DAC beachcroft

Dated 12th April 2016

(1) **NHS BRENT CLINICAL COMMISSIONING GROUP**

- and -

(2) **APOLLO MEDICAL SOFTWARE SOLUTIONS LTD**

Data Processing Agreement

FINAL VERSION FOR ACCEPTANCE
UNCHANGED SINCE MARCH 10TH 2016

DAC Beachcroft LLP
100 Fetter Lane London EC4A 1BN UK
tel: +44 (0) 20 7242 1011 fax: +44 (0) 20 7831 6630
DX 45 London

Table of contents

Clause heading and number — Page number

THIS DATA PROCESSING AGREEMENT (this "**Agreement**") is made the day of 2016 (the "**Effective Date**")

BETWEEN:

(1) **NHS BRENT CLINICAL COMMISSIONING GROUP** of Wembley Centre for Health and Care, 116 Chaplin Road, HA0 4UZ ("**Host**") and

(2) **APOLLO MEDICAL SOFTWARE SOLUTIONS LIMITED** incorporated and registered in England and Wales with company registration number 0747031 whose registered office is I2 Mansfield Centre Office Suite 0:1 Hamilton Way, Oakham Business Park, Mansfield, NG18 5FB ("**Subcontractor**")

the Host and the Subcontractor each being a "**Party**" and together the "**Parties**" to this Agreement.

BACKGROUND:

(A) The Host has been appointed as host of the North West London Whole Systems Integrated Care (WSIC) data warehouse under an Information Sharing and Hosting Agreement dated 1 October 2014 (as amended from time to time) (the "**ISA**") between the Host and the Provider Partners.

(B) The Host has contracted with various Provider Partners for certain data extraction services. The Parties now wish to record the specific terms and conditions upon which Processing of Data is to be performed by the Subcontractor, which will supersede any earlier such terms in relation to Processing of Data.

(C) This agreement is not intended to affect the obligations of the Subcontractor to Provider Partners under any direct agreements to which the Host is not a party, and the obligations of the Subcontractor to the Host shall not be affected by any agreement between the Subcontractor and a Provider Partner or any other third party.

THE PARTIES AGREE as follows:

1. **SPECIFIC OBLIGATIONS OF THE SUBCONTRACTOR**

1.1 In the performance of its obligations under this Agreement, the Subcontractor shall cooperate with third parties in accordance with the Host's instructions from time to time.

1.2 The Subcontractor shall not:

1.2.1 do anything that may materially damage the reputation of a CCG Partner and/or any Provider Partner (and the Subcontractor acknowledges that the use of the Data for research purposes or for sale to third parties in act that may materially damage the reputations of the CCG Partners and the Provider Partners); or

1.2.2 make, or permit any person, company or other body to make, any public announcement concerning this Agreement without the Host's prior written consent, except as required by law, any governmental or regulatory authority (including any relevant securities exchange), or any court or other authority of competent jurisdiction.

2. **CONDITIONS OF PROCESSING**

2.1 Where the Subcontractor undertakes any Processing of Data (whether during the term of this Agreement or following termination), the Subcontractor shall:

2.1.1 only Process Data in accordance with the Provider Partners' instructions, which may be given directly to the Subcontractor or relayed to the Subcontractor by the

Host from time to time. These instructions may be set out in this Agreement or be in the form of standing instructions of a general or specific nature. If there is any Data of which the Host is a Data Controller, then the Subcontractor shall (a) ensure that the Data is clearly identified as such, (b) only Process such Data in accordance with the instructions of the Host and (c) keep such Data separate from any other Data. In any event, the Subcontractor shall only undertake the Processing of Data to the extent, and in such a manner, as is necessary to comply with such instructions of the relevant Data Controller (i.e. the Host or the Provider Partners);

2.1.2 only Process Data to the extent, and in such manner, as is necessary for the purposes of the performance of its obligations under this Agreement and/or the Data Extraction Agreements or as required by Applicable Law or a Regulator, including (for the avoidance of doubt) addressing data quality issues in the data feeds, supporting system developments, and de-identifying data for the purpose of creating, amending, developing or maintaining the De-Identified Dataset;

