processed at source and will route via NHS-PET which provides an audit point and consistency of data ingress into FDP-AS.

2 Appendix C – NHS Standards and PracticesConceptual Model

2.1 Integration Patterns

Interoperability between NHS-PET and data platforms (e.g., FDP-AS) is a critical requirement and NHS-PET must support the following interactions with platforms for data processing under the explicit instruction of the relevant Data Controller.

- To pass treated data to a data platform.
- To be called by data platform to invoke a defined data privacy treatment on specified data.
- To be called by data platform to reidentify and reinsert sensitive data into treated data.

Integration services must support the secure transfer of data to and from NHS-PET. Data will be transported in batch, micro-batch and streaming modes and will primary be structured and semi-structured data.

The platform must be able to support multiple integration patterns, including but not limited to the following examples.

2.1.1 Runtime NHS-PET

Data is transferred to the destination data platform, where it is securely stored. NHS-PET full differential privacy control treatments based on specific usage purposes and contexts are configured for that dataset, but the data is stored in cleartext. At query run time, based on the purpose and access context, the privacy controls are applied to the return dataset. This model can be used to provide privacy protection at access time.

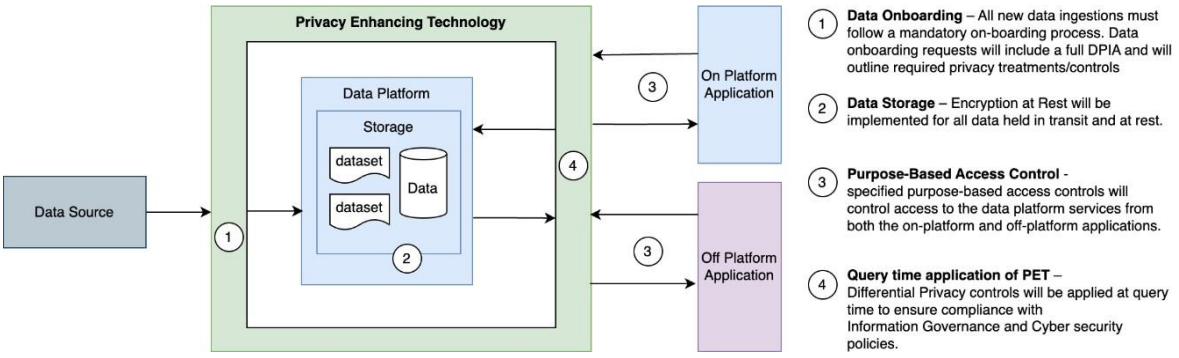


Figure 4 – Runtime NHS-PET

1. Data source adds data to the platform storage. All new ingestions must follow a mandatory onboarding process, which includes a full DPIA and specification of the privacy treatments for each purpose and access context.
2. Data is securely stored.
3. Specified purpose-based privacy controls will control access to the data.

4. On query time, the specified purpose-based privacy controls are applied, and the privacy-treated dataset is returned.

Crucially, this pattern must fail-closed i.e., in the case that the privacy treatment fails or cannot be matched, the data is not returned to the query.

This pattern has the benefit of reducing the number of privacy-treated copies of data which need to be stored, and reduces burden associated with processes such as key-rotation.

2.1.2 NHS-PET as a Data Interface

Data is transferred to the destination data platform via NHS-PET.

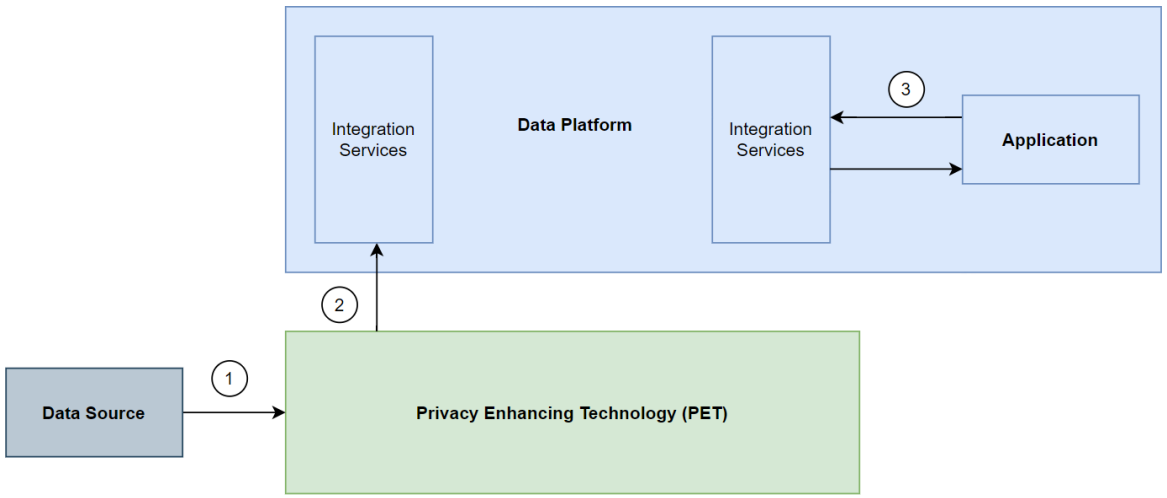


Figure 5 - NHS-PET as a Data Interface

1. The data source sends a dataset to NHS-PET for privacy treatment purposes and onward routing to the data platform. NHS-PET validates the data against a predefined metadata specification, applies any required privacy treatments and audits the data flow.
2. NHS-PET makes the treated dataset available to the destination data platform, which consumes and models the dataset.
3. Applications query the data platform and results are returned according to the access controls implemented by the data platform.

2.1.3 NHS-PET as a Service

Data sources retain responsibility for data orchestration and privacy treatment.

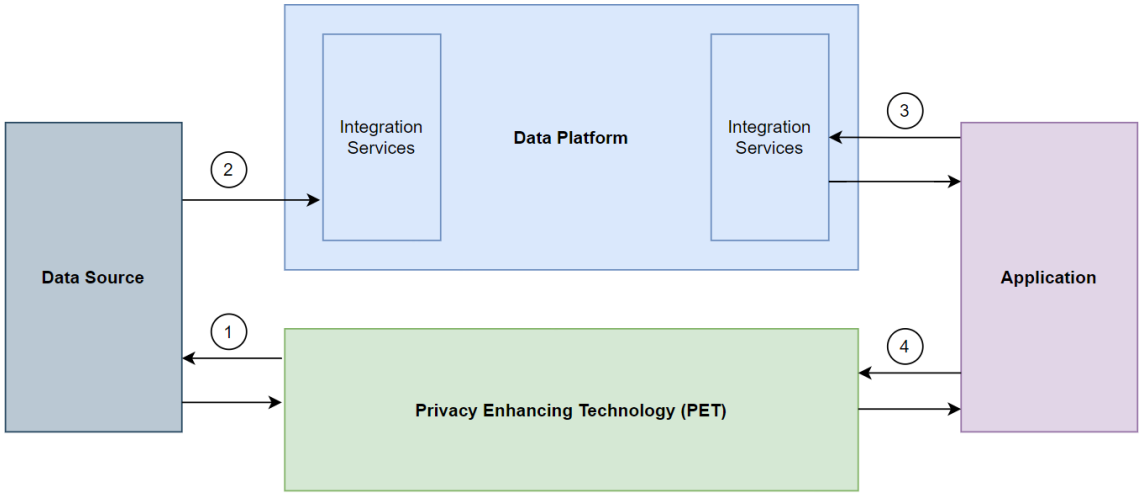


Figure 6 - NHS-PET as a Service

1. The data source sends a data set to NHS-PET for privacy treatment purposes. NHS-PET audits the receipt of the data, validates it against the metadata specification, and applies any privacy treatments.
2. Once NHS-PET has processed the data set it is made available to the source system. The source system maintains responsibility for onward orchestration and makes the data to the intended destination data platform.
3. Applications query the data platform and results are returned according to the access controls implemented by the data platform.
4. Applications may have a requirement to re-identify data, subject to information governance controls. In this circumstance the application would send the result to NHS-PET for re-identification. NHS-PET authorises the request and return the re-identified results back to the application.

This pattern describes some FDP-AS inter-tenant transfers, and re-identification use-cases.

2.1.4 Hidden NHS-PET

A data orchestration component of the target data platform is responsible for receiving a dataset from the data source and processing prior to inclusion in the data model. The data platform orchestration tool is responsible for routing the data via NHS-PET prior to onboarding into the data model. This model can be used to provide privacy protection at access time and provide to provide transparent re-identification of data.

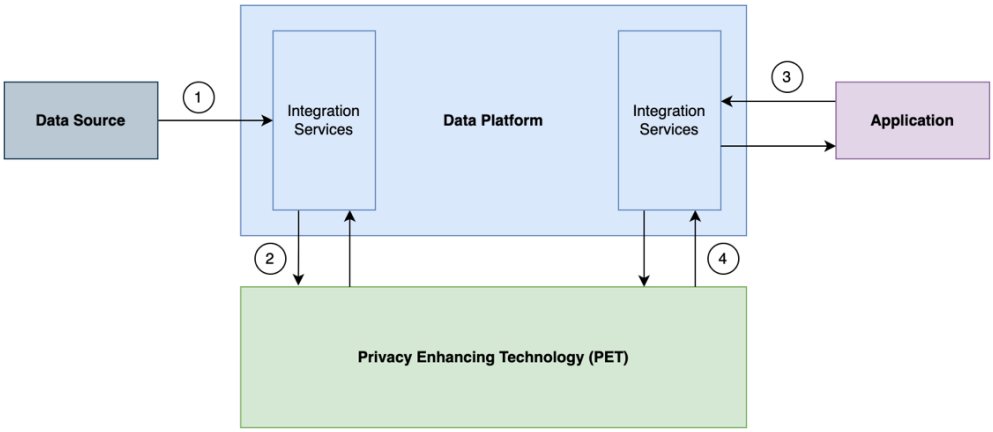


Figure 7 - Hidden NHS-PET

1. The data source sends data to the data platform integration services component. The data is routed to NHS-PET for privacy treatment.
2. The NHS-PET solution audits the receipt of the data, validates it against the metadata specification, and applies any privacy treatments and makes the data available for the data platform.
3. Applications query the data platform and results are returned according to the access controls implemented by the data platform.
4. Where applications have a requirement to re-identify data, the data platform will proxy the request to NHS-PET for reidentification. NHS-PET authorises the request and returns the re-identified results back to the data platform, subject to IG and access controls, which then returns to the application.

2.2 FDP System Logical Model

The diagram below describes the high level model illustrating the logical relationship between data sources, NHS-PET, FDP-AS and Marketplace, to highlight the specific interactions required to support inter-tenant transfers across the FDP ecosystem.

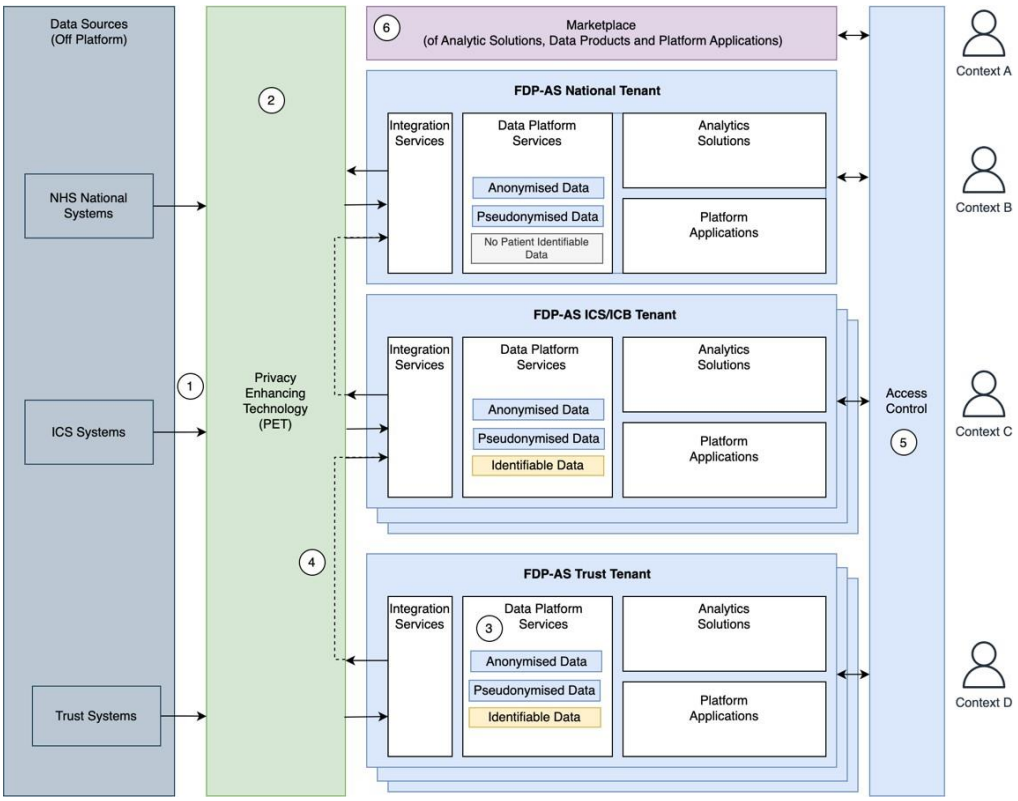


Figure 8 - Logical Model

1. NHS-PET is a standalone service (NHS-PET as a Data Interface) located logically between data sources and the FDP-AS platform providing a data orchestration and privacy service for FDP-AS data ingress and inter-tenant transfers.
2. Data treatments for example anonymisation, masking, generalisation and pseudonymisation are applied. Data is made available to be consumed by FDP-AS tenants.
3. Privacy treated data is modelled by FDP-AS and is made available for specific purposes.
4. Data may be shared between FDP-AS tenants for an appropriate need. These data flows are routed via NHS-PET which provides an audit point and may be required to process or reprocess the data for example aggregation or re-identification.
5. FDP-AS users access the platform and are given access to the data according to their role and purpose. FDP-AS retains responsibility for applying access level controls using the access control layer.
6. Marketplace provides application use-case functionality. There is no direct integration with NHS-PET and access is governed by the FDP-AS access control layer.

2.3 High Level Component Flow

Figure 8 below describes the required high-level interactions between the key sub-components within a data platform and NHS-PET.

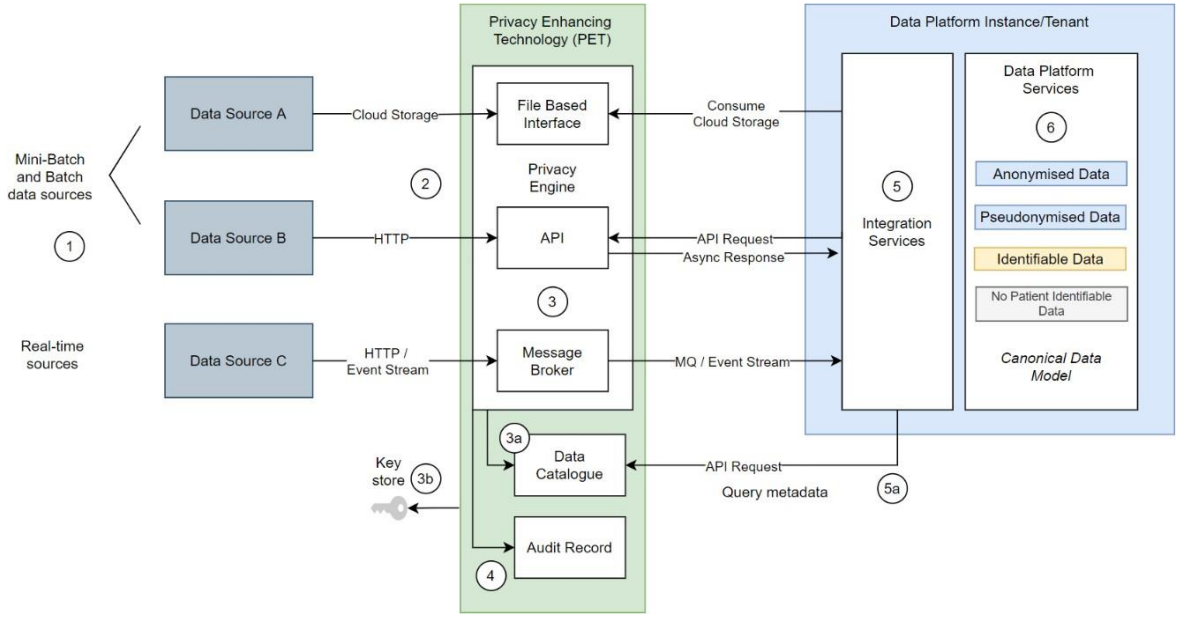


Figure 9 - Logical Data Component Flow

1. Source NHS systems typically export data using a mini-batch or batch pattern transferred using an API or file transfer protocol. Streaming data may also be provided in support of real-time or near real-time processes. Data exports will typically be structured as defined by specifications published by NHSE.
2. A range of transfer methods are required to accommodate source systems including file-based protocols, including secure file transfer, cloud storage protocols and HTTPS REST API. A queuing interface will be required to support streaming data.
3. The dataset is validated and treatments including anonymisation, masking and pseudonymisation are applied in accordance with the controls set out by the DPIA and managed by the (3a) data catalogue. Where cryptographic data treatments are performed keys may be stored and managed using an (3b) external key store.
4. Immutable audit records are created within NHS-PET to record the data flow process including data ingress, data validation, privacy processing and data egress.
5. Data is made available to be consumed by the data platform. The platform consumes the dataset and retrieves the corresponding (5a) metadata records including structure and purpose-based access controls. The data is modelled according to the metadata specification and added to a canonical data model.
6. Data is available for usage and access controls allow access to data for a given set of purposes. Access controls for a given dataset are determined by the Data Controller and are managed by the data catalogue.

2.4 Common Dataset Flows

NHS-PET will be required to support several data flows. The following examples highlight some of the common scenarios, with an emphasis on FDP use cases.

2.4.1 National Tenant Dataflow

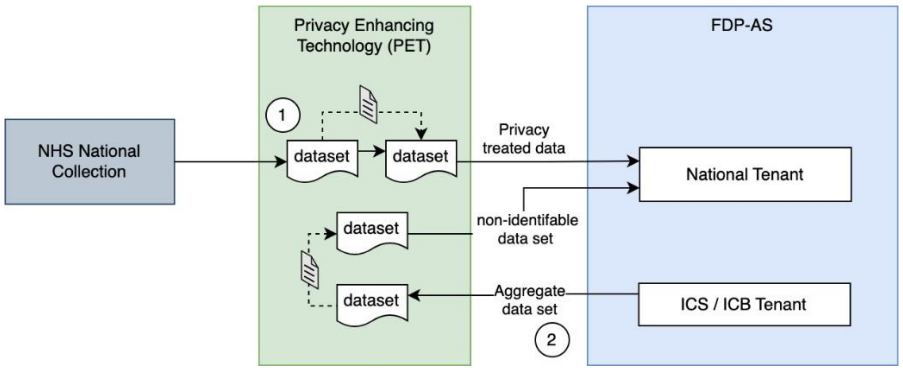


Figure 10 - National Tenant Dataflow

Data from NHS National systems (1) is routed via NHS-PET which provides an audit point for the data transfer and applies any data privacy controls. Where sufficient data privacy treatments are applied at source by the data provider NHS-PET is only required to provide an audit point. FDP-AS consumes the treated data which is modelled and made available in the national FDP-AS tenant.

