Appendix 2F to the Connection Agreement

Connecting Party as Joint Controller with NHS Digital (Connecting Party Lead): Special Terms

The terms set out in this Appendix 2E shall apply where it has been determined by the parties that the Connecting Party is acting as a joint Controller with NHS Digital in respect of Personal Data it Processes pursuant to this Connection Agreement.

The terms set out in this Appendix 2E govern only the Processing of Personal Data of which NHS Digital is joint 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 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 parties undertake to comply with the applicable Data Protection Laws in respect of their Processing of Personal Data as Controllers.

3. The parties agree that the Connecting Party shall:

   3.1 be the point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

   3.2 be responsible for the parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

   3.3 be responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Service(s) where consent is the relevant legal basis for that Processing; and

   3.4 make available to Data Subjects the essence of this Appendix 2E (and notify them of any changes to it) concerning the allocation of responsibilities as joint Controllers and its role as point of contact.

4. The Connecting Party shall make available in its public-facing privacy policy the information set out in paragraph 3 above, where such privacy policy must be readily available by hyperlink or otherwise on all of its public facing services and marketing.

5. Notwithstanding paragraphs 3 and 4, the parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Laws as against the relevant party as Controller.

6. Each of the parties undertakes that it shall:

   6.1 report to the other party at agreed intervals on:

      6.1.1 volumes of requests from Data Subjects to exercise rights under the GDPR;

6.1.2 any other requests, complaints or communications from Data Subjects relating to the other party's obligations under applicable Data Protection Laws;

6.1.3 any communications from the ICO or any other regulatory authority in connection with Personal Data; and

6.1.4 any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law;

6.2 notify the other immediately if it receives any request, complaint or communication made as referred to in paragraphs 6.1.1 to 6.1.4;

6.3 provide the other party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in paragraphs 6.1.1 to 6.1.4 to enable the other party to comply with the relevant timescales set out in the Data Protection Laws;

6.4 not disclose or transfer the Personal Data to any third party unless necessary for the performance of this Connection Agreement and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Connection Agreement or is required by law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party;

6.5 request from the Data Subject only the minimum information necessary to perform this Connection Agreement and treat such extracted information as confidential;

6.6 ensure that at all times it has in place appropriate technical and organisational measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

6.7 take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data.

7. Each party shall use its reasonable endeavours to assist the other to comply with any obligations under applicable Data Protection Laws and shall not perform its obligations under this Appendix 2E in such a way as to cause the other party to breach any of its obligations under applicable Data Protection Laws to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

8. Each party shall notify the other party promptly and without undue delay, and in any event within 24 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other party and its advisors with:

8.1 sufficient information and in a timescale which allows the other party to meet any obligations to report a Personal Data Breach under the Data Protection Laws;

8.2 all reasonable assistance and information to enable the other party to deal with the Personal Data Breach, including cooperation with Supervisory Authorities.

9. Each party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has been lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it were that party's own data, at its own cost with all possible speed.

10. The Connecting Party shall:

10.1 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 2E. 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 2E, including but not limited to a written description of the technical and organisational security measures it has in place;

10.2 ensure that is personnel:

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

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

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

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

10.2.5 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,

10.3 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;

10.4 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;

10.5 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

10.6 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.

11. Each party shall:

11.1 provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

11.2 maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Service(s), in accordance with the terms of Article 30 GDPR.

12. The parties shall take account of any guidance issued by a Supervisory Authority and, on not less than 30 Working Days' notice to the Connecting Party, NHS Digital may amend the terms of this Appendix 2E to ensure they comply with any guidance issued by a Supervisory Authority.

13. 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.

14. 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.

15. The Connecting Party shall comply (and shall procure that all its contractors and agents comply) with NHS Digital's 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.

16. 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 products and services.

17. 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.

18. 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.

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

20. 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.

21. 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 2E.