2.1.3 not itself determine or seek to determine the purposes for which and the manner in which any Data are, or are to be, Processed;

2.1.4 not Process any Data in any way which results or might result in a Security Incident;

2.1.5 ensure the reliability of any of the Subcontractor's Personnel who have access to the Data;

2.1.6 promptly notify the Host if complying with an instruction or request from the Host or a Provider Partner to Process any Data, in the Subcontractor's professional opinion, likely to result in a Security Incident or is otherwise likely to adversely affect the interests of the Host, a Provider Partner and/or any Data Subject;

2.1.7 not transfer any Data to any third party without obtaining the prior written consent of the Governing Group and the Host;

2.1.8 not transfer any Data outside England;

2.1.9 ensure that all of its Personnel who will have access to the Data are informed of the confidential nature of the Data and are contractually obliged to comply with the obligations set out in this clause 2;

2.1.10 ensure that neither it nor any of its Personnel publish, disclose or divulge any of the Data to any third party unless directed in writing to do so by the Governing Group;

2.1.11 without prejudice to the general nature of Clause 2.1.16 below:

(a) notify the Host and the Governing Group upon receipt of any complaint, notice, request for disclosure, notice of any investigations or any other communication relating to the Processing of Data performed by the Subcontractor or either Party's compliance with the Applicable Laws (including any request made by Data Subjects for disclosure of any Data). Such notice must be given to the Host:

(i) immediately upon receipt, where the relevant communication is received from any Regulator; and

(ii) within three (3) Working Days of receipt in all other cases;

(b) promptly forward to the Host any and all communication the Subcontractor receives, which does not fall within the ambit of Clause (a) above but nevertheless concerns the Data Extraction Agreements, or otherwise

concerns the Subcontractor's dealings with the CCG Partners, any Provider Partner or Data;

(c) provide all assistance and cooperation as may be reasonably requested by the Host in assessing and responding to any communication falling under this Clause 2.1.11, including by:

(i) providing full details of the complaint or request;

(ii) complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the reasonable instructions of the Governing Group or (in the case of Data of which a Provider Partner is Data Controller) the relevant Provider Partner;

(iii) providing the Governing Group or relevant Provider Partner with any Personal Data it holds in relation to a Data Subject (within the timescales reasonably required by the Governing Group or relevant Provider Partner), provided that no Provider Partner will be provided with any Personal Data of which it is not a Data Controller; and

(iv) providing the Governing Group or relevant Provider Partner with any information reasonably requested by the Governing Group or relevant Provider Partner; and

(d) not directly respond to any communication falling under this Clause 2.1.11 unless it has obtained the express written consent of the Host or the Governing Group (acting on behalf of itself or one or more Provider Partners, as appropriate), save where the Subcontractor is compelled to do so by court order;

2.1.12 notify the Host of any investigation being initiated by any Regulator that it has breached any Applicable Law with regard to the Processing of Personal Data (or any finding or determination being made in respect of such investigation) and in so notifying the Host, it shall provide an initial notice (which notice shall contain a summary of the relevant event) within two (2) Working Days of the occurrence of the relevant event, as well as a full report (which report shall set out all of the details pertaining to the relevant event in full) within four (4) Working Days of the occurrence of the relevant event;

2.1.13 maintain a record of all Processing of Data carried out by or on behalf of the Subcontractor, and ensure that such record is at all times:

(a) maintained in such a way that: (i) details the Data that is Processed; (ii) details the nature, date and time of such Processing; (iii), details any Data Subjects; and (iv) any information as may be reasonably requested by the Host, Governing Group or a Provider Partner can be ascertained from such record;

(b) kept up-to-date and fully auditable; and

(c) made available to the Host, the Provider Partners or the Governing Group (or any of their third-party representatives), upon written request;

2.1.14 promptly (and in any event within a maximum of four (4) Working Days) comply with any request of the Host to provide a copy of any or all Data which is under the Subcontractor's custody or control, in the format and on the media reasonably specified by the Host;