Aggregated data will also be provided from the ICS/ICB tenant level into the national tenant. NHS-PET will route the data flow, audit the transfer, and process the data to make it non-identifiable. The de-identification method will use a common treatment configuration to maintain referential integrity of data allowing the joining of data sets. Note that the Runtime NHS-PET pattern may be used to support this data flow.

2.4.2 Trust Tenant Dataflow

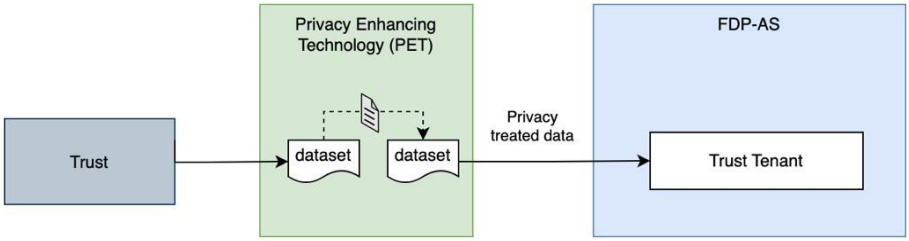


Figure 11 - Trust Tenant Dataflow

Trust data is required at both ICB/ICS and Trust tenant levels. Data at a Trust level tenant is required for the purpose of direct and secondary care use-cases and comprises both identifiable and non-identifiable data. At the ICB/ICS tenant level, it is important to support the joining of datasets across source trusts. To facilitate the joining of datasets and aggregation use-cases key identifiers, for example NHS Number, will be privacy treated using a common key or seed. Note that the Runtime NHS-PET pattern may be used to support this data flow.

2.4.3 Inter-Tenant Data Flow

Within the tenant hierarchy it is anticipated that datasets may need to exist at both the Trust tenant level and the ICS/ICB level. In this scenario the Trust dataset would be routed via NHS-PET for privacy treatment for modelling at the ICS/ICB instance level. To enable the joining of datasets at the ICS/ICB level a common treatment configuration would be used.

Any transfers would be controlled under the instruction of the relevant Data Controller. Note that the Runtime NHS-PET pattern may be used to support this data flow.

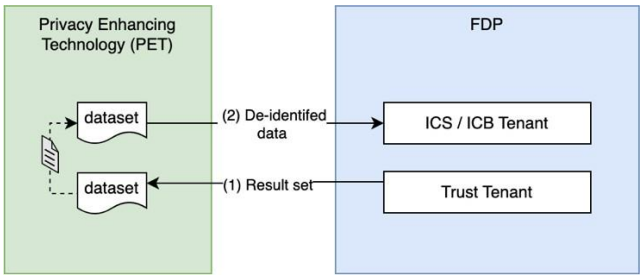


Figure 12 – Inter-Tenant Data Flow

2.4.4 Re-identification Example

Various use cases within FDP support a requirement for data to be identifiable, for example to support a care intervention. Such an intervention would be determined within FDP using de-identified data. The application would send the request to reidentify to FDP-AS which, using the Hidden NHS-PET pattern, would facilitate a re-identification request to NHS-PET.

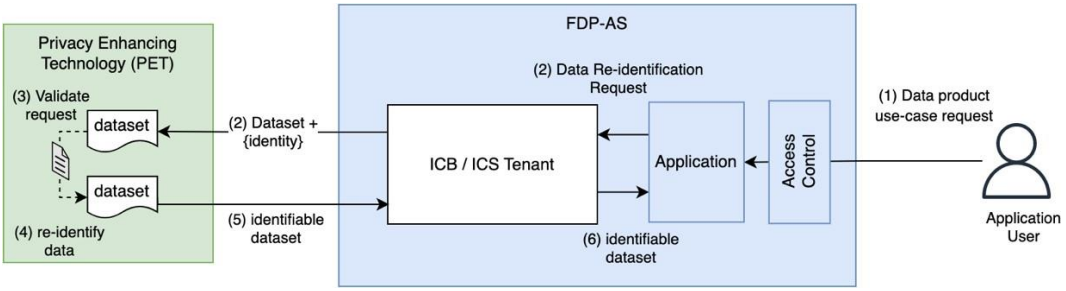


Figure 13 - Reidentification Example

3 NHS-PET Components and Capabilities

3.1 Component Services

It is anticipated that the NHS-PET solution will comprise of a NHS-PET vendor solution and supporting services as described below.

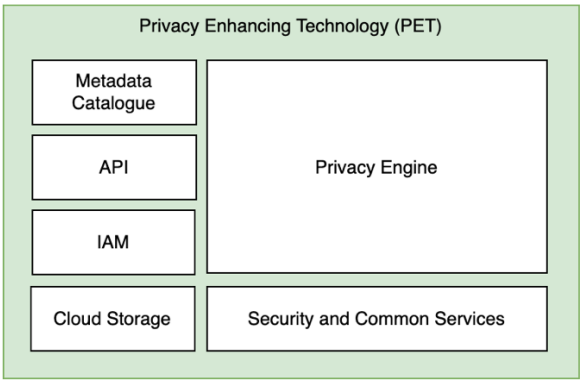


Figure 14 - NHS-PET Component Services

Metadata Catalogue – Reference database responsible for maintaining the metadata required by the NHS-PET and data consumers including FDP-AS.

Privacy Engine – Core NHS-PET technology product responsible for data orchestration, privacy data processing, rules management and audit.

API – Provide a common perimeter API service for the NHS-PET vendor product, metadata catalogue and storage capabilities.

IAM – Common service responsible for authentication and authorisation capabilities across the API, storage, and Core NHS-PET vendor platform. User access level identity management will use existing NHS identity providers such as CIS2, NHS.net AD, Azure AD or Okta.

Cloud Storage – Backing storage for the privacy engine and components.

Security and Common Services – Services required for the operational management of the platform including monitoring and alerting, operations dashboards, logging, deployment, configuration, and environment management.

3.2 Capability Model

The following capability model details the key capabilities that the NHS-PET solution should deliver. We accept that multiple technical components may be combined to fulfil these capabilities. Bidders are permitted to exceed these capabilities.

The descriptions below should be interpreted as providing structure around the requirements stated in Schedule 2, Appendix 2D – NHS-PET Requirement Catalogue.

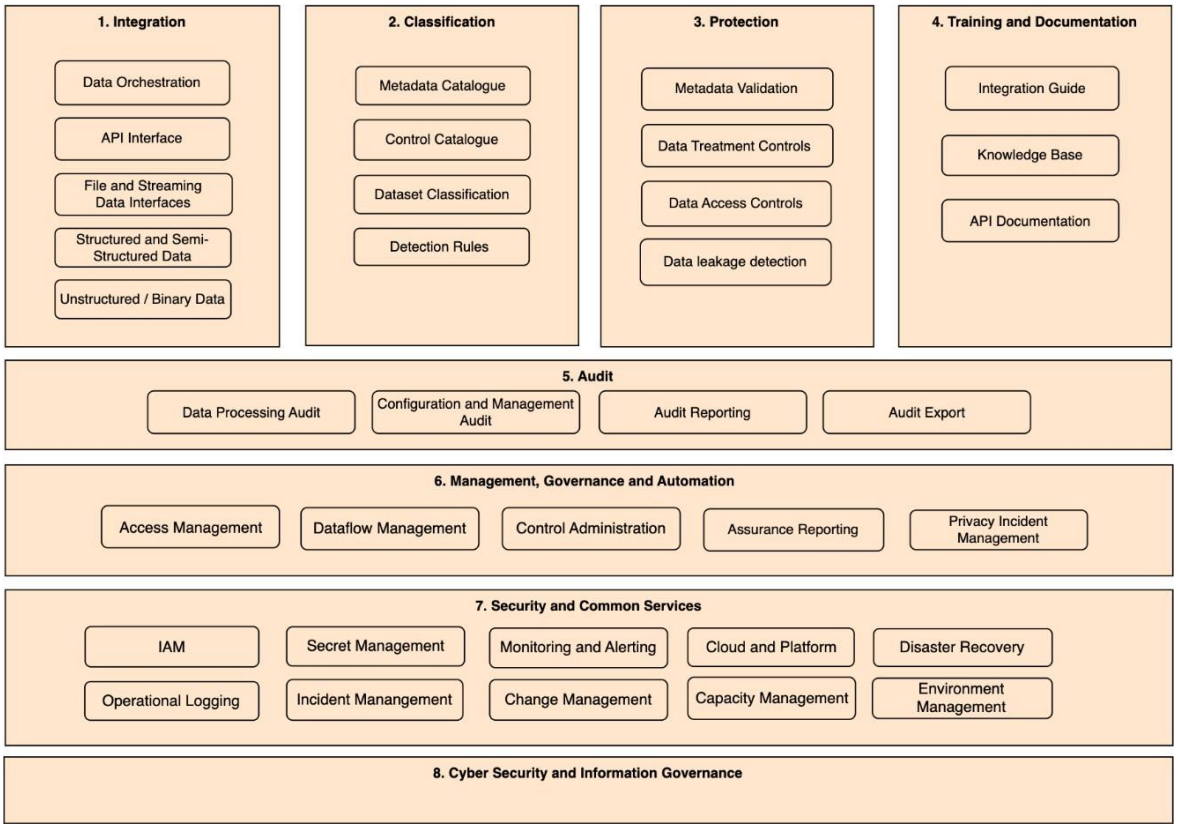


Figure 15 - NHS-PET Capability Model

3.2.1 Integration

The data integration capability is responsible for data ingress, orchestration of data processing activities and data egress for NHS-PET. The service must support common data transfer patterns and including mini-batch, batch, file transfer, REST API and streaming data. Supported technologies should include secure file transfer, cloud storage (e.g. AWS S3), HTTP API and message streaming.

To ensure security all inbound requests must be authenticated and authorised using a technique appropriate to the transfer type. As an example, secure file transfer using a pre-shared SSH key or HTTP using an OAuth client credential grant or API token. Data transfer requests are mapped to a configuration set which validates and processes the transfer as a data pipeline.

Data will be provided to NHS-PET in a variety of formats including structured, semi-structured and unstructured data. Column delimited and object formats including JSON or XML. Column delimited formats would include standard formats including CSV or custom

delimited formats. Object data may include healthcare domain specific standards including HL7 and FHIR.

Audit records must be generated at the point of ingress, privacy processing and egress. The audit should contain a reference to the data source, destination and associated configuration set to support data lineage and audit activities.

All data must be encrypted whilst it is being processed and stored at rest. Once data has been processed and delivered to or consumed by the destination data platform it should be deleted. The only enduring data should be configuration, metadata, audit, and operational records.

3.2.2 Classification

Classification capabilities refer to the process of categorising personal data based on its sensitivity or risk level. NHS-PET must include effective classification capabilities to help organisations identify and categorise personal data based on factors such as the type of data, the purpose for which it is being processed, and the potential harm that could result from its unauthorised disclosure.

The structure of inbound data will be described in the metadata catalogue and will include the data structure, types, and data privacy classification. In many cases ingress data sources for example Trust admissions will align to specifications maintained by NHS England. The catalogue will need to include support for these standardised data specifications. Refer to *Appendix B – National Dataset Specification* Example

The solution should have the ability to hold a Data Catalogue for storing an inventory of data assets. The Data Catalogue should be easily accessible, filterable, and searchable by users of the system to support a compliance and validation processes.

NHS-PET will provide a personal confidential data discovery capability to help mitigate the risk of personal confidential data leakage. The capability is required to detect divergence from the configuration profile this could include additional fields and changes to the classification of existing fields. NHS-PET will provide a standardised library of rules and classifications (e.g., telephone number, email address), as well as supporting custom definitions, provided by the Authority, which cover NHS-specific data items e.g., clinical codes.

3.2.3 Protection

The protection capability describes the validation of data against the metadata specification, the implementation of data treatment controls and personal confidential data leak detection capabilities.

Data will be validated inbound for conformance against the expected metadata configuration. Where a mapping or metadata configuration does not exist processing will cease, and an error will be raised. Where the dataset does not confirm to the expected dataset, for example unexpected fields or data type validation processing and based on the severity of the validation issue processing may cease further processing and an error raised.

The NHS-PET solution must provide standard data treatment controls including common data privacy techniques including anonymisation, pseudonymisation, hashing, tokenisation, encryption, redaction, masking, and generalisation. A catalogue of available controls will be curated and made available by the solution provider to ensure that privacy techniques are

implemented in a standard and consistent manner thereby maintaining the integrity and trust in the platform.

Data privacy techniques including encryption and hashing make use of secret keys and/or seeds. These secret keys and seeds must be protected using secure key management capabilities within. Secret management administration must be controlled to restrict access to designated administrators only.

Data access control measures will be recorded in the metadata catalogue. Controls are to be based on both the type and classification of the data attributes defined based on role or purpose. Data platforms will consume both the metadata and these access controls into its own data model.

The NHS-PET solution must provide a data lineage service tracking the processing of data as it flows through the NHS-PET service. The data lineage information is required to support a data audit and governance process and must be made available to users of the system and sharable in a user-friendly format.

Leakage detection describes the process of maintaining conformance against the privacy controls described in the metadata catalogue. NHS-PET must detect and mitigate the risk of unexpected sensitive (special category) data being introduced into data sets. It will achieve this by periodically scanning datasets and asserting against the metadata schema and data classifications. Where a discrepancy is detected, an incident should be raised to the Data Services service desk for further investigation.

3.2.4 Audit

The Audit capability is core to tracking how special category data is processed and transferred to data platforms.

The NHS-PET solution should control configuration and management activity based on the principle of least privilege. A detailed immutable audit log is required to include access to and modification of configuration items.

All audit records must contain relevant meta data including system datetime, relevant identifiers including systems, users, configuration and data flows, processing activities and modifications. In support of enterprise level reporting and correlation it must be possible to export audit records to a SIEM service.

3.2.5 Training and Documentation

The NHS-PET solution must provide NHS-PET administrators with training materials, such as user guides, integration, and API documentation to help them understand how to use and integrate with NHS-PET to comply and demonstrate compliance with data protection policies.

Integration guides will be provided by the NHS-PET provider for data providers and consumers to describe the high-level process and technical details required to integrate systems with NHS-PET. Technical documentation will be provided in support of the feature rich API capability. REST API specifications will be provided in OpenAPI v3 format.

The NHS-PET solution must provide a knowledge base providing general documentation resource describing the classification, protection and audit & management capabilities of NHS-PET. The NHS-PET solution must deliver documentation of all types as an intuitive web-based system with search and filter capabilities to allow NHS-PET users to find relevant

information. This knowledge base must be kept up to date with system features and capabilities.

3.2.6 Management, Governance and Automation

NHS-PET must incorporate effective management, governance, and automation capabilities to ensure efficient administration of the platform required to maintain the confidentiality, integrity, and availability of data.

The administration management console must implement robust role-based access controls and the tools required to configure all aspect of the solution including management accounts, incident management, ingress and egress data flows, control catalogue, metadata, privacy and access controls. An approval process may be required for a subset of administration tasks.

The NHS-PET solution must deliver governance capabilities capable of controlling and managing compliance with privacy regulations and policies. The governance component should include features such as access controls, audit logs, and real-time monitoring to detect and respond to any violations. This will include risk management and incident response procedures to manage any data breaches.

The NHS-PET solution must deliver automation capabilities to streamline data management and governance processes. Automation can help reduce the risk of human error, increase efficiency, and enable the NHS-PET to scale to meet the demands of large datasets. The automation component should include features such as machine learning algorithms to detect anomalies, intelligent workflows to automate routine tasks, and self-learning models to adapt to changing data landscapes.

The NHS-PET solution must deliver metadata management capabilities to securely store, measure, and report on metadata. Metadata is information about the data, e.g., data source, owner, destination, recipient tenant, lineage, logs.

The NHS-PET solution must deliver the capability to create dashboards and operational reports. The ability for users of the platform to build on-demand and scheduled sets of information and visualisation to be used as required. To maintain records of all data breaches, any related facts about the breaches, their consequences and all actions taken to remediate them. Records will then be reviewed by the desired authority to verify compliance.

3.2.7 Security and Common Services

The NHS-PET platform including application and infrastructure must have robust security capabilities to safeguard the platform and data held within it from insider threats, cyber-attacks, and data breaches. Application-level security controls should include access control, authentication, request validation and data encryption. NHS-PET must have appropriate security monitoring systems to detect and respond to any security threats. NHS-PET as a system must be compliant with the specification described in Schedule 2, Appendix 2B - Security Requirements.

To provide consistent and reliable services across different platforms and applications, the NHS-PET should also include features such as identity management, data validation, and error handling to ensure that the data processed by the NHS-PET is accurate and reliable. To support incident management, governance, auditing processes the logs must be stored securely such that they cannot be altered or interfered with.

Security credentials and secrets including platform credentials, seeds, cryptographic keys and must be stored and managed securely with the capability to manage (create, exchange, store, replace and destroy) cryptographic keys. There should be the ability for NHS England to manage their own cryptographic keys using an external Key Management System (KMS), backed by Hardware Security Modules (HSM). Further, the solution must support rotation of keys with low administration overhead, and support an approach for re-tokenising data with rotated keys with low impact to downstream tokenised data consumers.

To support operational concerns the platform must be provided with robust monitoring and alerting system. The monitoring system will measure system KPIs including business level metrics such as feed processing and technical indicators such as API request rates, response time and metric which indicate the health and capacity of the platform. Automated alerting should be used to notify when metrics breach key operational thresholds. The system must be designed to support an agreed set of SLAs which the monitoring system will be used to report against. Refer to *Schedule 2, Appendix 2C - Ways of Working and Service Catalogue*.

Change management provides the ability to plan and manage the schedule of releases and maintenance tasks to avoid system conflicts and track impacts. All changes must be logged, and a history of change must be kept. It must be possible to revert to historical versions of the system configuration. Release patterns and procedures should be designed to maintain availability, reduce downtime, minimise operational risk.

NHS-PET will be deployed on infrastructure and will scale elastically, and cost effectively as determined by the demand level. The solution provider will monitor cost and capacity trends proactively supporting capacity and cost optimisation. Costs should be managed on a transparent basis and include the ability to attribute costs by dimensions including data-source, tenant, use-case, and data flow.

Non-production environments and a sandbox capability will be required for the testing and assurance of features and key configuration changes prior to deployment in production.

3.2.8 Cyber Security and Information Governance

Capability which describes the Cyber Security and Information Governance requirements. Please refer to *Schedule 2, Appendix 2B – Security Requirements.*

4 Supporting Management Processes

4.1 High Level Processes

The flow diagrams below provide a summary level illustration of the key data management flows that the NHS-PET solution must implement, and are described below in the context of FDP. They include data onboarding and amendments, incident management and a Data Controller review process.

