Appendix 2D to the Connection Agreement

Connecting Party as Controller (Independently or Jointly with Others): Special Terms

The terms set out in this Appendix 2D (**"Controller Terms"**) shall apply where it has been determined by the parties that the Connecting Party is acting as a separate and independent Controller (i.e. separate and independent from NHS Digital) in respect of Personal Data it Processes pursuant to this Connection Agreement. It is acknowledged that where the Connecting Party is acting as a Controller, it may be acting alone or as a joint Controller with the End User Organisation.

The terms set out in this Appendix 2D 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 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 (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;

"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.

2. The Connecting Party shall:

2.1 use the Personal Data solely for the Purpose;

2.2 Process the Personal Data at all times in accordance with the terms of this Connection Agreement and comply with the requirements of the Data Protection Laws in respect of its Processing;

2.3 maintain good information governance standards and practices, meeting or exceeding the Data Security and Protection Toolkit standards required of its organisation type; 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;

2.4 not share the Personal Data with any third party (other than the End User Organisation) without the prior written consent of NHS Digital;

2.5 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:

2.5.1 are aware of and comply with the Connecting Party's duties set out in this Appendix 2D;

2.5.2 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;

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

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

2.5.5 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;

2.6 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:

2.6.1 the pseudonymisation and encryption of the Personal Data;

2.6.2 the ability to ensure the on-going confidentiality, integrity, availability and resilience of Processing systems and services;

2.6.3 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;

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

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

2.7 unless otherwise agreed in writing with NHS Digital, cease Processing the Personal Data immediately upon expiry or termination of this Connection Agreement and 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 in compliance with this paragraph within a reasonable time but in any event not later than 90 days after termination or expiry.

2.8 identify a relevant legal basis for its Processing of the Personal Data and immediately notify NHS Digital if it no longer has a legal basis for Processing the Personal Data;

2.9 immediately notify any Personal Data Breach to NHS Digital as soon as the Connecting Party discovers such Personal Data Breach and provide such information and cooperation as may be required by NHS Digital;

2.10 inform NHS Digital immediately if it receives any communication from the ICO which relates to the Personal Data, unless explicitly prohibited from doing so by the ICO;

2.11 not Process or otherwise transfer or permit the transfer of any Personal Data in or to any Restricted Country without the prior written consent of NHS Digital 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. The Connecting Party shall ensure that any transfer made with the prior written consent of NHS Digital is permitted under, and complies with the requirements of, the Data Protection Laws; and

2.12 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.

3. 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 for the Processing of Personal Data which shall be provided within 10 days of receipt of such written notice.

4. In the event of any change in applicable law, including the Data Protection Laws, the Connecting Party shall take such steps (including agreeing to additional obligations and/or executing additional documents) as may be requested by NHS Digital to ensure that the sharing of the Personal Data with the Connecting Party and the Processing by the Connecting Party complies with applicable laws.

5. The Connecting Party shall maintain complete and accurate records and information necessary to demonstrate compliance with this Appendix 2D, 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 2D. 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 2D, including but not limited to a written description of the technical and organisational security measures it has in place.

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

7. 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 the terms of this Appendix 2D to ensure they comply with any guidance issued by a Supervisory Authority.

8. The Connecting Party shall comply (and shall procure that all its contractors and agents comply) with NHS Digital's Data Security Protection Toolkit.

9. 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 and provision of relevant product and services.

10. 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.

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

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

13. Appendix 2A sets out the details of the Processing and reflects the only Processing which the Connecting Party is permitted to carry out pursuant to this Connection Agreement.

14. 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, including this Appendix 2D.

15. Where the Connecting Party is acting as joint Controller with the End User Organisation or a third-party organisation e.g. a GP practice which receives the Connecting Party's products and services, the Connecting Party shall ensure that it complies with the requirements of Article 26 of the GDPR.