2.1.15 not make further copies of the Data except for backup copies necessary for the purposes of fulfilling its obligations under this Agreement and the Data Extraction Agreements which will remain subject to the provisions of Clause 3;

2.1.16 provide all assistance and cooperation as may be reasonably requested by the Host to allow the Host, any other CCG Partner and/or any Provider Partner to comply with all Applicable Laws. Such assistance shall include the granting of access to the Subcontractor's equipment, facilities, and Personnel, if and to the extent such access is requested by any Regulator undertaking any assessment of the Host's or any Provider Partner's compliance with any Applicable Laws; and

2.1.17 comply with Applicable Laws and refrain from doing anything or failing to do anything which results or may result in the Host or any Provider Partner breaching any Applicable Law.

2.2 Notwithstanding anything else in this Agreement, the Subcontractor shall not provide any Provider Partner or any other third party (including, for the avoidance of doubt, any CCG Partners) with any copies of, or information regarding or derived from, any Data of which that Provider Partner is not Data Controller, unless the Subcontractor is expressly instructed to do so by the Data Controller of that Data (either through a direct communication with the Subcontractor or in the form of instructions from the Governing Group).

2.3 If and to the extent the Subcontractor is a Data Controller in its own right with respect to any Data the Subcontractor shall, in addition to Clause 2.1, comply with all obligations that apply to it as a Data Controller under the Data Protection Legislation. The restrictions imposed on the Subcontractor under Clause 2.1 shall not apply to the extent that the Subcontractor is (in its capacity as a Data Controller of any Data) required by Applicable Law to carry out an act otherwise restricted by Clause 2.1.

3. INFORMATION SECURITY

3.1 The Subcontractor shall implement appropriate technical and organisational measures to protect the Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure (including information security arrangements that are consistent with the principles of the most current version of ISO 27002 (Code of Practice for Information Security Management)), and ensure that such measures are appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Data and have regard to the nature of the Personal Data which is to be protected. Without prejudice to the generality of the foregoing, the Subcontractor shall:

3.1.1 implement and at all times maintain an information security management system within its business and organisation which complies with all national guidelines and the highest appropriate industry standards of storage (and is, in any case, is compliant with the requirements set out in Schedule 2 (Information Security Controls)), conduct regular penetration testing to verify the security of the system and provide a report on the results of such testing to the Host and the Governing Group at least once every three months;

3.1.2 ensure that all Data which is Processed by the Subcontractor and its Personnel (including any Data that is commercially sensitive) are subjected to the controls of the information security management system the Subcontractor implements and maintains pursuant to Clause 3.1.1 above, and that all hardware used for the purposes of this Agreement is kept in a physically secure environment protected by a fully-managed industry-standard firewall which complies with the most current version of the ISO/IEC 27000 series of standards;

3.1.3 ensure that no Data is Processed outside of a secure environment controlled by the Subcontractor and agreed by both parties to be acceptable;

3.1.4 use, and ensure that the latest version of anti-virus definitions and software available from an industry-accepted anti-virus software vendor are used to check for, contain the spread of, and minimise the impact of malicious software, and provide a report on the extent of such impact to the Host and the Governing Group at least once every three months;

3.1.5 back up servers to the extent necessary to minimise the risk of loss of any of the Data, and maintain and implement a business continuity and disaster recovery plan to the reasonable satisfaction of the Host and the Governing Group; and

3.1.6 (without prejudice to the generality of the other provisions of this Clause 3.1 and Clause 3.2 below) implement and maintain the specific information security controls which are set out in Schedule 2 (Information Security Controls).

3.2 The Subcontractor shall use all reasonable efforts to ensure that Security Incidents are:

3.2.1 prevented from occurring at all, as far as is reasonably practicable;

3.2.2 prevented from recurring, should they happen at all; and

3.2.3 appropriately contained and mitigated to ensure that the adverse impact of any actual, potential, or threatened Security Incident on the Host and the Data Subjects are kept to an absolute minimum.