Note in these flow diagrams, a number of user personas are involved, from both the NHS-PET solution provider, the Authority, and the Data Controlling organisation.

Onboarding Coordinator – Authority staff - Coordinating role responsible for managing the data onboarding process across the data source, NHS-PET and FDP-AS.

Data Controller – Data Controlling organisation staff - Considered at an organisation level having legal responsibility for the data and data sharing agreements and DPIA process. The Data Controller is responsible for determining which data can be shared for which purpose and provides explicit instruction to data processors, NHS-PET, and FDP.

IG Lead – Data Controlling organisation staff - Represents the IG process which provide national standards and governance.

NHS-PET Administrator – NHS-PET solution provider staff - Responsible for configuring NHS-PET as expressed by the Data Controller

NHS-PET Approver – NHS-PET solution provider staff - Responsibility to peer review of any configuration changes for example data transfers and privacy processing.

4.1.1 Dataset Onboarding Process

The dataset onboarding process flow requires the interaction between a number of roles to ensure that data is integrated with FDP-AS via NHS-PET. All data processing is undertaken as explicitly instructed by the Data Controller organisation.

An Onboarding Coordinator initiates the process by submitting a request to onboard the new dataset. The Data Controller organisation has responsibility for ensuring access to the datasets is for given purposes and to also ensure that the data is de-identified and complies with privacy regulations.

An IG Lead evaluates the data sharing schedule and advises and ensures that the appropriate templated instruction for classification and application of privacy controls has been applied. Following approval, the NHS-PET administrator configures the new dataset and submits the change(s) for review.

A NHS-PET Approver role reviews the configuration change(s) against the provided instructions validating that all privacy requirements have been addressed before finally approving the dataset integration. Following the approval and publishing of the change(s) the onboarding coordinator is informed and works with the data source and FDP-AS to initiate and test the data flow.

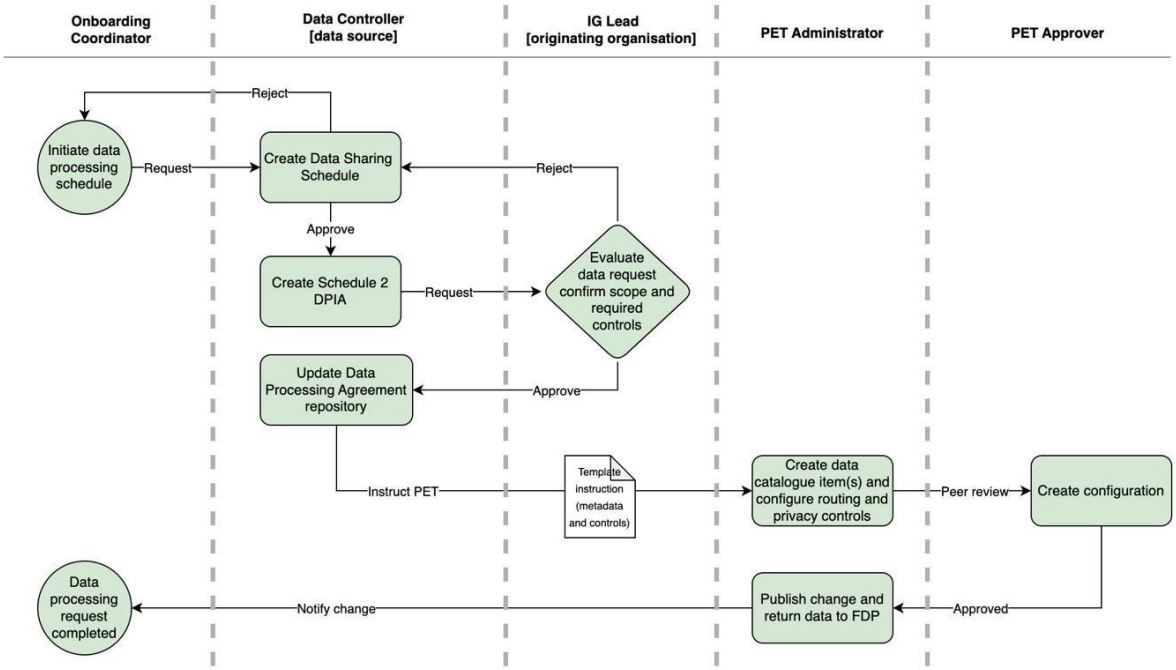


Figure 156 - Dataset Onboarding Process

4.1.2 Data Modification / Deletion Process

Responsible for managing the modification or the deletion of an existing dataset. The process includes the submission of a modification request, data evaluation, modification assessment, and data integration.

The onboarding coordinator initiates the modification request and provides a detailed description of the changes required. The data controller organisation evaluates the impact of the modification on privacy compliance, while the IG lead assesses the proposed modifications for quality and suitability and outlines any necessary changes to the data controls and instructions.

The NHS-PET administrator integrates the modified dataset into the existing model. The NHS-PET approver reviews the modifications ensuring the new privacy requirements are met. The modification process flow helps to maintain compliance with privacy regulations while allowing for modifications to the dataset to meet changing needs.

All data deletion and safe retention activities must be subject to the NHS Data Retention Schedule - refer to Appendix C – NHS Standards and Practices - Data retention policy and guidance.

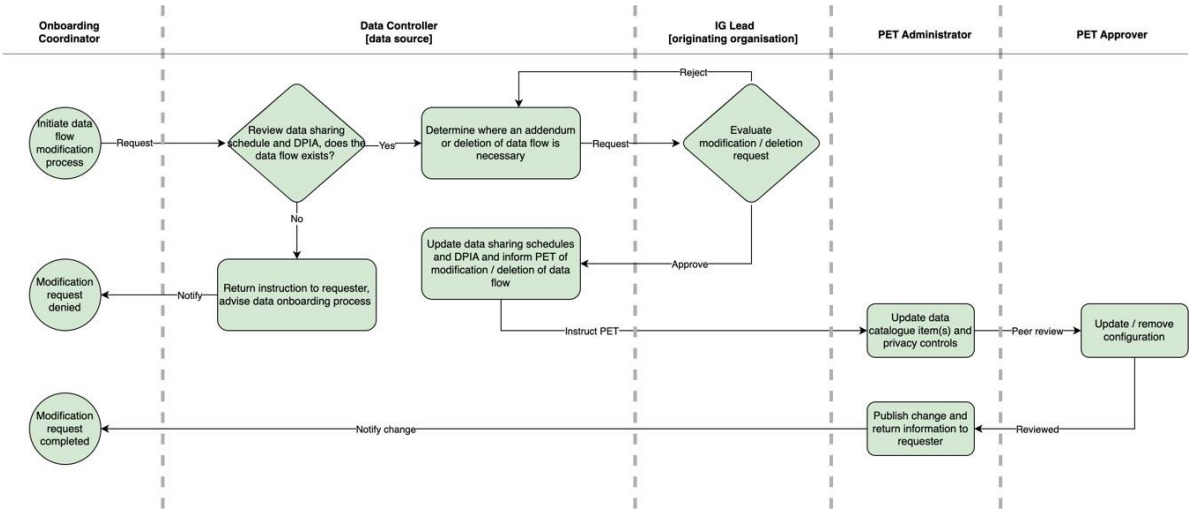


Figure 176 - Dataset Modification Process

4.1.3 Annual Review Process

The Data Controller organisation has a responsibility on a biannual basis to assess the relevance, and accuracy of datasets in the system. This ensures that the data is managed in accordance with the Data Controllers explicit instruction in a compliant and transparent manner, and only used for intended purposes.

The process includes dataset identification, data assessment, and potential configuration remediation, and is critical in identifying any potential privacy breaches and mitigating them before they occur.

The data controller is responsible for the dataset and ensuring that NHS-PET adheres to the applicable data protection laws and regulations, while the IG lead is responsible for defining and implementing the data governance policies and procedures that must be followed.

The NHS-PET administrator is responsible for ensuring that NHS-PET is configured to support the data review process, including performing data cleansing and de-identification tasks. The annual review process is an essential component of the NHS-PET operational framework that helps to maintain the trust and confidence of organisations whose personally identifiable data is being collected and processed.

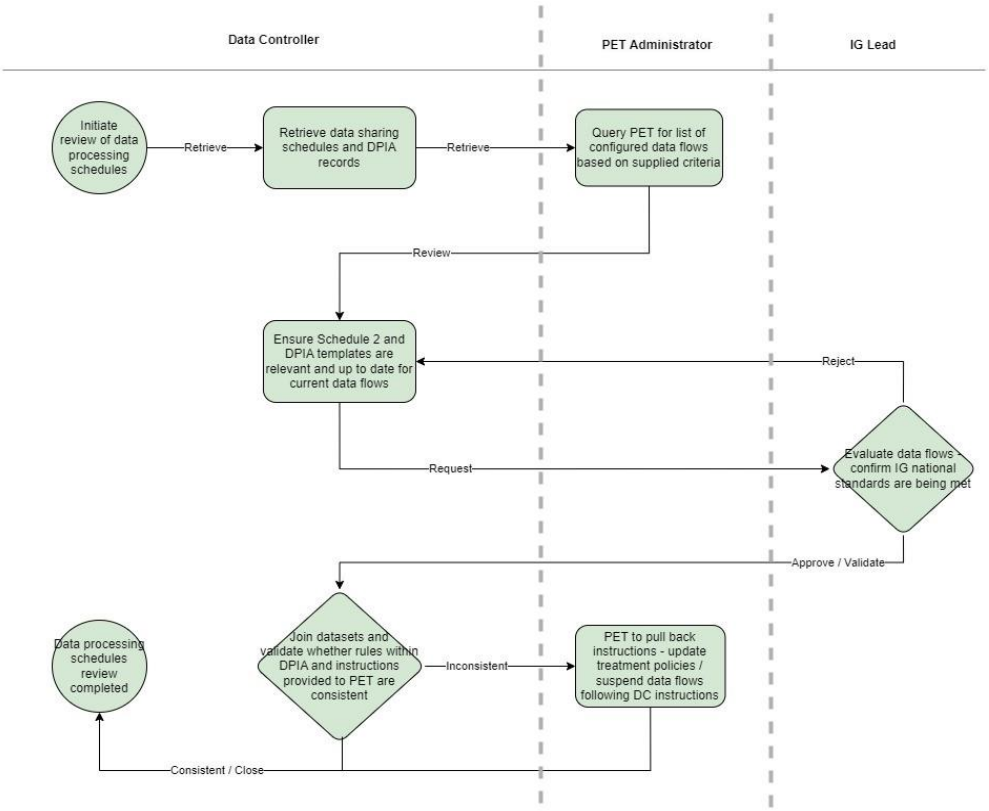


Figure 18 7 - Annual Dataset Review Process

4.1.4 Data Incident Management Process

The data incident management process refers to the steps and roles required to handle incidents that are related to a suspected breach of sensitive patient data. The NHS-PET Administrator, NHS-PET Supplier, IG lead and Data controller will investigate the incident and determine the initial scope of the breach and any required actions. The NHS-PET administrator implements any actions under the explicit instruction of the Data Controller.

The data breach process is subject to the process and requirements described in *Schedule 2, Appendix 2B – Security Requirements*.

4.2 NHS-PET Business Administration Interface

It is critical that the solution provide a comprehensive and intuitive web-based management console to enable NHS-PET Business Administrators to manage the NHS-PET service and support key operational processes.

Access to administration interface must be via HTTPS and must implement a Role Based Access Control (RBAC). RBAC must be used to limit the scope of access and capability by organisation and business role. To support scaling and maintain the security of user level accounts the console must use an NHS identity provider. The identity provider supports standard authentication integration patterns including SAML and OIDC.

The expected high-level function must include: -

Access controls

- Manage users and roles – Manage access to the NHS-PET administration console including RBAC groups, roles, and policies.
- Manage API – Configure API consumers, manage granular access to APIs and provide relevant API keys.

NHS-PET Configuration Management

- Manage dataset specification templates – Support NHS standard and custom dataset metadata configurations.
- Metadata management – view and manage metadata catalogue.
- Manage access control policies - Support NHS standard and custom dataset metadata configurations.
- Manage privacy treatments – Manage available treatment catalogue and implementation configurations.
- Manage data discovery / leak detection patterns – Support custom NHS data discovery patterns and rules.
- Mechanism for the optional scheduling of changes
- To ensure the integrity of the configuration the system must support separation of change, approval and publish activities.

Data Flow Management

- Manage data orchestration – Add and modify dataflow pipelines including data source, validation, discovery / leak detection, treatments, controls, destination.
- Manage required data discovery rules and policies.
- Data validation incident management – Identify and troubleshoot.
- Data discovery / leak detection incident management – Identify and troubleshoot.
- Enable / Disable data flows.
- Mechanism for the optional scheduling of changes.
- To ensure the integrity of the configuration the system must support separation of change, approval and publish activities.

Audit Review

- Audit review – Search and filter capability providing configuration related audit information.
- Audit review – Audit the data flows processed by the system.
- Annual review process – Provide an extract of the configured data flows and controls.
- Usage reporting and statistics filtered by dimensions including data source, data specification, metadata attribute and control policy.

Training and Documentation

- Administration guide – comprehensive documentation to describe the functionality of the administration system.
- Configuration guide – information regarding how to configure data flows and orchestration.
- API Reference guide including OpenAPI v3 documentation and examples.

5 Implementing NHS-PET

NHS-PET will be implemented to meet FDP timescales. In order to meet each milestone, the Successful Supplier will need to deliver the following capabilities in line with milestones as set out in the Contract - Schedule 7, Milestones.

Please refer to the following Table which highlights the implementation capabilities, timelines and associated activities. The corresponding phases, outline at a high-level the indicative activities the Successful Supplier will need to carry out during implementation, please note the phases below could be running in tandem. The Successful NHS-PET Supplier should be able to provide additional capabilities and features throughout the implementation cycle across different phases.

Phase	Descriptions	Capabilities Specific to NHS-PET	Relevant Data	Phase Start Date	Milestone	Milestone Date
P1 Basic NHS-PET Services	Establishing baseline NHS-PET capability with basic services. This can be split into 2 sub-phases: a) Make NHS-PET Solution ready to be integrated with the FDP-AS Platform (including testing). b) Integrate with FDP-AS platform (dependency on FDP-AS going live). NB: This includes relevant mobilisation activity (if applicable).	• API and File based data integration. • Provide baseline data treatments and access controls. • Audit and logging • Administration capability • Migrate any existing FDP-AS ingress dataflows via the NHS-PET solution. • Operational support capability including a non-production environment capability	1. Basic NHS-PET Services go-live will align to FDP-AS go-live. This will involve the migration of existing datasets. Assume 1600 input datasets. 2. Please refer to section 5 (Capacity Model) of Schedule 1A, Background and Context for indicative volumetrics. Assume the 'low adoption' scenario for NHS-PET immediately after Milestone 1.	Oct/Nov 2023	**Milestone 1** – Basic NHS-PET Services Live Note this is a Key Milestone Basic NHS-PET Solution-Readiness Complete - Basic NHS-PET Services go-live, ready to process configured data flows - Relevant testing complete - Successful integration with NHSE Operational and Service Management Model, including SOC services NB: As part of mobilisation activity, all relevant implementation resource and personnel will be onboarded (including Security and Vetting)	Jan 31, 2024
P2 Scaled NHS-PET Services	Provide additional NHS-PET capabilities including data format support (object data, data streams etc.), data reidentification API, and enhanced administration processes in support of wider onboarding.	• Reidentification API. • Data metadata validation. • Extend data format support object data, data streams. • Scaled management processes in support of wider onboarding. • Continuous improvement activity in support of FDP-AS and Data controller requirements.	The data capacity requirements for P2 are uncertain, please refer to section 5 (Capacity Model) of Schedule 1A, Background and Context for indicative volumetrics. Assume the 'low adoption' scenario for NHS-PET immediately after Milestone 2.	Feb 2024	**Milestone 2** - Scaled NHS-PET Services Solution Complete - Scaled NHS-PET Services go-live, ready to process configured data flows in line with increased adoption - Relevant testing complete - Successful integration with NHSE Operational and Service Management Model, including SOC services	March 31, 2024

P3 NHS-PET – Audit and Adherence	Incorporating additional capabilities around data validation, PID discovery and optimised incident management and governance.	• Data PID leakage detection. • Additional data treatments. • Scaled Incident and operational management. • Data governance and management capability. • Continuous improvement activity in support of FDP-AS and Data controller requirements.	The data capacity requirements for P3 are uncertain, please refer to section 5 (Capacity Model) of Schedule 1A, Background and Context for indicative volumetrics. Assume the 'low adoption' scenario for NHS-PET immediately after Milestone 3.	April 2024	**Milestone 3** - NHS-PET Implementation Complete - Completion of NHS-PET functional and non-functional scope - Relevant testing complete - Successful integration with NHSE Operational and Service Management Model, including SOC services	May 31, 2024
P4 Run	The run and operation of NHS-PET solution along with continuous improvement.	N/A	See all scenarios in section 5 (Capacity Model) of Schedule 1, Appendix 1A for indicative volumetrics.	Feb 2024 onwards	N/A	N/A

Table 1 - Overview of indicative Implementation Phases

6 Appendix A - Illustrative Data Flow Example

The following illustrative scenario describes the processing of a theoretical dataset into an FDP-AS ICS/ICB Tenant. The dataset is required to analyse the prevalence of diabetes for a particular patient population.

Scenario:

- A dataset specification is provided by an FDP Trust level tenant
- The dataset contains the following attributes: Gender, Patient Name, NHS Number, Postal Address, Date of Birth.
- The dataset needs to retain referential integrity with patient records elsewhere on the Data Platform and must show the patients gender and age.

Activities:

1. The Data Controller evaluates the dataset structure and determines that the associated specification and any stated controls are valid.
2. A risk assessment is performed by the Data Controller, and it is determined that a number of protections should be undertaken.
    - Data masking: replace patient names with unique identifiers and remove Postal Addresses.
    - Pseudonymisation: calculate the Patient ID from the NHS Number
    - Generalisation: replace patient by ages with a range using a bucketing algorithm
    - Approved purpose: Diabetes Population Health
3. The dataset is configured in NHS-PET (refer to Dataset Onboarding Process)
4. The protected dataset is consumed by the FDP platform, modelled and is made available for secondary use.
5. A person performs analysis on the dataset either directly using the analysis tools or hosted application provided by the FDP-AS.

Re-identification flow:

6. A pattern is identified and there are grounds to contact either the patient or care provider. To support this FDP-AS initiates a re-identification request on behalf of the user.
7. The re-identification request and associated result set is passed to NHS-PET and is authorised based on a user role and purpose agreed with the Data Controller.
8. Upon successful authorisation of the re-identification request NHS-PET processes the submitted result set and recovers the identifiable attributes, in this case NHS Number and returns is returned to FDP-AS.

Notes on integration with the National Patient Demographics service

The National Person Demographic Service (PDS) is hosted on National NHSE systems, and acts as a single source of the truth for matched Patient records at a national level. Data from PDS is required for numerous national use cases and data products.

