Appendix 2B to the Connection Agreement

Connecting Party is Processor for and on behalf of NHS Digital as Controller: Special Terms

The terms set out in this Appendix 2B (**"Processor Terms"**) shall apply where it has been determined by the parties that the Connecting Party is acting as a Processor (i.e. for and on behalf of NHS Digital) in respect of Personal Data it Processes pursuant to this Connection Agreement.

The terms set out in this Appendix 2B govern only the Processing of Personal Data of which NHS Digital is Controller, for the Purpose. Processing of Personal Data carried out by the Connecting Party for the purposes of providing products or services to an End User Organisation, Individual End User or other third party shall be subject to and governed by separate data protection terms (Controller to Processor, Controller to Data Subject, Controller to Controller or joint Controller terms as appropriate) between the Connecting Party and the relevant End User Organisation, Individual End User or other third party.

1. In this Appendix:

   "Controller", "Data Subject", "Processor", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the meanings set out in the Data Protection Laws and **"Process"** shall be construed in accordance with the definition of **"Processing"**;

   "Caldicott Principles" means the six principles developed by Dame Fiona Caldicott for appropriate use of patient information, as amended from time to time;

   "Data Protection Laws" means applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including 'the General Data Protection Regulation' (**"GDPR"**) and the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, Supervisory Authorities and other applicable government authorities;

   "Data Security and Protection Toolkit" means the online self assessment tool and guidance managed by NHS Digital which reflects the National Data Guardian for Health and Care's data security standards, and enables organisations to measure their performance against such standards;

   "**EU Exit"** means the exit of the United Kingdom from the European Union;

   "ICO" means the UK's Information Commissioner's Office;

   "NHS Constitution" means the NHS Constitution for England as amended from time to time;

   "Restricted Country" means any country other than the United Kingdom;

   "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 or post-EU Exit by the UK's ICO;

2. The parties acknowledge that:

   2.1 where any Personal Data is Processed in connection with this Connection Agreement, the Connecting Party shall be acting as a Processor and NHS Digital as a Controller;

   2.2 the provisions of this Appendix 2B govern only the Processing of Personal Data of which NHS Digital is Controller, for the purposes of enabling the Connecting Party to access the Service(s); and

   2.3 Processing of Personal Data carried out by the Connecting Party for the purposes of providing products and services to an End User Organisation, Individual End User or other third party shall be subject to and governed by separate data protection terms between the Connecting Party and the relevant End User Organisation, Individual End User or other third party, and the Connecting Party shall ensure that such terms are in place.

3. Appendix 2A sets out the details of the Processing, as required by Article 28(3) of the GDPR, and reflects the only Processing which the Connecting Party is permitted to carry out pursuant to this Connection Agreement.

4. The Connecting Party shall ensure it has robust business continuity management plans and supporting procedures.

5. Insofar as any Personal Data of which NHS Digital is Controller is Processed pursuant to this Connection Agreement by the Connecting Party, its agents or subprocessors, the Connecting Party shall and shall procure that its agents and subprocessors shall:

5.1 not Process the Personal Data other than on the documented instructions of NHS Digital unless the Connecting Party is required to do otherwise by law. If it is so required the Connecting Party shall promptly notify NHS Digital before Processing the Personal Data, unless prohibited by law;

5.2 taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security commensurate to the risk, including inter alia as appropriate:

5.2.1 the pseudonymisation and encryption of the Personal Data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

5.2.3 the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident;

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and

5.2.5 NHS Digital's cyber security guidance and policy (where available) on the NHS Digital web site;

5.3 take reasonable steps to ensure the reliability and integrity of any Connecting Party personnel who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary in relation to this Connection Agreement in the context of that individual's duties to the Connecting Party, ensuring that all such individuals:

5.3.1 are aware of and comply with the Connecting Party's duties under this Appendix 2B;

5.3.2 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 NHS Digital or as otherwise permitted by this Connection Agreement;

5.3.3 are subject to user authentication and log on processes when accessing the Personal Data;

5.3.4 have undertaken appropriate training in relation to Data Protection Laws and in the use, care, protection and handling of the Personal Data; and

5.3.5 are subject to confidentiality undertakings with the Connecting Party that are in writing and are legally enforceable or subject to professional or statutory obligations of confidentiality;