3.3 The Subcontractor shall provide to the Governing Group, upon request by the Host or the Governing Group, a written description of the measures undertaken under this Clause 3.

3.4 The Host has appointed a Senior Information Risk Owner ("**SIRO**") in relation to its obligations under the ISA and shall notify the Subcontractor of the identity of the SIRO and of any change of SIRO. The Subcontractor shall implement any additional information security requirements reasonably required by the SIRO.

3.5 Without prejudice to the generality of Clause 3.2, if the Subcontractor discovers or has any reason whatsoever to suspect that a Security Incident has taken place, or is likely to take place, the Subcontractor shall:

3.5.1 immediately notify the SIRO, the Governing Group, the relevant Provider Partners and any other persons or entities that the Host may require the Subcontractor to notify (and for the avoidance of doubt, a failure to make such notifications within 24 hours shall constitute a material breach of this Agreement);

3.5.2 assign appropriate resources (which must as a minimum include at least one senior Personnel of the Subcontractor who is a director) to oversee and manage the actual or suspected Security Incident through to resolution to the satisfaction of the Host;

3.5.3 provide all assistance and cooperation as may be reasonably requested by the Host in assessing and responding to such Security Incident;

3.5.4 undertake a full investigation to identify the cause, effect, and impact of such Security Incident, as well as steps the Subcontractor proposes to take so as to avoid, contain, or mitigate the adverse impact of such Security Incident;

3.5.5 devise a remedial plan of action to its ensure compliance with Clause 3.2 and notify the Host, the Governing Group and the Provider Partners of this remedial plan within three Working Days;

3.5.6 promptly implement the remedial plan of action devised further to Clause 3.5.5 above, incorporating such changes to the remedial plan of action as may be required by the Host, the Governing Group or the Provider Partners; and

3.5.7 keep the Host informed of the status of such Security Incident and its resolution by providing the Host with regular interim reports at least once every two (2) days while the Security Incident remains unresolved, as well as a final report once such Security Incident is resolved, detailing the status and/or outcome of investigation undertaken pursuant to Clause 3.5.4 and the plan of action the Subcontractor devises and implements pursuant to Clause 3.5.5, as appropriate.

4. FREEDOM OF INFORMATION

4.1 The Subcontractor acknowledges that the Host (and each of the other CCG Partners) is subject to the requirements of the Freedom of Information Act 2000 ("**FOIA**") and shall assist and cooperate with the CCG Partners (including the Host) to enable the CCG Partners to comply with their disclosure obligations under the FOIA. The Subcontractor agrees:

4.1.1 that this Agreement and any other recorded information held by the Subcontractor on a Provider Partner's behalf for the purposes of this Agreement are subject to the obligations and commitments of the Provider Partner under FOIA;

4.1.2 that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under FOIA is a decision solely for the entity to whom the request is addressed;

4.1.3 that where the Subcontractor receives a request for information under FOIA and the Subcontractor itself is subject to FOIA, it will liaise with the relevant CCG Partner or Provider Partner as to the contents of any response before a response to a request is issued and will promptly (and in any event within 2 Working Days) provide a copy of the request and any response to the relevant CCG Partner or Provider Partner;

4.1.4 that where the Subcontractor receives a request for information under FOIA and the Subcontractor is not itself subject to FOIA, it will not respond to that request (unless directed to do so by the relevant CCG Partner or Provider Partner to whom the request relates) and will promptly (and in any event within 2 Working Days) transfer the request to the relevant CCG Partner or Provider Partner;

4.1.5 that any Provider Partner, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of FOIA, and regulation 16 of the Environmental Information Regulations 2004, may disclose information concerning the Subcontractor and this Agreement either without consulting with the Subcontractor, or following consultation with the Subcontractor and having taken its views into account; and

4.1.6 to assist the Provider Partners in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by that Provider Partner within 5 Working Days of that request and without charge.

4.2 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, the content of this Agreement is not the confidential information of either Party.