Data from PDS is typically combined with other national datasets and pseudonymised before analysis can take place. In this case it is vital that pseudonymised PDS data can be joined with other pseudonymised national datasets. Data from PDS and data products derived from PDS will flow into FDP but will also be used in existing national analytics platforms.

In some cases, analysis will result in the need for direct patient intervention, so the data will need to be re-identified.

In some cases, analytical output will need to be shared with external 3rd parties. In this case, further NHS-PET processing will be required to fully anonymise the data before distribution.

When a data set is to be linked with other datasets through personal identifiable information that is pseudonymised, the PET system must keep track of the underlying identity of the persons so that the pseudo keys can be a valid method for linkage. When this occurs, the PET system must be able to link the person identity information with that included in PDS. NHS-PET should not build its own siloed registry of personal identifiable information.

7 Appendix B – National Dataset Specification Example

Source systems e.g., Trust systems may supply datasets according to standard specifications determined by NHS England. These controlled specifications define the records including column structure, data types, formats, and the high-level privacy processing actions. NHS-PET will be configured with standardised versioned template configurations to support these interactions supporting an efficient data onboarding process.

Example representing a Trust level admission flow.

Action	Description
Cleanse	Will look/check for patient Identifiable data e.g. NHS Number, DOB in the data. (also known as 'Leaky PID Cleansing) and then redact if found.
Redact	This field will not flow or be used for derivations - eg first name/surname.
Pseudo	This field will be pseudo'd. Pseudo version applied to be noted on the derivation tab.
No Action	Data will pass through the processing as it is and remain unchanged.
Derived	Field to be used for derivations but wont be disseminated.
Sensitive	Process to handle sensitive/restricted content eg.HIV.
On Hold	Data item redacted until further investigation.
Table Link	Field used to link multiple tables across dataset. No clean / pseudo action to be taken on this field as its used to join tables together.

APC_ADMISSION v1.0

Position	Data Element	NHSDD Format	Column Name	UniqueKey Member	Processing Action	NHSDD Element Description (Including Data Attributes) URL	Note
1	ACTION	max an12	Action		Redact		
2	NON CDS UNIQUE IDENTIFIER	max an35	NonCdsUniqueIdentifier	Yes	Cleanse	https://www.datadictionary.nhs.uk/data_elements/non_cds_unique_identifier.html	
3	ORGANISATION IDENTIFIER (CODE OF PROVIDER)	min an3 max an6	OrganisationIdentifierCodeOfProvider	Yes	No Action	https://www.datadictionary.nhs.uk/data_elements/organisation_identifier__code_of_provider_.html	
4	ORGANISATION SITE IDENTIFIER (OF TREATMENT)	min an5 max an9	OrganisationSiteIdentifierOfTreatment		No Action	https://www.datadictionary.nhs.uk/data_elements/organisation_site_identifier__of_treatment_.html	
5	REPORTING PERIOD START DATE	an10 CCYY-MM-DD	ReportingPeriodStartDate		No Action	https://www.datadictionary.nhs.uk/data_elements/reporting_period_start_date.html	
6	REPORTING PERIOD END DATE	an10 CCYY-MM-DD	ReportingPeriodEndDate		No Action	https://www.datadictionary.nhs.uk/data_elements/reporting_period_end_date.html	
7	LOCAL PATIENT IDENTIFIER (EXTENDED)	max an20	LocalPatientIdentifierExtended		Cleanse	https://www.datadictionary.nhs.uk/data_elements/local_patient_identifier__extended_.html	
8	NHS NUMBER	n10	NhsNumber		Pseudo	https://www.datadictionary.nhs.uk/data_elements/nhs_number.html	
9	POSTCODE OF USUAL ADDRESS	max an8	PostcodeOfUsualAddress		Derived	https://www.datadictionary.nhs.uk/data_elements/postcode_of_usual_address.html	
10	PERSON BIRTH DATE	an10 CCYY-MM-DD	PersonBirthDate		Derived	https://www.datadictionary.nhs.uk/data_elements/person_birth_date.html	
11	DURATION OF ELECTIVE WAIT	max an4	DurationOfElectiveWait		No Action	https://www.datadictionary.nhs.uk/data_elements/duration_of_elective_wait.html	
12	INTENDED MANAGEMENT CODE	an1	IntendedManagementCode		No Action	https://www.datadictionary.nhs.uk/data_elements/intended_management_code.html	
13	HOSPITAL PROVIDER SPELL IDENTIFIER	max an20	HospitalProviderSpellIdentifier		Cleanse	https://www.datadictionary.nhs.uk/data_elements/hospital_provider_spell_identifier.html	
14	START DATE (HOSPITAL PROVIDER SPELL)	an10 CCYY-MM-DD	StartDateHospitalProviderSpell		No Action	https://www.datadictionary.nhs.uk/data_elements/start_date__hospital_provider_spell_.html	
15	START TIME (HOSPITAL PROVIDER SPELL)	an8 HH:MM:SS	StartTimeHospitalProviderSpell		No Action	https://www.datadictionary.nhs.uk/data_elements/start_time__hospital_provider_spell_.html	
16	ADMINISTRATIVE CATEGORY CODE (ON ADMISSION)	an2	AdministrativeCategoryCodeOnAdmission		No Action	https://www.datadictionary.nhs.uk/data_elements/administrative_category_code__on_admission_.html	
17	PATIENT CLASSIFICATION CODE	an1	PatientClassificationCode		No Action	https://www.datadictionary.nhs.uk/data_elements/patient_classification_code.html	
18	METHOD OF ADMISSION (HOSPITAL PROVIDER SPELL)	an2	MethodOfAdmissionHospitalProviderSpell		No Action	https://www.datadictionary.nhs.uk/data_elements/method_of_admission__hospital_provider_spell_.html	
19	ADMISSION SOURCE (HOSPITAL PROVIDER SPELL)	an2	AdmissionSourceHospitalProviderSpell		No Action	https://www.datadictionary.nhs.uk/data_elements/admission_source__hospital_provider_spell_.html	
20	WARD CODE	max an12	WardCode		No Action	https://www.datadictionary.nhs.uk/data_elements/ward_code.html	
21	WARD INTENDED CLINICAL CARE INTENSITY	an2	WardIntendedClinicalCareIntensity		No Action	https://www.datadictionary.nhs.uk/data_elements/ward_intended_clinical_care_intensity.html	
22	ACTIVITY TREATMENT FUNCTION CODE	an3	ActivityTreatmentFunctionCode		No Action	https://www.datadictionary.nhs.uk/data_elements/activity_treatment_function_code.html	
23	INTENDED PRIMARY PROCEDURE (OPCS)	an4	IntendedPrimaryProcedureOpcs		Sensitive	https://www.datadictionary.nhs.uk/data_elements/primary_procedure__opcs_.html	
24	NCEPOD URGENCY CODE	an2	NcepodUrgencyCode		No Action	https://www.ncepod.org.uk/	
25	NCPP PRIORITY_CODE	an2	NcppPriorityCode		No Action	https://fssa.org.uk/_userfiles/pages/files/covid19/prioritisation_master_240720.pdf	
26	DISEASE OUTBREAK NOTIFICATION DESCRIPTION	max an20	DiseaseOutbreakNotificationDescription		Cleanse	https://datadictionary.nhs.uk/data_elements/disease_outbreak_notification_description.html	
27	DISEASE OUTBREAK NOTIFICATION (SNOMED CT)	min n6 max n18	DiseaseOutbreakNotificationSnomedCt		Sensitive	https://datadictionary.nhs.uk/data_elements/disease_outbreak_notification__snomed_ct_.html	

Figure 189 – Example templated Data Specification

8 Appendix C – NHS Standards and Practices

NHS Service Standard Principles, expands on GDS's Service Standard:
https://service-manual.nhs.uk/standards-and-technology/service-standard

GDS Service Standard principles:
https://www.gov.uk/service-manual/service-standard

NHS Architecture principles:
https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-architecture/principles

The Technology Code of Practice:
https://www.gov.uk/guidance/the-technology-code-of-practice

NCSC Cloud Security principles:
https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

NHS Data and Application Security:
The solution must comply with NHS Data Security and Protection Toolkit
GPG44: Using authenticators to protect an online service - GOV.UK (www.gov.uk)
GPG45: How to prove and verify someone's identity - GOV.UK (www.gov.uk)
Security and authorisation - NHS Digital
DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services - NHS Digital

Data retention policy and guidance
Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

Information Security Management
ISO - ISO/IEC 27001 — Information security management

Development Frameworks
NHS digital, data and technology standards - NHS Digital which embodies the
Government Design Principles - GOV.UK (www.gov.uk)
Developer hub (digital.nhs.uk)

NHS Accessibility Standards
NHS England » Accessible Information Standard
NHS (DCB1605): Accessible Information
Government WCAG 2.1 AA Accessibility Standard

Service Management
ISO 200001 for service management systems

NHS - Privacy Enhancing Technology (NHS-PET)

Schedule 2 Appendix 2C: Ways of Working and Service Catalogue

Name of Contracting Authority	**NHS England**
Procurement for	**NHS - Privacy Enhancing Technology (NHS-PET)**
Project reference	**C177577**
Find a Tender Service Contract Notice reference	**FTS-007743**
Date of Publication	**21 June 2023**
Tender Submission Response Deadline	**26 July 2023**

Contents

1 Introduction

1.1 Purpose of the Document

This document describes the Ways of Working for the NHS - Privacy Enhancing Technology (NHS-PET), as part of both the NHS landscape and, more specifically, as part of the overall Federated Data Platform programme – the first use of PET within the NHS.

It outlines the operating model requirements of the NHS-PET and sets out the high-level responsibilities of the Successful Supplier.

The document should be used as a reference to enable Participants to understand their roles and responsibilities in relation to delivering NHS-PET. The document will emphasise the expectations for the Successful Supplier and detail the requirements. The Successful Supplier will have the opportunity to further shape and contribute to these requirements.

1.2 Guide to the Document

This document outlines the principles, high level delivery expectations, and ways of working that the Successful Supplier will need to adhere to for delivery of NHS-PET.

The document's first three sections provide a conceptual outline of this delivery, from the FDP's structure and relationship with wider NHS organisations, to an overview of privacy in the context of the FDP and what is needed through procuring NHS-PET. Section 5 describes the service catalogue in the context of the NHS and FDP. Section 6 provides an indication for the processes that NHS-PET is expected to need to support

Section 1: Introduction (this section): The purpose and guide to this document is set out in the introduction, including some key terms that are used throughout the document.

Section 2: Organisation overview: An overview of the FDP's structure and relationship with wider NHS organisations.

Section 3: Federated Data Platform Privacy: An overview of the need for privacy and the context of the Federated Data Platform in which NHS-PET is being procured.

Section 4: Privacy Enhancing Technology: An explanation of the NHS-PET and its operation in the context of the FDP and NHS Governance

Section 5: Service Catalogue: The service catalogue defines the key services for NHS-PET to be provided to the NHS and its stakeholders.

Section 6: Indicative NHS-PET processes: Indicative processes that the NHS-PET Successful Supplier is expected to need to support.

1.3 Glossary

- **Control** – measures that are required to maintain privacy of the data including treatment and appropriateness of access
- **Treatment** – a technical process applied to a dataset
- **Anonymisation** – data is de-identified such that the original value cannot be determined
- **Pseudonymisation** – data protection technique that involves processing data in such a way that it is not possible to attribute them to a specific person without the use of additional information.
- **Re-identification** – the process of turning pseudonymised data back into personal data
- **Data Controller** – the person or organisation that has control over a set of personal data and is the main decision-maker

See **Schedule 8 Glossary** for the full NHS-PET glossary.

2 Organisation Overview

2.1 Partnership Principles

The FDP Programme takes a long-term approach to improving the data capabilities within the NHS.

The Successful NHS-PET Supplier will be a part of the FDP programme in supporting NHS England's aspirations to improve healthcare access for the public. In this role, the Successful NHS-PET Supplier will support the programme to deliver sustainable outcomes including:

- **Building Data Capability**: enabling NHS England to have a lasting, improved data capability throughout the lifecycle of this contract
- **Knowledge Exchange**: empowering NHS England in increasingly growing their in-house talent and knowledge
- **Unlocking Efficiencies**: delivering against a long-term vision of reducing costs through increased efficiencies and automation
- **Continuous Improvement and Innovation**: developing industry-led insights for continuous improvement and innovation to continue to improve data protection, cyber security and privacy
- **Improving Demand Responsiveness**: responding quickly to on-going and emerging demands on the NHS through flexible resourcing models
- **Transparency:** providing transparency on cost, platform development, change management and platform operations to enable a productive partnership
- **Collaboration:** the NHS-PET Successful Supplier will need to collaborate and integrate with NHS staff across a large variety of NHS organisations, as well as the Federated Data Platform technology and work well with the FDP-AS Successful Supplier; NHS-PET will need to co-exist with the FDP that is expected to be continuously developing and improving

3 Privacy Enhancing Technology

3.1 Introduction

The Successful NHS-PET Supplier will deliver a NHS-PET service that provides data privacy and protection to:

1. In the first case – the FDP;
2. In future cases – more widely than FDP, as it will be a reusable and standalone capability that could be made available to systems as an enterprise solution across the NHS.

3.2 Illustrative NHS-PET data flow

The Successful NHS-PET Supplier will deliver a solution that will be involved in all data flows across FDP where any Information Governance controls are required. Not all data ingested into FDP will require treatment by NHS-PET – the relevant Data Controller will always be responsible for determining the treatment required and conducting this through NHS-PET.

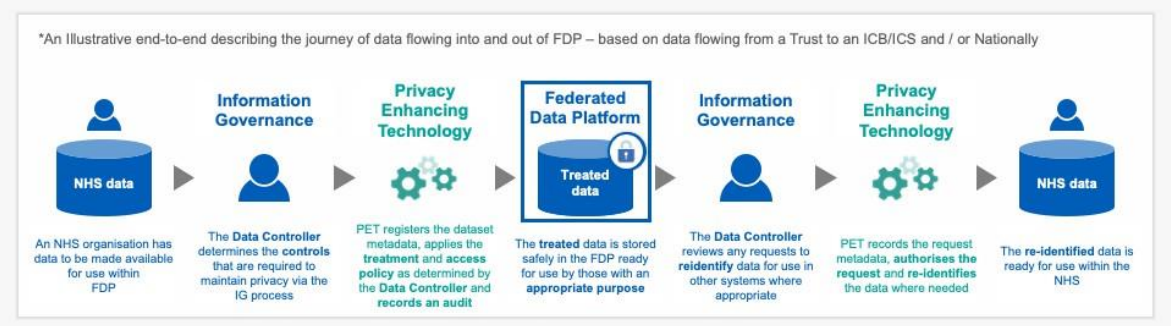


Figure 1 Data Flow of FDP

Data flows may take the form of one-off ingestion or ongoing data pipelines; the NHS-PET solution will apply controls to both as directed by the relevant Data Controller.

See **Appendix 2B – Information Governance and Security** for details on the requirements relating to the use of DPIAs and the Approval process with NHS-PET.

3.3 NHS-PET integration with FDP

The Successful NHS-PET Supplier will deliver a solution that is distinct and independent from the FDP.

The NHS-PET Successful Supplier is expected to understand the scope of FDP and the delineation and interaction between the services, particularly where capabilities are shared across the two.

See **Schedule 2 Appendix 2A Technical Specification** for the description of capabilities provided by NHS-PET and those common with FDP.

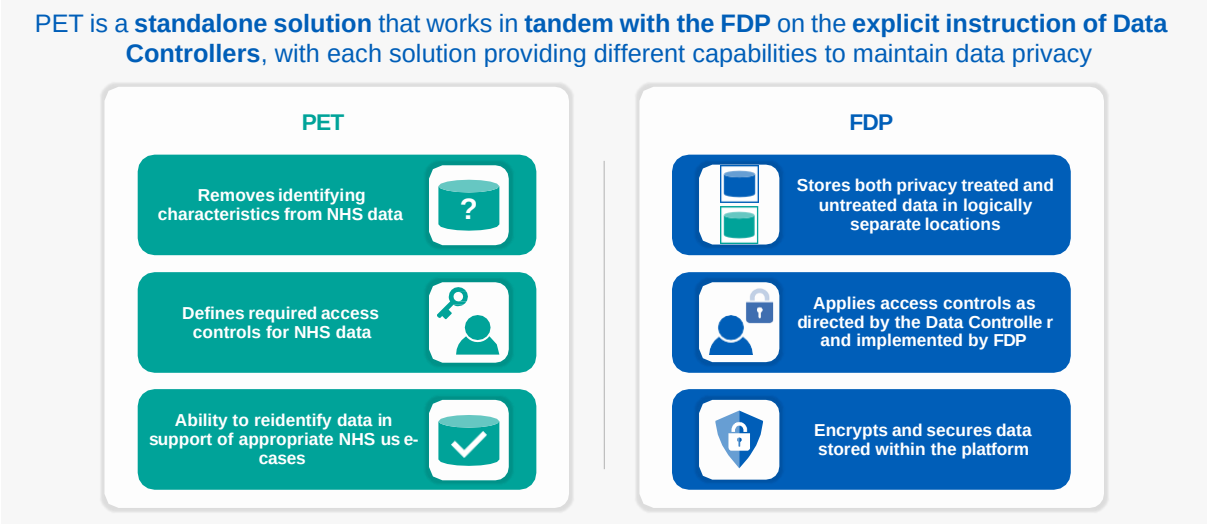


Figure 2 PET and FDP Comparison

3.4 Operating model requirements and considerations

NHS-PET is a solution that contributes to the broader Information Governance framework in which Information Governance support is required across multiple organisations within the NHS. NHS-PET is supplying the solution to applying controls on the data defined by Data Controllers.

The NHS-PET Successful Supplier will also need to manage new and changing demand from NHS organisations, including where NHS organisations themselves may change through new, merging or abolished bodies.

Support and assurance from NHS England will be provided for Trusts and ICS/ICB Information Governance Leads to onboard data in the initial phases of FDP implementation.

The Information Governance requirements and expectations of the NHS-PET Successful Supplier (including Procedures for managing Information Governance Incidents) are set out in **Appendix 2B – Information Governance and Security Requirements**.

3.5 Mobilisation

The Successful NHS-PET Supplier will mobilise to drive NHS-PET to be available and integrated for the overall FDP-AS go-live, and the NHS-PET Successful Supplier will need to work in close collaboration with the programme team, NHS-E and the FDP-AS Supplier to ensure a successful launch.

See **Appendix 2A Technical Specification, Section 5,** for further details on NHS-PET implementation phasing and requirements.

3.6 FDP Governance

This section describes the anticipated governance structure, forums, and processes for the FDP Programme.

Given the use of NHS-PET for FDP in the first instance, the Successful NHS-PET Supplier will integrate with these forums, as well as NHS technical, delivery, programme management cadence and other relevant governance forums as required by NHS England.