5.4 Process the Personal Data in accordance with the Data Protection Laws (as applicable) and:

5.4.1 not do or permit anything to be done in performing its obligations under this Connection Agreement which might cause NHS Digital in any way to be in breach of the Data Protection Laws, to the extent that the Connecting Party is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations; and

5.4.2 immediately inform NHS Digital if, in its opinion, compliance with this Connection Agreement or compliance with any instruction received from NHS Digital infringes, or might reasonably be considered to infringe, the Data Protection Laws;

5.4.3 provide reasonable assistance to NHS Digital in relation to any data protection impact assessments and/or any prior consultations to the Supervisory Authority which are required, in each case solely in relation to Processing of the Personal Data by the Connecting Party on behalf of NHS Digital and taking into account the nature of the Processing and information available to NHS Digital;

5.4.4 notify NHS Digital immediately upon becoming aware of a Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach providing NHS Digital with sufficient information to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

b) communicate the name and contact details of the data protection officer or other relevant contact from whom more information may be obtained;

c) describe the likely consequences of the Personal Data Breach; and

d) describe the measures taken or proposed to be taken to address the Personal Data Breach;

5.4.5 cooperate with NHS Digital and take such steps as are directed by NHS Digital to assist in the investigation, mitigation and remediation of a Personal Data Breach;

5.4.6 not inform any third party of a Personal Data Breach, except as may be strictly required by applicable law, without first obtaining NHS Digital's prior written consent;

5.4.7 notify NHS Digital immediately if it:

a) receives any of the following requests from a Data Subject (or third party on their behalf): (i) a Data Subject access request; (ii) a request to rectify any inaccurate Personal Data; (iii) a request to have any Personal Data erased or blocked; (iv) a request to restrict the Processing of any Personal Data; (v) a request to obtain a portable copy of Personal Data, or to transfer such a copy to any third party; or (vi) an objection to any Processing of Personal Data;

b) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Laws;

c) receives any communication from a Supervisory Authority or any other regulatory authority in connection with the Personal Data Processed under this Connection Agreement; or

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

(each a "Relevant Communication");

5.4.8 taking into account the nature of the Processing, provide NHS Digital with full cooperation and assistance in relation to any Relevant Communications (whether received by the Connecting Party or NHS Digital directly) including:

a) provision of all data requested by NHS Digital within the timescale specified by NHS Digital in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a Data Subject;

b) where applicable, providing such assistance as is reasonably requested by NHS Digital to enable it to comply with the relevant request within the Data Protection Laws' statutory timescales; and

c) assistance as requested by NHS Digital with respect to any request from a Supervisory Authority, or any consultation by NHS Digital with a Supervisory Authority;

5.4.9 appoint and identify to NHS Digital a named individual within the Connecting Party to act as a point of contact for any enquiries from NHS Digital relating to the Personal Data;

5.4.10 not Process or otherwise transfer, or permit the transfer, of any Personal Data in or to any Restricted Country unless the transfer is required by EU, UK or member state law to which the Connecting Party is subject, and if this is the case, then the Connecting Party shall inform NHS Digital of that requirement before Processing the Personal Data, unless a law prohibits such information being provided on important grounds of public interest;

5.4.11 in respect of any Processing in, or transfer of Personal Data to any Restricted Country permitted in accordance with paragraph 5.4.10 above, the Connecting Party shall, when requested by NHS Digital, promptly enter into an agreement with NHS Digital including or on such provisions as the Standard Contractual Clauses and/or such variation as a regulator or NHS Digital might require. Such terms shall, in the event of any conflict, take precedence over those in this Appendix 2B and the Connecting Party shall comply with any reasonable instructions notified to it in advance by NHS Digital with respect to the transfer of Personal Data;