4.3 Notwithstanding any other term of this Agreement, the Subcontractor consents to the publication of this Agreement in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of FOIA.

4.4 In preparing a copy of this Agreement for publication under Clause 4.3 the Host may consult with the Subcontractor to inform decision-making regarding any redactions, but the final decision in relation to the redaction of information will be at the Host's absolute discretion.

4.5 If the Host elects to publish this Agreement, the Subcontractor will assist and cooperate with the Host to enable the Host to do so.

5. AUDIT

5.1 An Auditor may conduct an audit of the Subcontractor's business to review the Subcontractor's compliance with this Agreement.

5.2 In respect of any audit conducted pursuant to Clause 5.1, the Subcontractor shall comply with all reasonable requests and directions by an Auditor to enable the Auditor to verify and/or procure that the Subcontractor is in full compliance with its obligations as such under this Agreement and/or the Data Extraction Agreements. In particular, the Subcontractor shall permit an Auditor to:

5.2.1 inspect and/or take copies of all records made or maintained by the Subcontractor under this Agreement and/or the Data Extraction Agreements; and/or

5.2.2 enter and inspect the premises used in connection with the Processing of Data; and/or

5.2.3 interview any Personnel of the Subcontractor who are engaged in the Processing of Data (or has any supervisory responsibility with respect to such Processing activities).

5.3 An Auditor shall be entitled to undertake an audit of any Sub-subcontractor, and this Clause 5 shall apply mutatis mutandis to any such audit of a subcontractor of the Subcontractor undertaken by or on behalf of an Auditor.

5.4 The Subcontractor shall conduct audits of its Sub-subcontractors' compliance with the equivalent obligations to those under this Agreement at reasonable intervals or as and when reasonably required by the Host (and in any case no less frequently than once every three months), and shall provide the Host with interim reports of such audits once every three months and a detailed annual report of all audits conducted in a year.

5.5 The Subcontractor will arrange for independent audits of the security and resilience of the software and physical and virtual systems, networks and hardware in accordance with Schedule 2 (including the non-technical management and organisational processes necessary to limit the accessibility of the virtual environment) in conjunction with the Host and/or the Governing Group, and shall provide a detailed report to the Host no less than once every twelve months. The Subcontractor shall also provide interim reports to the Host no less than once every three months. To the extent that such audits are arranged by the Host, the Subcontractor will provide all reasonable assistance requested by the Host and its appointed third-party auditors.

5.6 For the avoidance of doubt, the right of audit under this Clause 5 may be exercised independently of and in addition to any right of audit under the Data Extraction Agreements.

6. RIGHTS IN THE DATA

The Subcontractor acknowledges and agrees that nothing in this Agreement grants or shall be deemed to grant to the Subcontractor any right, title, or interest whatsoever (including any Intellectual Property Right whatsoever) in or to the Data or any part thereof, except the limited right to Process the Data for the purpose of the performance of its obligations under, and in accordance with, this Agreement and the Data Extraction Agreements.

7. RETURN OF DATA

7.1 The Host or the Provider Partners may, at any time during the term of this Agreement or upon termination or expiry of this Agreement, require the Subcontractor to:

7.1.1 securely return all or part of the Data to the Host or to each relevant Provider Partner to whom it belongs;

7.1.2 securely destroy all or part of the Data (in accordance with the then-current standard of CESG or any successor body); or

7.1.3 securely migrate all or part of the Data to a third-party software provider and provide all reasonable assistance with ensuring safe migration and data integrity of the Data, including the nomination of a named representative of the Subcontractor for the Host to contact;

within a specified timeframe.

7.2 Where the Host makes a request under Clause 7.1, the Subcontractor shall, promptly and in any event no later than thirty (30) days after receipt of such request:

7.2.1 comply with such request;

7.2.2 certify in writing to the Host that it has complied with such request and that it no longer retains any of the relevant Data under its custody or control; and

7.2.3 certify in writing that, where the Host has requested the secure destruction of Data, the Subcontractor has securely destroyed (or procured the secure destruction of) the relevant Data.