3.6.1 Governance Forums – Overview

The FDP Programme will integrate with existing NHS England governance forums, as well as running FDP-specific governance forums and working groups. Each will play a key role in the smooth running of the Programme and support effective decision making. There are four layers of governance set out in this document (see Figure 3):

1. **Strategic level governance:** existing NHS England governance forums that the FDP will report into; and thus, the NHS-PET Successful Supplier should be aware of and may need to feed into.
2. **FDP Programme level governance:** FDP specific forums that govern the Product lifecycle and wider operations of the FDP Programme. The NHS-PET Successful Supplier will be required to engage with this level of governance as required.
3. **Relevant working groups:** Working groups designed to support initial decision making and progress across the Product lifecycle.

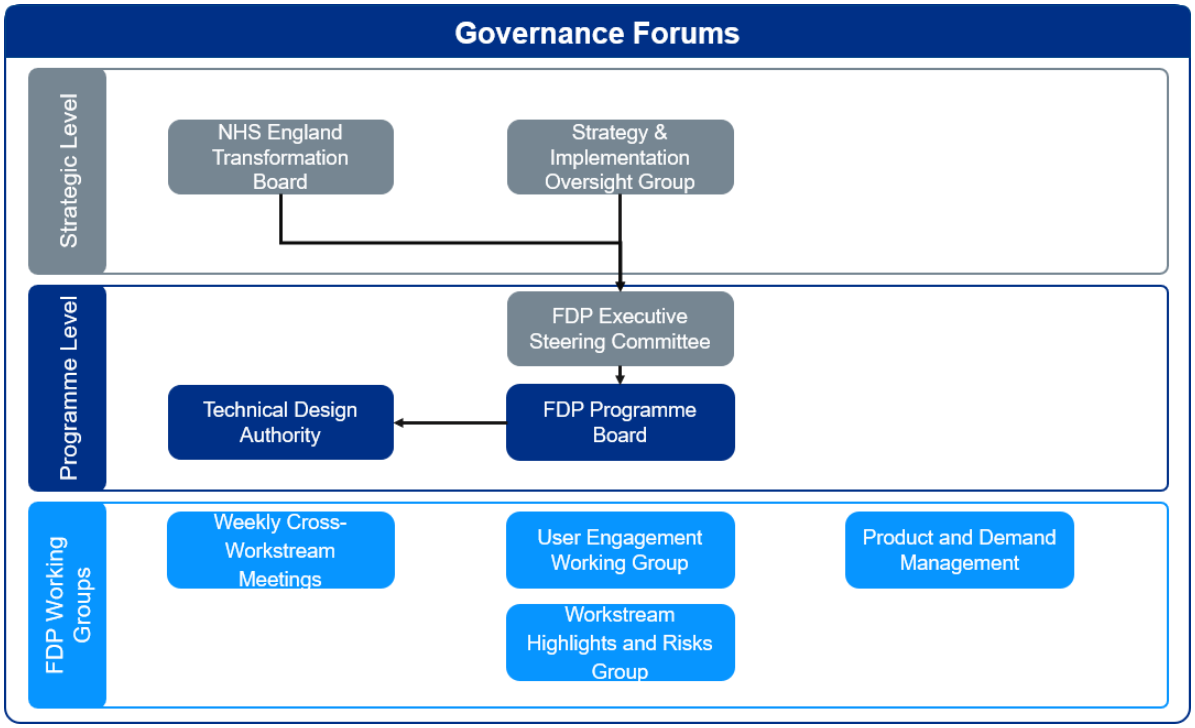


Figure 3 Indicative Governance Forums on the Strategic, Programme, and FDP Working Group Level

The NHS-PET Successful Supplier will need to engage with Information Governance, likely at both a Local and National level with Information Governance Leads.

The exact roles and inputs for each forum will need to be determined upon contract award between NHS England and the Successful Supplier.

Strategic Level Governance

The Successful Supplier will report into the following Strategic Level Governance Forums:

- **NHS England Transformation Board:** Responsible for overseeing and coordinating the implementation of large-scale changes and improvements to NHS England. The FDP will be a key part of NHS England's Transformation Portfolio, and hence the Programme will report into this. The Transformation Board will be the final point of escalation for the FDP Programme and will provide high-level oversight to the Programme.
- **Strategy and Implementation Oversight Group**: Responsible for providing oversight and guidance for the development and implementation of the organisation's strategy. This group will approve annual plans for NHS-PET.

It is not expected that the NHS-PET Supplier will attend any of the Strategic Level Governance Forums, although there will be a requirement from the NHS-PET Supplier to feed into regular updates via the FDP Programme Team.

FDP Working Groups

The FDP Programme will also be supported by several working forums, designed to promote efficient governance. These forums include:

- **Weekly Cross-Workstream Meetings**: Meeting of different teams and stakeholders involved in the FDP Programme to collaborate and coordinate. This includes commercial-led status meetings and update meetings with Product teams. The forum is expected to meet weekly. The NHS-PET Successful Supplier is expected to need to attend this forum.
- **User Engagement Working Group**: Responsible for ensuring that the needs and requirements of users are understood and incorporated into the design and development of Products. This includes gathering and sharing user feedback and collaborating with other teams to realise the received feedback. The forum is expected to meet quarterly. The NHS-PET Successful Supplier is not expected to need to attend this forum.
- **Workstream Highlights and Risks Group**: Responsible for providing regular updates and summaries of the progress of various workstreams as well as risk management. This includes sharing of update reports and important decisions, identifying milestones and the identification and mitigation of risks. The forum is expected to meet weekly. The NHS-PET Successful Supplier is expected to need to attend this forum.
- **Product Management Group**: Responsible for managing the development, delivery, and ongoing support of Products. The forum is expected to meet weekly. The NHS-PET Successful Supplier is not expected to need to attend this forum.
- **Demand Management Group**: Responsible for ensuring that Products meet the needs and requirements of users. This includes identifying user needs for new Products and definition of Product features and benefits. The forum is expected to meet weekly. The NHS-PET Successful Supplier is not expected to need to attend this forum.
- **Technical Design Authority**: Responsible for the scope and initiation of technical work related to the FDP Programme, and as an interlock between the FDP and DMIS Technical Design Authority to ensure decisions are taken with a view of the wider landscape
- **Operational meetings**: Regular governance relating to the successful operation of the service day to day. These meetings will be defined and mobilised once the contract has been awarded. The NHS-PET Successful Supplier is expected to attend these forums.

As the programme moves into operational running there will be additional BAU governance forums for clinical risk and IG – the NHS-PET Successful Supplier is expected to attend governance that is relevant to their scope.

3.6.2 Knowledge Transfer

The successful supplier is expected to deploy knowledge transfer mechanisms throughout the development, build and run phases of delivery to reduce NHS's reliance on the supplier.

4 Service Catalogue

The High-Level Service model shown below defines how NHS-PET should integrate with the existing NHS Service Landscape, see Figure 4 below.

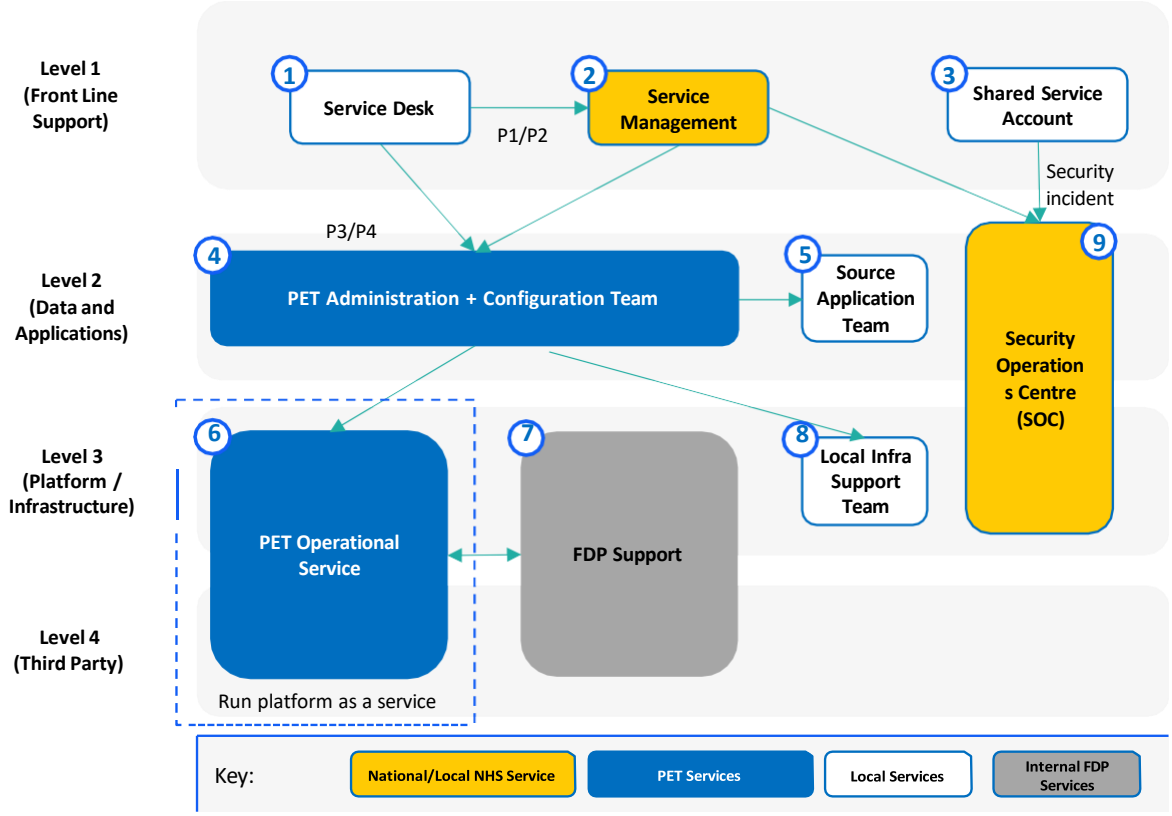


Figure 4 High Level Service model landscape

#	Team	Role	In Scope for NHS-PET Supplier
1	Service Desk	Act as a first line support for NHS England and Healthcare providers	N
2	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.	Y
3	Shared Service Account	Collect the event logs from operational and analytical systems then triage tickets to relevant support teams	N

4	NHS-PET Administration & Configuration Team	Apply the technical controls defined by Data Controllers through configuration and administration of the NHS-PET solution.	To be proposed by suppliers
5	Source Application Team	Proactively manage the availability of the source applications, identifying issues and potential problem areas	N
6	NHS-PET Operational Service	Self-sufficient, autonomous team responsible for the E2E delivery, operation, support and maintenance of NHS-PET, continuously provisioning the tools and services to help the other PODs to solely focus on their delivery objectives	Y
7	FDP Support	FDP Supplier platform management, operations and support for the FDP	N
8	Local Infra Support Team	Monitor and maintain the local infrastructure (On-premise and Cloud) ensuring it continuously operates and is available to their agreed level of performance and availability	N
9	Security Operations Centre (SOC)	Establish and integrate a security management capability in the public Cloud environment	N

Table 1 High Level Service model Role Descriptions

This high-level service model is in alignment with the broader FDP Service Model, which will augment the existing NHS Data and IG Services Model.

5 Indicative NHS-PET processes

NHS-PET will help ensure privacy and security of data across the NHS use of FDP and other enterprise data platforms in a standardised way.

The NHS-PET Successful Supplier will be involved in a number of Information Governance processes related to this. The following examples highlight a set of non-exhaustive indicative scenarios that the NHS-PET Successful Supplier should be aware of:

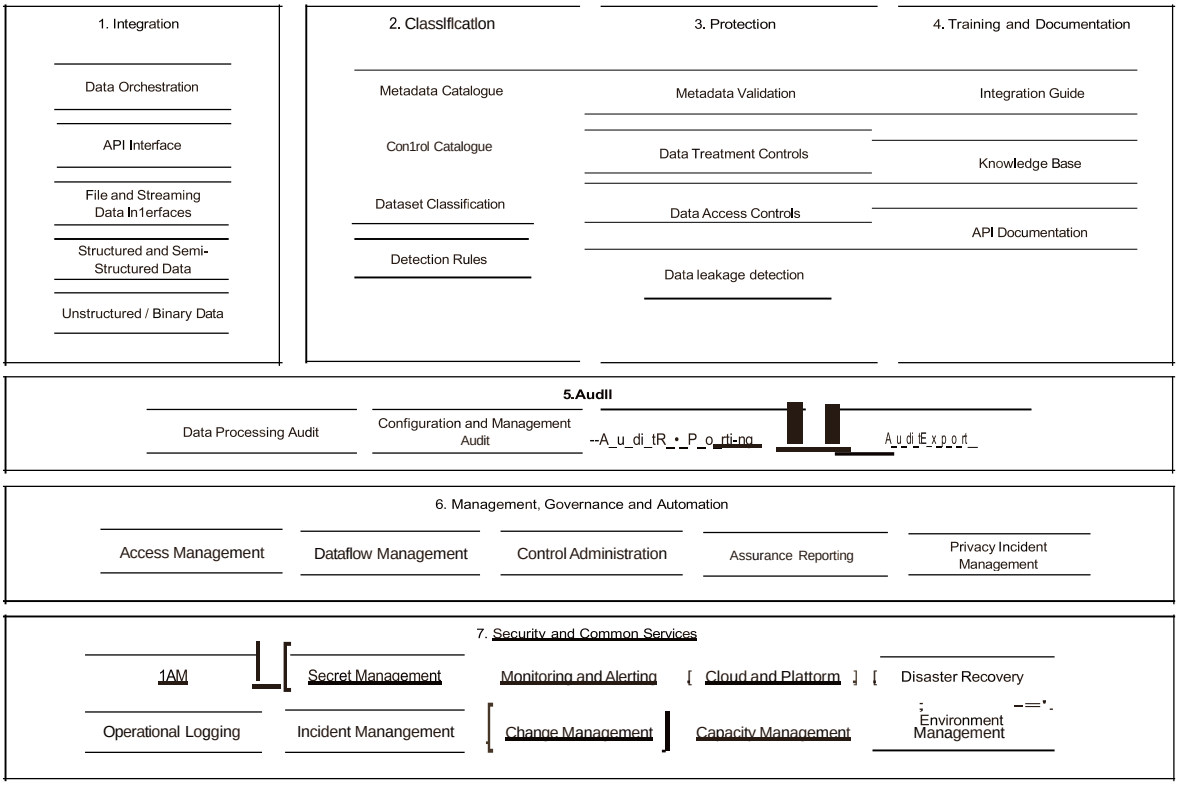
Figure 5 Indicative NHS-PET Supplier involvement in processes

See **Schedule 2 Appendix 2A Technical Specification** and **Schedule 2 Appendix 2D NHS-PET Requirements Catalogue** for more details on indicative process involved in NHS-PET.

Ref	Level 1	Level 2	Requirement	As per Quality Envelope Evaluation Criteria, Question 1a: Bidders must complete Column E in tab NHS-PET Requirements Catalogue - NHS-PET Requirements Catalogue, Schedule 2, Appendix 2D for each and every requirement, confirming that their organisation will meet each and every requirement by inputting "1. Can meet requirement".
1.1.1	Integration	Data Orchestration	The Supplier Solution provides a data pipeline capability to configure how data should be received, authorised, validated, audited, processed and made available to consumers	
1.1.2	Integration	Data Orchestration	The Supplier Solution supports for common patterns including Runtime NHS-PET, NHS-PET as a Data Interface, NHS-PET as a service and Hidden NHS-PET, as described in Schedule 2, Appendix 2A	
1.1.3	Integration	Data Orchestration	The Supplier Solution is modular, templated based configuration to support reuse, standardisation and consistency	
1.1.4	Integration	Data Orchestration	Application logging must be provided at each process stage of data pipelines	
1.1.5	Integration	Data Orchestration	Logging should contain summary information and should be added to logs where appropriate to describe the transaction	
1.1.6	Integration	Data Orchestration	The platform will support interoperability with existing NHS systems and technologies to facilitate data exchange and integration. This includes using standardised protocols and formats, supporting data portability.	
1.1.7	Integration	Data Orchestration	Implement clear data deletion and retention policies that specify how long data will be retained, and when it will be securely deleted	
1.1.8	Integration	Data Orchestration	The platform should only retain source and the associated data for as long as required to process and deliver the data	
1.1.9	Integration	Data Orchestration	Data is received, acknowledged and a task is added to a work queue for scheduling based on availability of resources e.g. compute	
1.1.10	Integration	Data Orchestration	All data transfers must be protected in transit using encryption. Where TLS is used as the transport protocol this must be at least TLS version 1.2	
1.1.11	Integration	Data Orchestration	The Supplier Solution must process data in an atomic transaction whereby the unit of transfer e.g. file is processed on an all or nothing basis	
1.2.1	Integration	API Interface	The Supplier Solution provides a REST API giving access for data processing purposes	
1.2.2	Integration	API Interface	The Supplier Solution provides a REST API giving access for configuration management	
1.2.3	Integration	API Interface	The Supplier Solution provides a REST API giving access for operational monitoring and management	
1.2.4	Integration	API Interface	The Supplier Solution provides a REST API giving access for audit and reporting	
1.2.5	Integration	API Interface	The Supplier Solution provides a REST API to giving status on data processing tasks	
1.2.6	Integration	API Interface	Implement standard based token based API security for example key based access, OAuth client credential	
1.2.7	Integration	API Interface	The Supplier Solution provides a generic and versioned API service.	
1.3.1	Integration	File and Streaming Data Interfaces	The Supplier Solution supports batch and mini-batch file based processing	
1.3.2	Integration	File and Streaming Data Interfaces	The Supplier Solution supports integration with cloud storage datasources for example AWS S3 or Azure Storage	
1.3.3	Integration	File and Streaming Data Interfaces	The Supplier Solution supports HTTPS based file transfer	
1.3.4	Integration	File and Streaming Data Interfaces	The Supplier Solution supports SFTP based file transfer	
1.3.5	Integration	File and Streaming Data Interfaces	The Supplier Solution provides message queue capability based on protocols including Kafka, AMQP, JMS	
1.3.6	Integration	File and Streaming Data Interfaces	The Supplier Solution supports for cloud vendor streaming services for example Kafka, AWS Kinesis or Azure Event Hub	
1.3.7	Integration	File and Streaming Data Interfaces	Authenticate and authorise all data transfer requests using a mechanism appropriate for the transfer type	
1.4.1	Integration	Structured and semi-structured data	The Supplier Solution must support structured and semi-structured data including but not limited to standard column delimited formats such as CSV, custom delimited format as well as object formats including JSON and XML	
1.4.2	Integration	Structured and semi-structured data	The Supplier Solution supports custom formatted / delimited data formats columner data formats.	
1.4.3	Integration	Structured and semi-structured data	The Supplier Solution must validate provided data against expected configuration and reject any invalid transfers	
1.4.4	Integration	Structured and semi-structured data	The Supplier Solution provides support for health domain specific object formats including HL7 and FHIR	
1.5.1	Integration	Unstructured / Binary Data	The Supplier Solution supports unstructured textual data formats such as PDF	
1.5.2	Integration	Unstructured / Binary Data	The Supplier Solution provides support for binary objects such as images and multimedia	
2.1.1	Classification	Metadata Catalogue	The Supplier Solution provides general purpose metadata managament capability capable of supporting structured, semi-structured, un-structured and binary / multi-media data types	
2.1.2	Classification	Metadata Catalogue	The Supplier Solution supports standardised NHS dataset specifications through the provision of versioned metadata templates	
2.2.1	Classification	Control Catalogue	The Supplier Solution provides a library of approved data treatments rule and policies	
2.2.2	Classification	Control Catalogue	The Supplier Solution provides an approved list of available data access controls - role, purpose and policy based models	
2.2.3	Classification	Control Catalogue	The Supplier Solution provides an approved list of available data discovery / data leak controls	
2.3.1	Classification	Dataset Classification	Associate configured data sets with policy based rules reflecting the Patient Identifiable Data (PID) classification applied to the source dataset	
2.3.2	Classification	Dataset Classification	The Supplier Solution provides a standardised library of detection rules and classifications (e.g. telephone number, email address)	
2.3.3	Classification	Dataset Classification	The Supplier Solution provides the ability to define custom detection rules and classifications (e.g. NHS number, clinical coding)	
2.4.1	Classification	Detection Rules	The Supplier Solution provides a standard library of common detection rules for example dates, addresses, phone numbers, identifiers	
2.4.2	Classification	Detection Rules	The Supplier Solution provides a means for defining custom pattern matching detection rules required for NHS or health domain data types e.g. clinical codes and patient identifiers	
2.4.3	Classification	Detection Rules	Manage detection rules on a policy or group basis	
2.4.4	Classification	Detection Rules	Associate a severity level with detection policies to determine the course of action if triggered. Example measures could include applying masking, raising a warning notice, stopping processing combined with raising an incident to the NHS service desk	