5.4.12 not authorise any subprocessor to Process the Personal Data other than with the prior written consent of NHS Digital. In all cases where a subprocessor is appointed, the Connecting Party shall:

a) notify NHS Digital in writing of the intended subprocessor and provide NHS Digital with full details of the Processing to be undertaken by the proposed subprocessor;

b) provide NHS Digital with such information regarding the subprocessor as NHS Digital may reasonably require;

c) include terms in the contract between the Connecting Party and the subprocessor which offer at least the same level of protection for the Personal Data as those set out in this Appendix 2B. Upon request, the Connecting Party shall provide a copy of its agreements with subprocessors to NHS Digital (which may be redacted to remove confidential commercial information not relevant to the requirements of this Appendix 2B);

d) carry out adequate due diligence on each subprocessor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Appendix 2B including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Data Protection Laws and provide evidence of such due diligence to NHS Digital where requested by NHS Digital or a Supervisory Authority;

e) insofar as that contract involves the Processing and/or transfer of Personal Data in or to any Restricted Country, ensure that (at NHS Digital's option): (i) the Standard Contractual Clauses are at all relevant times incorporated into the agreement between the Connecting Party and the subprocessors; or (ii) before the subprocessor first Processes the Personal Data, procure that it enters into an agreement incorporating the Standard Contractual Clauses with NHS Digital;

f) remain fully liable to NHS Digital for any failure by a subprocessor to fulfil its obligations in relation to the Processing of any Personal Data;

5.4.13 cease Processing the Personal Data immediately upon the end of any connection to use of Service(s) to which the Processing relates (the **"Relevant Date"**); and

5.4.14 as soon as reasonably practicable thereafter, at NHS Digital's option, either return, or securely and irrevocably delete from its systems (so that such Personal Data cannot be recovered or reconstructed), the Personal Data and any copies of it or of the information it contains and certify that all copies of the Personal Data have been deleted or returned in compliance with this paragraph within a reasonable time but in any event not later than 90 days after the Relevant Date.

6. The Connecting Party shall maintain complete and accurate records and information necessary to demonstrate compliance with this Appendix 2B, shall make all such records and information available to NHS Digital on request and allow for and contribute to audits, including inspections by NHS Digital or an independent auditor mandated by NHS Digital of its data processing facilities, procedures and documentation which relate to the Processing of Personal Data, in order to ascertain compliance with the terms of this Appendix 2B. The Connecting Party shall provide full cooperation to NHS Digital in respect of any such audit and shall at the request of NHS Digital, provide evidence of compliance with its obligations under this Appendix 2B, including but not limited to a written description of the technical and organisational security measures it has in place.

7. The Connecting Party warrants that it has and its agents, subprocessors and employees have the necessary legal authority in any country where any Processing of Personal Data is authorised take place under this Connection Agreement and undertakes to comply with any of the Data Protection Laws which are applicable in such country.

8. Without prejudice to any other provision of this Connection Agreement, NHS Digital may, on reasonable notice, request a detailed written description of the technical and organisational methods employed by the Connecting Party and its subprocessors for the Processing of Personal Data which shall be provided within 10 days of receipt of such written notice.

9. NHS Digital may, at any time on not less than 30 Working Days' notice, revise this Appendix 2B by replacing it with any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme.

10. The parties agree to take account of any guidance issued by a Supervisory Authority. NHS Digital may on not less than 30 Working Days' notice to the Connecting Party amend this Appendix 2B to ensure that it complies with any guidance issued by a Supervisory Authority.

11. The Connecting Party shall comply (and shall procure that all its contractors, subprocessors and agents comply) with the Data Security Protection Toolkit; abide by the Caldicott Principles; and not do anything which would cause NHS Digital or the End User Organisation to be in breach of the NHS Code or the NHS Constitution.

12. The Connecting Party shall comply with its obligations under the Network and Information Systems Regulations 2018 to the extent applicable to its performance of this Connection Agreement or provision of relevant products and services.

13. Should a Service require identity verification of an Individual End User the Connecting Party shall comply with the Identity Verification and Authentication Standards for Health and Care as set out or linked to on a Services Web Page.

14. The Connecting Party shall (and shall procure that all its contractors and subcontractors) comply with NHS Digital's cyber security guidance and policy (where available) as set out on the NHS Digital web site.

15. The Connecting Party shall ensure it has robust business continuity management plans and supporting procedures.

16. The Connecting Party shall indemnify NHS Digital, and keep NHS Digital indemnified, against damages, costs, claims, demands, expenses, professional costs, charges and/or monetary penalty notices arising from enforcement by a Supervisory Authority and/or assertion of rights by Data Subjects, arising from a breach by the Connecting Party of the Data Protection Laws and/or the data processing provisions set out in this Connection Agreement.