7.3 On termination of this Agreement for any reason the Subcontractor shall, as soon as reasonably practicable:

7.3.1 return, destroy or transfer to a third party (as required by the Host) all information, software and materials provided to it under this Agreement other than the Data; and

7.3.2 provide the Governing Group, the Host and the Provider Partners with a report setting out the steps taken in relation to the migration, return or destruction of the Data.

8. SUBCONTRACTING

8.1 The Subcontractor shall not subcontract any of its obligations under this Agreement to any third party without the prior written consent of the Governing Group and the Host.

8.2 Where the Host and the Governing Group consent to the use of Sub-subcontractors by the Subcontractor, in respect of each and every Sub-subcontractor, the Subcontractor shall:

8.2.1 carry out adequate due diligence on such Sub-subcontractor to ensure that the Sub-subcontractor is able to comply with the relevant obligations under this Agreement that are to be subcontracted to that Sub-subcontractor (including, where relevant, the Sub-subcontractor's ability to implement and maintain the specific information security controls which are set out in Schedule 2 (Information Security Controls)) and provide evidence of such due diligence to the Host upon request;

8.2.2 require such Sub-subcontractor, when Processing the Data, to do so in compliance with the instructions of the Provider Partners from time to time (whether given directly or relayed via the Host and/or the Subcontractor); and

8.2.3 ensure that a suitable written agreement between the Subcontractor and each Sub-subcontractor, the terms of which are no less onerous than those of this Agreement (particularly with respect to the treatment of the Data) and which enables an Auditor to directly conduct an audit of the Sub-subcontractor in accordance with Clause 5 above, is executed before the Sub-subcontractor is allowed to commence performance of any of the subcontracted obligations of the Subcontractor, and provide a copy of such agreement to the Host upon request;

8.2.4 remain fully liable to the Host for all acts and/or omissions of the Sub-subcontractor.

9. WARRANTIES AND INDEMNITIES

9.1 The Subcontractor warrants to the Host that:

9.1.1 the Subcontractor has obtained all relevant licences, permits, and authorisations, and completed all relevant registrations and other formalities required in order to lawfully perform its obligations under this Agreement and the Data Extraction Agreements;

9.1.2 there is no proceeding pending or, to the knowledge of the Subcontractor, threatened, which has or may have a material adverse effect on this Agreement or on the ability of the Subcontractor to perform its obligations under this Agreement and the Data Extraction Agreements;

9.1.3 the Subcontractor is not aware as at the Effective Date of anything within its reasonable control which will or might adversely affect its ability to fulfil its obligations under this Agreement or the Data Extraction Agreements.

9.2 The Subcontractor shall notify the Host promptly (and in any case within 24 hours) if it becomes aware of any proceedings or any other matter which will or might have a material adverse effect on this Agreement or on the ability of the Subcontractor to perform its obligations under this Agreement and/or the Data Extraction Agreements.

9.3 The Subcontractor shall indemnify and keep the Host fully indemnified in respect of all fines, penalties, losses, liabilities, damages, claims, costs and expenses of whatsoever nature (whether incurred by the Host, by another CCG Partner or by any Provider Partner) that arise directly out of or in connection with the Subcontractor's or the Subcontractor's Personnel's acts and/or omissions under this Agreement, including those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any Applicable Law (including, for the avoidance of doubt, any Data Protection Legislation).

9.4 The Host's right to be indemnified under Clause 9.3 above shall be without prejudice to any other rights or remedies the Host may have, including, without limitation, injunctive or other equitable relief.

10. TERM AND TERMINATION

10.1 This Agreement shall commence on the Effective Date and shall continue until:

10.1.1 the Data Extraction Agreements have been terminated and the Subcontractor has ceased to Process the Data in any manner whatsoever; and

10.1.2 the Subcontractor has ceased to have any Data under its custody or control.

10.2 The Subcontractor may not terminate this Agreement except where it has given notice to terminate the Data Extraction Agreements. The Host may terminate this Agreement at any time by giving at least thirty (30) days' notice in writing to the Subcontractor.