3.1.1	Protection	Metadata Validation	Map inbound data of all types against to an expected meta-data configuration. Where a mapping or metadata configuration does not exist cease further processing and raise an error and incident
3.1.2	Protection	Metadata Validation	Validate the dataset against the metadata configuration. Where the data does not conform to the expected specification and based on the severity of the validation issue processing may cease further processing and an error is raised.
3.1.3	Protection	Metadata Validation	Validate against the metadata specification at a field level including but not limited to data types, numerical ranges, expected lengths and string formats
3.1.4	Protection	Metadata Validation	Based on the severity of the validation failures incidents will be raised that require investigation.
3.2.1	Protection	Data Treatment Controls	The Supplier Solution applies data privacy treatments regardless of data transport protocol
3.2.2	Protection	Data Treatment Controls	The Supplier Solution applies data masking/redaction to applicable data attributes by obfuscating or removing sensitive data elements
3.2.3	Protection	Data Treatment Controls	The Supplier Solution applies data generalisation on the data source using automated or static bucketing configuration
3.2.4	Protection	Data Treatment Controls	Anonymise data through removing or replacing personal identifying information non-identifying information
3.2.5	Protection	Data Treatment Controls	The Supplier Solution provides a pseudonymisation treatment capability
3.2.6	Protection	Data Treatment Controls	The Supplier Solution provides a tokenisation treatment capability which can support detokenisation
3.2.7	Protection	Data Treatment Controls	Hashing functions - use industry standard secure algorithms that are considered collision resistant
3.2.8	Protection	Data Treatment Controls	Maintain the integrity of data flows using shared or linked data control configurations. Examples include shared psudonymisation keys or hashing seed such that datasets may be joined at the ICS/ICB and national tenant levels
3.2.9	Protection	Data Treatment Controls	The Supplier Solution supports a preconfigured and standardised data controls made available in a common control catalogue to support consistency and re-use.
3.2.10	Protection	Data Treatment Controls	To enable the migration between an incumbent privacy process the system should support the import of secrets including encryption keys and hashing seeds/salts
3.2.11	Protection	Data Treatment Controls	A data lineage service will track the processing of data as it flows through the NHS-PET service
3.2.12	Protection	Data Treatment Controls	Apply privacy treatments to metadata encapsulated within binary or multi-media data files for example an x-ray image with patient data contained within the metadata
3.3.1	Protection	Data Access Controls	The Supplier Solution must implement a policy model based aligned to the NHS IG Framework
3.3.2	Protection	Data Access Controls	Requests for reidentification must be authenticated and authorised based on the data access policies defined in NHS-PET
3.4.1	Protection	Data Leakage Detection	The Supplier Solution will apply data discovery of special category data data across all data types and sources
3.4.2	Protection	Data Leakage Detection	The Supplier Solution applies data discovery to data processing for the purpose of leak detection. Where unexpected PID data is detected determine action based (for example raise an incident to NHS service desk) on defined severity
3.4.3	Protection	Data Leakage Detection	Use policy based configuration to provide flexibility over how and when discovery rules are applied. For example consider inline, periodic, on-demand or dynamic modes
3.4.4	Protection	Data Leakage Detection	The Supplier Solution should provide reporting of sensitive data that has been identified
4.1.1	Training and Documentation	Integration Guide	Documentation designed for data providers and consumers describing the high level process and technical details required to integrate systems with the NHS-PET system
4.1.2	Training and Documentation	Integration Guide	The Supplier Solution delivers documentation using an accessible and intuitive web based interface
4.2.1	Training and Documentation	Knowledge Base	Detailed documentation describing the classification, protection and audit & management capabilities
4.2.2	Training and Documentation	Knowledge Base	Intuitive web-based interface with search and filter controls allowing NHS-PET users to find relevant information.
4.2.3	Training and Documentation	Knowledge Base	The knowledge base must be kept up-to-date and aligned with system features and capabilities.
4.3.1	Training and Documentation	API Documentation	The Supplier Solution provides support technical documentation for APIs to include API registration, authentication, key flows with examples
4.3.2	Training and Documentation	API Documentation	The Supplier Solution provides API specifications in OpenAPI v3 format
5.1.1	Audit	Data Processing Audit	The Supplier Solution provides a file level audit of all data processing activities including data ingress, metadata validation, privacy processing, PID detection and data egress. The audit may include relevant tokenised identifiers required for correlation purposes.
5.1.2	Audit	Data Processing Audit	The Supplier Solution provides a data row-level audit of data processing which should include relevant tokenised identifiers required for correlation purposes.
5.1.3	Audit	Data Processing Audit	Audit records are immutable and must be stored securely with relevant role based access applied to control access
5.2.1	Audit	Configuration and Management Audit	The Supplier Solution provides a complete, robust and immutable record of all changes to the NHS-PET service including but not limited to data classification templates, policies, protection catalogue, data flows, PID discovery rules, user management. The audit must contain the relevant identifers for correlation purposes
5.2.2	Audit	Configuration and Management Audit	Where configuration are being applied the audit record must contain details of the relevant changes and change approver
5.3.1	Audit	Audit Reporting	The Supplier Solution providesan intuitive web-based audit search and reporting capability covering data processing, platform and configuration management activity
5.3.2	Audit	Audit Reporting	Audit information information should be restricted based on the role of the user
5.3.3	Audit	Audit Reporting	Audit reporting must support a filtering capability, expected dimenstions include data fields, date ranges, audit events, data types and data sources.
5.4.1	Audit	Audit Export	The Supplier Solution should provide the ability to export audit data in a standard format that is compatible with log aggregation and audit tooling.
5.4.2	Audit	Audit Export	The Supplier Solution should be able to integrate with security and compliance tools, such as SIEM and DLP systems.
5.4.3	Audit	Audit Export	The export feature should allow customisation of the data exported, such as selecting specific data fields, date ranges, and audit events.
5.4.4	Audit	Audit Export	The export feature should provide an audit trail that logs all export activities, including who exported the data, when, and where.

5.5.5	Audit	Audit Export	The Supplier Solution must provide an event stream (push) interface as the primary means for data export with a supporting batch (pull) based mechanism
6.1.1	Management and Governance	Access Management	Manage access to the NHS-PET administration console including users, roles and group management
6.1.2	Management and Governance	Access Management	Configure API consumers, control access to API capabilities and provide relevant access keys.
6.2.1	Management and Governance	Dataflow Management	Manage data orchestration, add and modify dataflow pipelines including data source, validation, discovery / leak detection, treatments, controls, destination
6.2.2	Management and Governance	Dataflow Management	Toggle mechanism to enable / disable data flows.
6.2.3	Management and Governance	Dataflow Management	To ensure the integrity of the configuration The Supplier Solution must support separation of change, approval and change publish activities
6.3.1	Management and Governance	Control Administration	Manage dataset specification templates – Supporting NHS standard and custom dataset metadata configurations.
6.3.2	Management and Governance	Control Administration	Manage access control policies - Supporting NHS standard and custom dataset metadata configurations.
6.3.3	Management and Governance	Control Administration	Manage privacy treatments – Manage available treatment catalogue and implementation.
6.3.4	Management and Governance	Control Administration	Manage data discovery / leak detection patterns – Manage custom NHS data discovery rules.
6.4.1	Management and Governance	Assurance Reporting	The Supplier Solution provides an inventory of configured data flows, data specifications, applicable controls and relevant metrics so that the Data Controllers can review assess data assets they are reponsible for.
6.5.1	Management and Governance	Privacy Incident Management	The service should develop and document an incident response plan that outlines the steps to be taken in case of a privacy incident. Should include clear instructions on incident investigation, containment, eradication, and recovery.
6.5.2	Management and Governance	Privacy Incident Management	The Supplier Solution integrates with existing incident management paltforms to allow tracking and management of incidents efficiently. Dedicated tool or a combination of existing systems such as ticketing, case management, or project management tools.
6.5.3	Management and Governance	Privacy Incident Management	The ability to regularly review and update incident management processes to ensure they are effective and aligned with best practices. This includes conducting regular risk assessments, testing incident response plans, and providing ongoing training to personnel involved in incident management.
7.1.1	Common Services	Monitoring & Alerting	The Supplier Solution provides the necessary insight to support the capacity management for PET as highlighted in Section 4.2 of Schedule 1, Appendix 1A.
7.2.1	Common Services	Cloud and Platform	The Supplier Solution should be able to operate at a high level of performance to ensure that sensitive category data is identified and classified in a timely manner as per the Performance Levels in Schedule 8 of the Contract.
7.2.2	Common Services	Cloud and Platform	The Supplier Solution must be capable of supporting high availability as per Schedule 8 of the Contract.
7.3.1	Common Services	Disaster Recovery	The Supplier Solution must support the SLA and KPIs as set out in Schedule 8 of the Contract.
7.4.1	Common Services	Incident Management	Operational management related incidents to include data processing, data transfer, configuration and technical incidents must be raised to the the NHS England Service Bridge, as described in Schedule 2, Appendix 2C Ways of Working
7.4.2	Common Services	Incident Management	The managed service must integrate and coordinate with the NHS England Service Bridge, as described in Schedule 2, Appendix 2C Ways of Working
7.4.3	Common Services	Incident Management	The Supplier Solution NHS-PET managed service should be aligned to ITIL and will be integrated into a wider NHS Service Management model
7.5.1	Common Services	Change Management	Support the review and approval of changes to the service by the governance framework, as described in Schedule 2, Appendix 2C Ways of Working
7.6.1	Common Services	Capacity Management	The Supplier Solution must elastically scale up and down to accommodate the processing demands on the system. Configurable capacity limits, throttling and queuing should be used to manage peak load and accommodate spikes in demand.
7.6.2	Common Services	Capacity Management	The Supplier Solution must be capable of supporting large batch transfer that will be associated with the onboarding and migration of new data sources.
7.7.1	Common Services	Environment Management	Testing and assurance of features and key configuration changes prior to deployment in production must be carried out in non-production environments
7.7.2	Common Services	Environment Management	Non-production and sandbox environments must only contain synthetic data
8.1.1	Information Governance & Security	NHS-PET Solution	Please refer to C177577_NHSE_PET_ITT_Schedule 2, Appendix 2B -Information Governance and Security Requirements


1. Integration
Data Orchestration
API Interface
File and Streaming Data In1erfaces
Structured and Semi-Structured Data
Unstructured / Binary Data
2. ClassIfIcatIon
Metadata Catalogue
Con1rol Catalogue
Dataset Classification
Detection Rules
3. Protection
Metadata Validation
Data Treatment Controls
Data Access Controls
Data leakage detection
4. Training and Documentation
Integration Guide
Knowledge Base
API Documentation
5.AudII
Data Processing Audit
Configuration and Management Audit
--A_u_di_tR_•_P_o_rti-ng
A_u_di_tE_x_p_o_rt_
6. Management, Governance and Automation
Access Management
Dataflow Management
Control Administration
Assurance Reporting
Privacy Incident Management
7. Security and Common Services
1AM
Secret Management
Monitoring and Alerting
Cloud and Plattorm
Disaster Recovery
Operational Logging
Incident Manangement
Change Management
Capacity Management
Environment Management
8. Cyber Security and Information Governance

SCHEDULE 3

CYBER SECURITY AND INFORMATION GOVERNANCE

NHS - Privacy Enhancing Technology(NHS-PET)

Schedule 2 Appendix 2B: Information Governance and Cyber Security

Name of Contracting Authority	**NHS England**
Procurement for	**NHS - Privacy Enhancing Technology (NHS-PET)**
Project reference	**C177577**
Find a Tender Service Contract Notice reference	**FTS-007743**
Date of Publication	**21 June 2023**
Tender Submission Response Deadline	**26 July 2023**

Contents

1 Executive Summary

Excellence in data governance and Cyber Security are essential for all data types flowing through the NHS. This must be achieved via NHS - Privacy Enhancing Technology (NHS-PET) by ensuring the following controls are implemented:

Appropriately administering, under explicit instruction of the Data Controller:

- 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, Common Law Duty of Confidentiality, PECR)
- Following the agreed Information Governance (IG) approval process for all new data flows which will include completion of DPIA's, approved by all parties

The Supplier shall follow the IG approach based on the '5 Safes' Framework which has been developed by the Office for National Statistics who have operated similar data access platforms for many years. These principles are highly regarded and considered to represent data protection best practice, and our guidelines bring context and detail for how we expect these to be delivered in context of NHS data:

1. Safe Settings - the platform has features that prevent inappropriate access, or misuse.
2. Safe Data - information is protected and is treated to protect confidentiality.
3. Safe People - individuals accessing the data are trained and authorised to use it appropriately.
4. Safe Projects - research projects are approved by data owners for the public good.
5. Safe Outputs - summarised data taken away is checked to ensure it protects privacy.

The Solution shall, in order to prevent identification of edge cases, suppress small outlying data groups from exported datasets and information made available in analytic reports.

Through the use of data lineage, the Solution shall show the full context of data management including the source of data, full version history of the data, data aggregation rules, quality of data sets and the end-to-end transformation underpinning the integrity of the data being made available through the Data Platform.

The Solution shall ensure the confidentiality and the integrity of the data, through the use of:

I. data modelling techniques implemented into the ingestion processes including relational techniques;
II. data relationship modelling;
III. hierarchical modelling; and
IV. object modelling.

2 Standards, Frameworks and Principles

The supplier, and the solution, shall adhere to the following standards, guidance, and frameworks.

2.1 ISO 27001

The supplier must hold a current and valid ISO27001 qualification which has been issued by a certified accreditation body **or** plans to be accredited before the Contract Award. Sufficient evidence of accreditation plans must demonstrate how the organisation is going to achieve the standards for ISO27001 in the required timeframe.

2.2 ISO27017

The supplier must hold a current and valid ISO27017 qualification which has been issued by a certified accreditation body **or** plans to be accredited before the Contract Award. Sufficient evidence of accreditation plans must demonstrate how the organisation is going to achieve the standards for ISO27017 in the required timeframe.

2.3 Cyber Essentials Plus

The supplier must hold a current and valid Cyber Essentials Plus certification which has been issued by a certified accreditation body **or** plans to be accredited before the Contract Award. Sufficient evidence of accreditation plans must demonstrate how the organisation is going to achieve the standards for Cyber Essentials Plus in the required timeframe.

2.4 Data Security Protection Toolkit

The Supplier shall comply with the NHS England Data Security and Protection Toolkit (DSPT) to at least standards met.

2.5 Additional IG/Cyber Security Requirements

a. The Suppliers Solution pre-configures all data in transit encryption, and defaults to the latest industry standards.
b. The Suppliers Solution will have accurate and detailed Asset inventory for the term of the contract.
c. The Suppliers Solution shall:
    a. Encrypt all physical media
    b. Utilise application-level encryption.
    c. Utilise data encryption in memory.
d. The Supplier shall ensure that before the Supplier makes changes to the solution, they are assessed for security impact, managed, and tracked through to completion.
e. The Supplier shall ensure relevant sources of information relating to threat, vulnerabilities and exploitation techniques for the Solution are monitored and each newly identified or increased threat is appropriately treated or mitigated by the Supplier.

f. The Supplier shall ensure that configuration and secrets management processes are in place to ensure the integrity of the cloud service throughout development, testing and deployment.
g. The Supplier shall ensure that the NHS-PET solution has the capability to integrate with NHS England external secret and key management services.
h. The Supplier shall evidence the separation of Production, Testing and Development environments for the Solution.
i. The Supplier's Solution shall apply granular access control, according to the 'principle of least privilege', enabling both 'standard' and 'administrative' user accounts.
j. The Suppliers Solution shall prompt administrators to re-verify themselves using MFA when performing high privilege actions.
k. The Supplier shall ensure that impact assessments are completed for any full or partial loss of data sets
l. The supplier shall carry out regular testing of the environment using 3rd party (pen testing)
m. The Supplier shall carry out robust JLM processes and reviews
n. The Supplier shall ensure that all systems administrators are strongly authenticated - conforming NIST 800-63B AAL2 guidelines
o. The Supplier shall ensure controls are in place to detect unusual queries, attempted large scale exports of data or administrator access to data raise an alert. Furthermore, that these controls are regularly tested and an established procedure to investigate the alerts is in place.
p. The Supplier shall assist controllers in the compliance with Freedom of Information requests where necessary
q. The Supplier shall ensure, where necessary, that opted out data is separated from non-opted out data prior to secondary use.
r. The Supplier shall support the removal or secure hiding of information that can be identified or could be reidentified.
s. The Supplier must implement a full and robust audit functionality which supports the ability for NHS Platforms and data controllers to understand action taken following the who, what, why, when and where principles of data access/management.
t. Individual DPIA's shall be completed for each use case within the Data Platform and the Supplier will shall be required to assist in the process of completing to the necessary IG documentation and adhere to the approved decisions taken within the documentations.
u. Development access to non-production environments outside of the UK, must be formally agreed with the NHSE and be carried out within the European Economic Area (EEA)/ European Union (EU) regions only. Exceptions to this must be formally agreed with NHSE. These development environments must not contain any patient data.
v. An NHS England approved scanning tool must be used by the Supplier to conduct the vulnerability assessment and must be monitored by approved personnel.
w. The Supplier shall provide a report 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.

x. The Supplier shall monitor for potential new threats, vulnerabilities or exploitation techniques that could affect the Solution, and are proactively assessed and corrective action is taken.
y. The Supplier shall implement and enforce Role-Based Access Control (RBAC) or Purpose Based Access Control (PBAC) at different levels of the system, according to NHSE IAM requirements.
z. The Supplier shall demonstrate that their solution complies with DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services to provide consistent and standardised user verification authentication across England.
aa. The Suppliers NHS-PET solution shall integrate with one or more of the following NHS Identity and Access Management (IAM) solutions:
    1. NHS Care Identity service 2 (NHS CIS2)
    2. NHS.net AD
    3. Azure AD
    4. Okta
bb. The Supplier shall provide the capability to allow NHS organisations to monitor the Solution, via integration into the NHS CSOC protective monitoring function.
cc. The Supplier and its Solution shall provide documentation of DR/BC plans for each.
dd. The Supplier and its Solution shall provide evidence of DR/BC testing and the corresponding results for itself and the Solution.
ee. Suppliers shall adhere to the 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.
ff. The Supplier shall align with NHS England's Public Key Infrastructure (PKI) policies and procedures which may include use of current NHS England certificates
gg. The suppliers shall be required to ensure system administrator and operator activities are logged, and the log files are protected against tamper and regularly reviewed.
hh. The suppliers shall be required to be tested against the OWASP top 10 web application vulnerabilities. Application Security Verification Standard (ASVS) level 2 must be achieved.
ii. NHS England Organisations shall regularly monitor, review and audit the Supplier service delivery.
jj. The Successful Supplier will be required to provide named individuals for each of the defined roles:
    - Executive Directors
    - The Senior Information Risk Owner
    - Information Asset Owners
    - Information Governance Team
    - Line Managers
    - All staff

3 Lawful Basis for Processing

3.1 Data Protection Act 2018 / UKGDPR14

Under the Data Protection Act 2018 and UK GDPR, the "first data protection principle": requires that all the processing of all personal data is completed lawfully, fairly and in a transparent manner. If no lawful basis applies to processing, it will be unlawful and in breach of the first principle. Individuals have the right to have data which has been processed unlawfully erased. Lawful basis for processing is one of several conditions for processing to meet UK Data Protection requirements.

The Successful NHS-PET Supplier will be categorised as a processor and as such will be given specific processing instructions by the identified controllers.

Health data is one of the Special Category data sets that would require both an Article 6 and Article 9 UK GDPR lawful basis to be applied. 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):** processing is necessary for compliance with a legal obligation
- **Article 6(1)(e):** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- **Article 9(2)(h):** processing is necessary for the purposes of preventative or occupational medicine...medical diagnosis, the provision of health or social care or the management of health or social care systems and services…'
- **Article 9(2)(i):** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...
- **Article 9(2)(j):** processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes...
- **Data Protection Act 2018, Schedule 1:** Part 1 describes conditions for processing personal data for health, public health, social care and research purposes; Part 2 sets out the conditions for processing personal data on the grounds of substantial public interest
- **Consent** may be used as a lawful basis for research when the above lawful bases cannot be applied:
    - **Article 6(1)(a):** the data subject has given consent for the processing
    - **Article 9(2)(a)**: the data subject has given explicit consent to the processing
        - There are two types of consent: implied consent and explicit consent. To process healthcare data on the basis of consent, you must use explicit consent as required in Article 9(2)(a). The NHS provides the following description: "***Explicit consent*** *- if confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be obtained in writing, verbally or through another form of communication such as sign language.*"

Source: *https://www.nhsx.nhs.uk/information-governance/guidance/consent-and-confidential-patient-information/*

The identified lawful basis will form part of the processing instructions.

3.2 Common Law Duty of Confidentiality (CLDOC)15

The common law duty of confidentiality is a broad principle of law that a person who receives information from another party in confidence cannot take advantage of it. That person must not make use of it to the prejudice of the person who gave the information without obtaining his/her consent. For direct care purposes it is generally the case that sharing of patient data for direct care purposes satisfies the CLDOC.

The Successful NHS-PET Supplier will be required to apply measures proportionate to the data, to ensure the maintenance of the CLDOC.

The successful supplier will be required to comply with the specific lawful basis for each data flow as defined by the data controller.

4 Incident Management

4.1 Notification of Near misses and Breaches

The successful supplier will be required to notify NHS England via the route to be defined by NHSE as well as the local controlling organisation of all near misses, suspected breaches and breaches that impact their services and data with 2 hours of the incident being identified. Suppliers will be required to adhere to the NHS-PET Breach Management Procedure which will be provided after contract award.

4.2 Implementing Lessons Learnt

The supplier shall be required to implement critical changes in response to incidents and outages that have occurred. Bug and incident fixes will be developed to address the fault or defect that was the root cause and to regression test to the fixes to ensure there is no compromise to existing functionality.

SCHEDULE 4

SUPPLIER SOLUTION

[Redacted under FOIA s41, Confidential information]

SCHEDULE 5

CHARGES & INVOICING

PART A: PRICING

1 PRICING MECHANISMS

1.1 Milestone Payments shall be as set out in Annex 1 to this Schedule.

1.2 Service Charges shall be calculated using the pricing mechanisms specified in Annex 2 to this Schedule and as more particularly set out in this Schedule.

Price Catalogue:

1.3 Where Annex 2, Part A (Price Catalogue) to this Schedule indicates that a Service Charge is to be calculated by reference to a volume based charging mechanism, the relevant Service Charges shall be calculated on the basis of the unit costs set out against that Service.

Rate Card:

1.4 Where Annex 2, Part B (Rate Card) to this Schedule indicates that a Service Charge is to be calculated by reference to the rate card, the relevant Service Charges shall be calculated on the basis of the rates set out against that Service.

PART B: CHARGING MECHANISMS

1 MILESTONE PAYMENTS

1.1 Subject to the provisions of Paragraph 1.3 of Part C in relation to the deduction of Delay Payments, on the Achievement of a Milestone the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Milestone.

1.2 Each invoice relating to a Milestone Payment shall be supported by a Milestone Achievement Certificate.

2 SERVICE CHARGES

2.1 Each Service to which a Service Charge relates shall commence on the Achievement of the Milestone after which such Services are to commence.

2.2 Service Charges shall be invoiced by the Supplier for each Service Period in arrears in accordance with the requirements of Part D.

2.3 If a Service Charge is to be calculated by reference to a fixed price pricing mechanism and the relevant Service:

(a) commences on a day other than the first day of a month; and/or

(b) ends on a day other than the last day of a month,

the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.

2.4 Any Service Credits that accrue during a Service Period shall be deducted from the Service Charges payable for the next following Service Period. An invoice for a Service Charge shall not be payable by the Authority unless all adjustments (including Service Credits) relating to the Service Charges for the immediately preceding Service Period have been agreed.

PART C: ADJUSTMENTS TO THE CHARGES

1 DELAY PAYMENTS

1.1 If a Key Milestone has not been Achieved on or before the relevant Milestone Date, the Supplier shall pay a Delay Payment to the Authority in respect of that Key Milestone. Delay Payments shall accrue, subject to the Delay Payments Cap:

(a) at the daily rate (the "**Delay Payment Rate**") determined in accordance with Paragraph 1.2;

(b) from (but excluding) the relevant Milestone Date to (and including) the date on which the Key Milestone is Achieved; and

(c) on a daily basis, with any part day's Delay counting as a day.

1.2 Where a Delay Payment is payable in respect of a Key Milestone, the Delay Payment Rate shall be the greater of [Redacted under FOIA s43, Commercial interests].

1.3 The Supplier shall, within 5 Working Days of each Delay Payment becoming payable, pay to the Authority in cleared funds on account of the relevant Delay Payment.

1.4 Any amounts paid to the Authority pursuant to Paragraph 1.3 shall not be refundable to the Supplier in any circumstances.

1.5 The Parties agree that Delay Payments calculated in accordance with the applicable Delay Payment Rates are in each case a genuine pre-estimate of the Losses which the Authority will incur as a result of any failure by the Supplier to Achieve the relevant Key Milestone by the Milestone Date. Delay Payment Rates are stated exclusive of VAT.

1.6 The Delay Payment in respect of a Key Milestone (net of any Delay Payment made in respect of that Key Milestone pursuant to Paragraph 1.3) shall be shown as a deduction from the amount due from the Authority to the Supplier in the next invoice due to be issued by the Supplier after the date on which the relevant Key Milestone is Achieved or the Delay Payments Cap is reached (as the case may be). If the relevant Key Milestone is not Achieved by the date on which the Delay Payments Cap is reached or exceeded ("**Delay Payments Cap Reached or Exceeded Date**") and no invoice is due to be issued by the Supplier within 10 Working Days of Delay Payments Cap Reached or Exceeded Date, then the Supplier shall within 10 Working Days of expiry of the Delay Payments Cap Reached or Exceeded Date:

(a) issue a credit note to the Authority in respect of the total amount of the Delay Payment in respect of the Key Milestone (net of any payment made in respect of the Key Milestone pursuant to Paragraph 1.3); and

(b) pay to the Authority as a debt a sum equal to the total amount of the Delay Payment in respect of the Key Milestone together with interest on such amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.

1.7 The Parties agree that Delay Payments will be capped at an amount equal to [Redacted under FOIA s43, Commercial interests] ("**Delay Payments Cap**").

2 SERVICE CREDITS

2.1 Service Credits shall be calculated by reference to the number of Service Points accrued in any one Service Period pursuant to the provisions of Schedule 8 (Performance Levels).

2.2 For each Service Period:

(a) the Service Points accrued shall be converted to a percentage deduction from the Service Charges for the relevant Service Period on the basis of one point equating to a 0.5% deduction in the Service Charges; and

(b) the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:

$$SC = TSP \times x \times AC$$

where:

SC is the total Service Credits for the relevant Service Period;

TSP is the total Service Points that have accrued for the relevant Service Period;

X is [Redacted under FOIA s43, Commercial interests]; and

AC is the total Services Charges payable for the relevant Service Period (prior to deduction of applicable Service Credits).

2.3 The liability of the Supplier in respect of Service Credits shall be subject to the Service Credit Cap provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Points in excess of such financial limit in accordance with the provisions of Schedule 8 (Performance Levels).

2.4 Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services actually received and are stated exclusive of VAT.

2.5 Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

3 INDEXATION

3.1 From the commencement of each Extension Period (where triggered by the Authority in accordance with Clause 4.3 (Term)) the Supplier may adjust the Service Charges for the remainder of that Extension Period in accordance with Paragraph 3.2 ("**Indexation Adjustment**").

3.2 The Indexation Adjustment shall be determined by multiplying the relevant Service Charges by the percentage increase to the Consumer Price Index as published by the Office for National Statistics from time to time (or failing such publication, such other index as the Parties may agree most closely resembles that index) published for the 12 months ending on the 31 January immediately preceding the relevant adjustment date.

3.3 Except as set out in this Paragraph 3, neither the Service Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.

PART D: INVOICING AND PAYMENT TERMS

1 SUPPLIER INVOICES

1.1 The Supplier shall:

(a) comply with the requirements of the Authority's e-invoicing system;

(b) prepare and provide to the Authority for approval of the format a template invoice within 10 Working Days of the Effective Date which shall include, as a minimum the details set out in Paragraph 1.2 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and

(c) make such amendments as may be reasonably required by the Authority if the template invoice outlined in (b) is not approved by the Authority.

1.2 The Supplier shall ensure that each invoice is submitted in the correct format for the Authority's e-invoicing system, or that it contains the following information:

(a) the date of the invoice;

(b) a unique invoice number;

(c) the Service Period or other period(s) to which the relevant Charge(s) relate;

(d) the correct reference for this Contract;

(e) the reference number of the purchase order to which it relates (if any);

(f) the dates between which the Services subject of each of the Charges detailed on the invoice were performed;

(g) a description of the Services;

(h) the pricing mechanism used to calculate the Charges;

(i) any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;

(j) the total Charges gross and net of any applicable taxes;

(k) details of any Service Credits or similar deductions that shall apply to the Charges detailed on the invoice;

(l) a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries;

(m) the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number); and

(n) where the Services have been structured into separate Service lines, the information at (a) to (m) of this Paragraph 1.2 shall be broken down in each invoice per Service line.

1.3 The Supplier shall invoice the Authority in respect of Services in accordance with the requirements of Part B. The Supplier shall first submit to the Authority a draft invoice setting out the Charges payable. The Parties shall endeavour to agree the draft invoice within 5 Working Days of its receipt by the Authority, following which the Supplier shall be entitled to submit its invoice.

1.4 The Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.

1.5 All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.

1.6 The Authority shall regard an invoice as valid only if it complies with the provisions of this Part D. Where any invoice does not conform to the Authority's requirements set out in this Part D, the Authority shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.

1.7 If the Authority fails to consider and verify an invoice in accordance with Paragraphs 1.3 and 1.6, the invoice shall be regarded as valid and undisputed for the purpose of Paragraph 2.1.

2 PAYMENT TERMS

2.1 Subject to the relevant provisions of this Schedule, the Authority shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.

2.2 Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

ANNEX 1

MILESTONE PAYMENTS

[Redacted under FOIA s43, Commercial interests]

ANNEX 2

SERVICE CHARGES

PART A – PRICE CATALOGUE

[Redacted under FOIA s43, Commercial interests]

PART B – RATE CARD

Rate Card (Onshore)							
Maximum day rate for each SFIA grade							
SFIA Skills Categories and levels version 8 (please click on this link for details of grades)							
SFIA Grade	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Rate	[Redacted under FOIA s43, Commercial interests]						

SCHEDULE 6

IMPLEMENTATION PLAN

[Redacted under FOIA s43, Commercial interests]

SCHEDULE 7

MILESTONES

[Redacted under FOIA s43, Commercial interests]

SCHEDULE 8

PERFORMANCE LEVELS

Part A: Performance Indicators and Service Credits

1 INTERPRETATION

1.1 In this Schedule the following expressions shall have the meanings ascribed in the table below:

incident	means an event experienced in relation to the Services that represents a failure of the Services to meet the requirements of the Service Description, the Supplier Solution and/or the Key Performance Indicators (as applicable);
response	means the actions to be taken by the Supplier when it is notified of, or becomes aware of, an incident, and "**Respond**" shall be construed accordingly;
resolve	means in relation to an incident either: (a) the root cause of the incident has been removed and the Services are being provided in accordance with the requirements of the Service Description, the Supplier Solution and/or the Key Performance Indicators (as applicable); or (b) the Authority has been provided with a workaround in relation to the incident deemed acceptable by the Authority (acting reasonably), and "**resolution**" and "**resolved**" shall be construed accordingly;
severity	means the ranking that defines the significance of an incident which is used to prioritise its treatment and severity definitions as set out under the heading "KPI Failure Range" in the table in Annex 1 to this Schedule; and
workaround	means a solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available.

1.2 Any terms used in Annex 1 to this Schedule but not defined in this Schedule, Annex 1 to this Schedule or elsewhere in this Contract, shall be interpreted in accordance with the Information Technology Infrastructure Library (ITIL) Glossary, as updated from time to time.

2 PERFORMANCE INDICATORS

2.1 Annex 1 to this Schedule sets out the Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

2.2 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 Annex 1.

2.3 Subject to Clause 19.1 (Supplier Relief Due to Authority Cause) Service Points, and therefore Service Credits, shall accrue for any KPI Failure in respect of a Critical KPI and shall be calculated in accordance with Paragraphs 3, 4 and 5.

3 SERVICE POINTS

3.1 No Service Points shall accrue to the Supplier in respect of any KPI Failure in respect of any Standard KPI.

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

3.3 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Critical KPI, Service Points shall accrue to the Supplier in respect of that Critical KPI as set out in Paragraph 3.4. Service Points shall continue to accrue in respect of a KPI Failure until such time as the Target Performance Level for the relevant Critical KPI is met or exceeded.

3.4 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 depending on whether the KPI Failure is a Minor KPI Failure, a Serious KPI Failure or a Severe KPI Failure, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 4.2 shall apply.

4 REPEAT KPI FAILURES AND RELATED KPI FAILURES

Repeat KPI Failures

4.1 If a KPI Failure occurs in respect of the same Critical KPI in any two consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a "**Repeat KPI Failure**".

4.2 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 x 2

where:

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

P = the applicable number of Service Points for that KPI Failure as set out in Annex 1 depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Serious KPI Failure, a Severe KPI Failure or a failure to meet the KPI Service Threshold.

Worked example based on the following Service Points regime for Service Availability:

Service Availability Severity Levels		Service Points
Target Performance Level:	99.90%	0
Minor KPI Failure:	99.5% - 99.89%	1
Serious KPI Failure:	99.00% - 99.49%	2
Severe KPI Failure:	98.00% - 98.99%	3

KPI Service Threshold:	below 98%	4

Example 1:

If the Supplier achieves Service Availability of 99.5% in a given Measurement Period, it will incur a Minor KPI Failure for Service Availability in that Measurement Period and accordingly accrue 1 Service Point. If, in the next Measurement Period, it achieves Service Availability of 98.5%, it will incur a Severe KPI Failure and accordingly accrue 3 Service Points, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 6 Service Points for the failure (i.e. SP = 3 x 2). If in the next Measurement Period it achieves Service Availability of 98.5%, the Supplier will again incur 6 Service Points.

Example 2:

If the Supplier achieves Service Availability of 98.5% in a given Measurement Period, it will incur a Severe KPI Failure for Service Availability in that Measurement Period and accordingly accrue 3 Service Points. If, in the next Measurement Period, it achieves Service Availability of 99.5%, it will incur a Minor KPI Failure and accordingly accrue 1 Service Point, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 2 Service Points for the failure (i.e. SP = 1 x 2). If in the next Measurement Period it achieves Service Availability of 98.5%, the Supplier will incur 6 Service Points.

Related KPI Failures

4.3 If any specific Key Performance Indicators refer to both Service Availability and Incident Management Response Times, the Incident Management Response Times achieved by the Supplier for any period of time during a Service Period during which the relevant Service or element of a Service is determined to be Non-Available shall not be taken into account in calculating the average Incident Management Response Times over the course of that Service Period. Accordingly, the Supplier shall not incur any Service Points for failure to meet Incident Management Response Times in circumstances where such failure is a result of, and the Supplier has already incurred Service Points for, the Service being Non-Available.

5 SERVICE CREDITS

5.1 Schedule 5 (Charges & Invoicing) sets out the mechanism by which Service Points shall be converted into Service Credits.

5.2 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.

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 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**").

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 KPI Failures that occurred during the Service Period;

(c) the severity level of each KPI Failure which occurred during the Service Period and whether each KPI Failure which occurred during the Service Period fell below the KPI Service Threshold;

(d) which KPI 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 Contract;

(l) Social Value Obligations (as applicable);

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

Information in respect of previous Service Periods

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

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

(p) 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; and

Information in respect of the next Quarter

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

1.3 The Performance Monitoring Report shall be reviewed and their contents agreed by the Parties at the next performance review meeting held in accordance with Paragraph 1.4.

1.4 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring 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.

1.5 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 help desk 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. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. 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 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each KPI Effective Date and the calculations of the amount of Service Credits for any specified period.

2.3 The Supplier shall ensure that the Performance Monitoring Report (as well as historic Performance Monitoring Reports) 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 on-line and are capable of being printed.

3 PERFORMANCE VERIFICATION

3.1 The Authority reserves the right to verify the Availability of the solution and/or the Services and the Supplier’s performance under this Contract against the Key Performance Indicators including by sending test transactions through the solution or otherwise.

ANNEX 1

KEY PERFORMANCE INDICATORS

[Redacted under FOIA s43, Commercial interests]

SCHEDULE 9

REPORTING AND GOVERNANCE

In this Schedule, the following definitions shall apply:

Board Member	means the initial persons appointed by the Authority and Supplier to the Boards as set out in ANNEX 1 and any replacements from time to time agreed by the Parties in accordance with Paragraph 2.3;
Boards	means the Service Management Board, Programme Board, Technical Board and Risk Management Board and "**Board**" shall mean any of them;
Project Managers"	means the individuals appointed as such by the Authority and the Supplier in accordance with Paragraph 3;
Risk Management Board	means the body described in Paragraph 6;
Service Management Board	means the body described in Paragraph 3; and
Technical Board	means the body described in Paragraph 5.

1. MANAGEMENT OF THE SERVICES

1.1 The Supplier and the Authority shall each appoint a representative for the purposes of this Contract through whom the Services shall be managed at a day-to-day:

- **Supplier Representative:** [Redacted under FOIA s40, Personal information]
- **Authority Representative:** [Redacted under FOIA s40, Personal information]

1.2 Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2. BOARDS

Establishment and structure of the Boards:

2.1 The Boards shall be established by the Authority for the purposes of this Contract on which both the Supplier and the Authority shall be represented.

2.2 In relation to each Board, the:

2.2.1 Authority Board Members;

2.2.2 Supplier Board Members;

2.2.3 frequency that the Board shall meet (unless otherwise agreed between the Parties);

2.2.4 location of the Board's meetings; and

2.2.5 planned start date by which the Board shall be established,

shall be as set out in ANNEX 1.

2.3 In the event that either Party wishes to replace any of its appointed Board Members, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority Board Member has at all times a counterpart Supplier Board Member of equivalent seniority and expertise.

Board meetings:

2.4 Each Party shall ensure that its Board Members shall make all reasonable efforts to attend Board meetings at which that Board Member's attendance is required. If any Board Member is not able to attend a Board meeting, that person shall use all reasonable endeavours to ensure that:

2.4.1 a delegate attends the relevant Board meeting in his/her place who (wherever possible) is properly briefed and prepared; and

2.4.2 that he/she is debriefed by such delegate after the Board Meeting.

2.5 A chairperson shall be appointed by the Authority for each Board as identified in ANNEX 1. The chairperson shall be responsible for:

2.5.1 scheduling Board meetings;

2.5.2 setting the agenda for Board meetings and circulating to all attendees in advance of such meeting;

2.5.3 chairing the Board meetings;

2.5.4 monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings;

2.5.5 ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within seven Working Days after the Board meeting; and

2.5.6 facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.

2.6 Board meetings shall be quorate as long as at least two representatives from each Party are present.

2.7 The Parties shall ensure, as far as reasonably practicable, that all Boards shall as soon as reasonably practicable resolve the issues and achieve the objectives placed before them. Each Party shall endeavour to ensure that Board Members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.

3. ROLE OF THE SERVICE MANAGEMENT BOARD

3.1 The Service Management Board shall be responsible for the executive management of the Services and shall:

3.1.1 be accountable to the Programme Board for comprehensive oversight of the Services and for the senior management of the operational relationship between the Parties;

3.1.2 report to the Programme Board on significant issues requiring decision and resolution by the Programme Board and on progress against the high level Implementation Plan;

3.1.3 receive reports from the Project Managers on matters such as issues relating to delivery of existing Services and performance against Key Performance Indicators, progress against the Implementation Plan and possible future developments;

3.1.4 review and report to the Programme Board on service management, co-ordination of individual projects and any integration issues;

3.1.5 deal with the prioritisation of resources and the appointment of Project Managers on behalf of the Parties;

3.1.6 consider and resolve Disputes (including Disputes as to the cause of a Delay or the performance of the Services) in the first instance and if necessary escalate the Dispute to the Programme Board;

3.1.7 be the forum at which the Supplier updates the Authority on its progress in respect of its obligation to innovate and continuously improve the Services; and

3.1.8 develop operational/supplier relationship and develop and propose the relationship development strategy and ensure the implementation of the same.

4. ROLE OF THE PROGRAMME BOARD

4.1 The Programme Board shall:

4.1.1 provide senior level guidance, leadership and strategy for the overall delivery of the Services;

4.1.2 be the point of escalation from the Technical Board and the Service Management Board; and

4.1.3 carry out the specific obligations attributed to it in Paragraph 4.2.

4.2 The Programme Board shall:

4.2.1 ensure that this Contract is operated throughout the Term in a manner which optimises the value for money and operational benefit derived by the Authority and the commercial benefit derived by the Supplier;

4.2.2 receive and review reports from the Service Management Board and review reports on technology, service and other developments that offer potential for improving the benefit that either Party is receiving, in particular value for money;

4.2.3 determine business strategy and provide guidance on policy matters which may impact on the implementation of the Services or on any optional Services; and

4.2.4 authorise the commissioning and initiation of, and assess opportunities for, optional Services.

5. ROLE OF THE TECHNICAL BOARD

5.1 The Technical Board shall be accountable to the Programme Board for oversight of the technology used in the Supplier Solution and ensuring that technological choices are made to maximise the long term value of the Supplier Solution as a business asset of the Authority.

5.2 The Technical Board shall:

5.2.1 ensure compliance with the Standards;

5.2.2 grant dispensations for variations from such compliance where appropriate;

5.2.3 assure the coherence and consistency of the systems architecture for the Supplier Solution;

5.2.4 monitor developments in new technology and reporting on their potential benefit to the Services;

5.2.5 provide advice, guidance and information on technical issues; and

5.2.6 assure that the technical architecture of the Supplier Solution is aligned to the Service requirements and has sufficient flexibility to cope with future requirements of the Authority.

6. ROLE OF THE RISK MANAGEMENT BOARD

6.1 The Risk Management Board shall identify and manage risks relating to the performance of the Services.

6.2 The Risk Management Board shall:

6.2.1 provide assurance to the Programme Board that risks are being effectively managed across the Services, including reporting the 'top 5' risks to the Programme Board on a monthly basis;

6.2.2 identify the risks to be reported to the Programme Board via the regular risk reports;

6.2.3 identify risks relating to or arising out of the performance of the Services and provisional owners of these risks.

7. CONTRACT MANAGEMENT MECHANISMS

7.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Contract.

7.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Authority, processes for:

7.2.1 the identification and management of risks;

7.2.2 the identification and management of issues; and

7.2.3 monitoring and controlling project plans.

7.3 The risk reports shall be updated by the Supplier and submitted for review by the Risk Management Board.

8. ANNUAL REVIEW

8.1 An annual review meeting shall be held throughout the Term on a date to be agreed between the Parties.

8.2 The meetings shall be attended by the GM UKI Healthcare and Government of the Supplier and the Deputy Director of Data Management and Integration Services Programme of the Authority and any other persons considered by the Authority necessary for the review.

ANNEX 1: REPRESENTATION AND STRUCTURE OF BOARDS

Service Management Board

Authority Members of Service Management Board	[Redacted under FOIA s40, Personal information]
Supplier Members of Service Management Board	[Redacted under FOIA s40, Personal information]
Start Date for Service Management Board meetings	January 2024
Frequency of Service Management Board meetings	Monthly
Location of Service Management Board meetings	Hybrid with face to face option available at NHS England, Wellington House, London
Quorum (number of attendees from each of the Supplier and the Authority)	Two Authority members and Two Supplier members (each, including the Chairperson or Co-Chairperson)

Programme Board

Authority members of Programme Board	[Redacted under FOIA s40, Personal information]
Supplier members of Programme Board	[Redacted under FOIA s40, Personal information]
Start date for Programme Board meetings	January 2024
Frequency of Programme Board meetings	Monthly
Location of Programme Board meetings	Hybrid with face to face option available at NHS England, Wellington House, London
Quorum (number of attendees from each of the Supplier and the Authority)	Two Authority members (including the Chairperson or Co-Chairperson) and one Supplier member

Technical Board

Authority Members of Technical Board	[Redacted under FOIA s40, Personal information]
Supplier Members of Technical Board	[Redacted under FOIA s40, Personal information]
Start Date for Technical Board meetings	January 2024
Frequency of Technical Board meetings	Fortnightly

Location of Technical Board meetings	Hybrid with face to face option available at NHS England, Wellington House, London
Quorum (number of attendees from each of the Supplier and the Authority)	Two Authority members (including the Chairperson or Co-Chairperson) and Supplier member(s) will attend as required by the Authority. Supplier members' attendance is not required to quorate this Board meeting.

Risk Management Board

Authority Members for Risk Management Board	[Redacted under FOIA s40, Personal information]
Supplier Members for Risk Management Board	[Redacted under FOIA s40, Personal information]
Start Date for Risk Management Board meetings	January 2024
Frequency of Risk Management Board meetings	Fortnightly
Location of Risk Management Board meetings	Hybrid with face to face option available at NHS England, Wellington House, London
Quorum (number of attendees from each of the Supplier and the Authority)	Two Authority members (including the Chairperson or Co-Chairperson) and one Supplier member

SCHEDULE 10

DISPUTE RESOLUTION PROCEDURE

1. If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

2. If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Paragraphs 3-5 of this Schedule 10.

3. Unless the Authority refers the Dispute to arbitration using Paragraph 4 of this Schedule 10, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

   (a) determine the Dispute;
   (b) grant interim remedies; and/or
   (c) grant any other provisional or protective relief.

4. The Supplier agrees that the Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

5. The Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Paragraph 3 of this Schedule 10, unless the Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Paragraph 4 of this Schedule 10.

6. The Supplier cannot suspend the performance of this Contract during any Dispute.

SCHEDULE 11

DATA PROCESSING AGREEMENT

The Schedule of Processing will be set out as follows:

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: [Redacted under FOIA s40, Personal information]
   b) Caldicott Guardian are: ……
   c) Chief Information Security Officer are: ……
   d) Senior Information Risk Officer are: [Redacted under FOIA s40, Personal information]
2) The contact details of the Processor:
   a) Data Protection Officers are: [Redacted under FOIA s40, Personal information] and [Redacted under FOIA s40, Personal information]
   b) Caldicott Guardian are: [Redacted under FOIA s40, Personal information]
   c) Chief Information Security Officer are: [Redacted under FOIA s40, Personal information]
   d) Senior Information Risk Officer are: [Redacted under FOIA s40, Personal information]
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
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. Administration of user (staff) data in order to administer use of the Data Platform and NHS-PET Solution and for the purposes above.

Description	Details
	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 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 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[1]
Controller for each Category of Personal Data	Is the Controller referred to in the Agreement for all Personal Data categories
Processor	
Subprocessors	
Commencement of Processing	
Product Name	

[1] Update as appropriate.

Description	Details[1]
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	{●}
Categories of Data Subject	{●}
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 [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	{●}

The Data Processing Schedule shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of the Data Processing Schedule shall be with the Controller at its absolute discretion.

The Data Processing Schedule shall also record the Supplier's compliance with the Authority's information governance framework document for the Programme ("IG Framework") as updated by the Authority and provided to the Supplier from time to time.

SCHEDULE 12

SERVICE REQUEST PROCEDURE

- Unless agreed otherwise by the Parties, the Authority Representative shall submit a draft Service Request, setting out the Configuration Services required, to the Supplier Representative by email.

- The Supplier shall arrange a date for a meeting between the Supplier and the Authority to discuss the draft requirement for Configuration Services within ten (10) Working Days of the date of such email (or sooner where requested by the Authority).

- The Authority and the Supplier shall discuss and agree the: (i) scope and duration of; and (ii) Charges for, such Configuration Services and shall prepare a final Service Request Form which shall be substantially in the form set out below.

- Unless agreed otherwise by the Parties, the Authority Representative and the Supplier Representative shall be the signatories to the agreed Service Request.

- The terms of the Agreement shall be incorporated into each Service Request Form once signed. The approved and signed Service Request Form shall come into force on the date of the last signature.

Service Request Form

This Service Request Form incorporates the terms of the agreement between the Authority and the Supplier dated [DATE OF AGREEMENT] 2023 ("Agreement").	
Date of submission: [DATE]	
Contact Information (including contact details – email & telephone):	
Authority Representative:	[NAME] [EMAIL] [PHONE NUMBER]
Supplier Representative:	[NAME] [EMAIL] [PHONE NUMBER]
Details of Configuration Services	
Scope of Configuration Services:	[INSERT DETAILS OF REQUIREMENT]
Configuration Services commencement date:	[DATE]
Configuration Services completion date:	[DATE]
Charges (calculated in accordance with Schedule 5 of the Agreement)	£[NUMBER] exc. VAT

Signatures	
On behalf of the Authority:	Signature:
	Name:
	Date:
On behalf of the Supplier:	Signature:
	Name:
	Date:

SCHEDULE 13

INSURANCE REQUIREMENTS

The Supplier shall ensure that it maintains the policy or policies of insurance referred to below during the Term:

Policy	Coverage (in each case for a single event or a series of related events and in the aggregate per annum)
Professional indemnity insurance	[Redacted under FOIA s41, Confidential information]
Public liability insurance	[Redacted under FOIA s41, Confidential information]
Employers' liability insurance	[Redacted under FOIA s41, Confidential information]
Product liability insurance	[Redacted under FOIA s41, Confidential information]

SCHEDULE 14

KEY PERSONNEL

[Redacted under FOIA s40, Personal information]

SCHEDULE 15

KEY SUBCONTRACTORS

Key subcontractor	Establishment	Subprocessor	Scope	Location of processing
Amazon Web Services EMEA Sarl	**Luxembourg**	**Yes**	**Cloud hosting and infrastructure**	**UK**
Bridewell Consulting Limited	**UK**	**Yes**	**Security, threat management & incident response services**	**UK**

SCHEDULE 16

DIGITAL & DATA ACADEMY

1. INTRODUCTION

1.1 The Parties agree to collaborate in order to achieve the following objectives:

1.1.1 the co-ordination of their training and recruitment efforts having regard to the workforce profile desirable for NHS Bodies using the Services, including co-ordination with other relevant suppliers of services to the Authority ("**Digital Suppliers**");

1.1.2 the creation of an apprenticeship scheme, or the alignment of the existing apprenticeship programmes of the Parties, aligned with usage of the Federated Data Platform; and

1.1.3 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 9 (Reporting & *Governance*).

3. APPRENTICESHIP SCHEMES

3.1 The Parties intend to co-ordinate their respective apprenticeship programmes in order to:

3.1.1 align and jointly plan apprentice recruitment;

3.1.2 co-ordinate and collaborate on apprentice programmes, including secondment and other learning arrangements;

3.1.3 collaborate on the procurement and management of training and education providers supporting apprenticeship programmes;

3.1.4 collaborate on setting up an infrastructure for training and development of apprentices;

3.1.5 establish ways of working and joint arrangements allowing for the HR management of apprentices on their apprenticeship programmes;

3.1.6 promote school and college engagement outside of the apprenticeship programmes; and

3.1.7 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:

3.2.1 collaborate on establishing requirements for the apprenticeship framework, based on occupational and professional standards, where necessary;

3.2.2 clearly define the roles and responsibilities of employers and apprentices;

3.2.3 develop training plans describing the required learning content and methods of learning and assessment;

3.2.4 identify or create appropriate academic, vocational or skills-related qualifications associated with relevant apprenticeship programmes;

3.2.5 invite the Supplier's subcontractors, as agreed with the Authority, to participate in achieving the objectives set out in this Schedule;

3.2.6 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

3.2.7 engage in discussions and collaborate with Digital Suppliers in pursuit of the purpose of the objectives set out above.

SCHEDULE 17

APPLICABLE SUPPLIER TERMS

As set out in the MOU forming part of Schedule 19

SCHEDULE 18

VARIATION FORM

Contract Details		
This Variation is between:	NHS England (**"the Authority"**); and IQVIA Limited (**"the Supplier"**)	
Contract name:	Privacy Enhancing Technology Services **("the Contract")**	
Contract reference number:	C228485	
Service Request reference:	N/A	
1. This Variation must be agreed and signed by both Parties and shall only be effective from the date it is signed by the Authority. 2. Words and expressions in this Variation shall have the meanings given to them in the Contract. 3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.		
Details of Proposed Variation		
Variation initiated by:		
Variation number:	V-[Atamis reference], VAR[xxx]	
Date variation is raised:		
Proposed variation:		
Reason for the variation:		
An Impact Assessment shall be provided within:		
Impact of Proposed Variation		
Likely impact of the proposed variation:		
Outcome of discussions over Proposed Variation		
Amendments to Contract / terms of Contract as varied:	[As set out in the Schedule]	
Financial variation:	Current Contract Value:	£
	Additional cost due to variation:	£
	New Contract value:	£
SIGNED BY the parties acting by their authorised representatives to indicate agreement to the terms of the Variation set out above		
Authority Signature		

Supplier Signature	

SCHEDULE 19

AUTHORITY USERS

1. INTRODUCTION

1.1 The Services are to be available to Authority Users.

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

2. MEMORANDA OF UNDERSTANDING

2.1 The Authority will enter into and maintain MoUs in a form not materially different from the form set out in the Annex to this Schedule with each Authority User provided access to the Services under this Agreement.

2.2 The Authority acknowledges that each MoU requires Authority User compliance with the Applicable Supplier Terms.

3. CHARGES FOR SERVICES

3.1 The Supplier acknowledges that:

3.1.1 the Authority is the contracting authority for Service provision and is responsible for payment of Charges;

3.1.2 the Authority assumes no liability for the acts or omissions of Authority Users; and

3.1.3 no further charges are payable in respect of Authority Users' use of Services other than those set out in this Agreement.

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 Authority Users or any NHS Bodies in relation to Services.

4. DATA PROCESSING

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

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

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

5. AUTHORITY USERS BENEFITTING FROM THE AGREEMENT

5.1 The Authority acknowledges that as third party beneficiaries of Services under the Agreement, use by Authority Users of the Services is subject to the terms and conditions of the Agreement, including its exclusions and limitations of liability, and compliance with the Applicable Supplier 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 Authority Users use the Services.

5.4 The Parties acknowledge that the limits on liability in Clause 9 of the Agreement apply to Supplier's liability to the Authority and any Authority User 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 Applicable Supplier Terms and any other agreements made between Supplier and the Authority, Authority Users or other third parties under or in connection with this Agreement.

Annex

Form of MoU

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 expensesincurred 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

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

20. THIRD PARTY BENEFIT

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, **t**his 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 .....

..... (Signature)

for and on behalf of **[*Controller*]**

..... (Date)

SIGNED by .....

..... (Signature)

for and on behalf of **[*Processor*]**

.....

(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
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.

5) 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]*
6) 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*]
7) The Processor shall comply with any further written instructions with respect to Processing by the Controller.
8) 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**[2]
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. 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

[2] Update as appropriate.

Description	Details[2]
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[3]
Controller for each Category of Personal Data	Is the Controller referred to in the Agreement for all Personal Data categories
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**	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.

[3] Update as appropriate.

Description	Details[3]
State law to preserve that type of data	
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	