10.3 Without prejudice to any rights that have accrued under this Agreement or any of its rights or remedies, the Host may terminate this Agreement with immediate effect by giving written notice to the Subcontractor if the Subcontractor commits a material breach of any term of this Agreement and (if that breach is remediable) fails to remedy that breach within a period of thirty (30) days after being notified in writing to do so.

10.4 The termination or expiry of this Agreement for whatever reason shall not affect the accrued rights or obligations of either Party arising out of this Agreement and/or the Data Extraction Agreements.

10.5 Any provision of this Agreement which contemplates performance or observance subsequent to any termination or expiry of this Agreement (including, for the avoidance of doubt, Clauses 2, 3, 5, 7 and 10) shall survive any termination of this Agreement and continue in full force and effect (together with any other provisions required to interpret or enforce the same).

11. GENERAL PROVISIONS

11.1 Consideration

In consideration of the Subcontractor entering into this Agreement, the Host shall pay the Subcontractor the sum of £1.00 (one pound sterling), the receipt and sufficiency of which the Subcontractor acknowledges by executing this Agreement.

11.2 Disputes

Where there is a dispute, the aggrieved Party shall notify the other Party in writing of the nature of the dispute with as much detail as possible about the deficient performance of the other party. A representative from senior management of each of the parties (together the "**Representatives**") shall meet in person or communicate by telephone within five Working Days of the date of the written notification in order to reach an agreement about the nature of the deficiency and the corrective action to be taken by the respective Parties. The Representatives shall produce a report about the nature of the dispute in detail to their respective boards and if no agreement is reached on corrective action, then the chief executives of each Party shall meet in person or communicate by telephone, to facilitate an agreement within five Working Days of a written notice by one to the other. If the dispute cannot be resolved at board level within a further five Working Days, or if the agreed upon completion dates in any written plan of corrective action are exceeded, either party may seek the legal remedies to which it is entitled under this Agreement.

11.3 Governing Law and Jurisdiction

This Agreement is governed by and shall be construed in accordance with the laws of England and Wales, and the Parties agree to submit to the exclusive jurisdiction of the courts of England. Notwithstanding the foregoing, the Host shall be entitled to seek the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of this Agreement in any court of competent jurisdiction.

11.4 Amendment and Variation

No amendment or variation to this Agreement, or any revocation or extension of this Agreement, shall be effective unless it is made in writing and signed by the Parties.

11.5 Third Party Rights

Any CCG Partner (other than the Host) or Provider Partner who is affected by the Processing of Data undertaken by the Subcontractor shall be a third party beneficiary under this Agreement and shall be entitled to enforce and benefit from each and every term of this Agreement as if it was itself a party to this Agreement. The Parties agree that no consent of any CCG Partner (other than the Host) or Provider Partner is required to amend or terminate this Agreement (whether or not in a way that varies or extinguishes rights or benefits in favour

of any such CCG Partner). Otherwise, a person who is not a Party to this Agreement shall have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

11.6 **Assignment**

The Subcontractor shall not be entitled to assign or otherwise transfer its rights or obligations under this Agreement in whole or part to any third party.

11.7 **Entire Agreement**

This Agreement contains the entire understanding and agreement of the Parties in respect of the Processing of the Data and supersedes all prior oral or written communications and agreements between the Parties in relation to such Processing. This Agreement may not be amended except in writing signed by authorised representatives of both the Host and the Subcontractor. In entering into this Agreement neither Party has relied on any representations or warranties other than those expressly made in this Agreement. No party shall have any claim for innocent or negligent misrepresentation based on any statement in this Agreement.

11.8 **Notices**

All notices that are required to be given under this Agreement shall be in writing and shall be sent to the address of the Party as set out in this Agreement, as may be updated by each Party from time to time by notice to the other. Any notice shall be delivered by hand or sent by pre-paid first class post or other "next working day" delivery service or by email with a delivery receipt requested. Any notice or communication shall be deemed to have been received, if delivered by hand, on signature of a delivery receipt, or if sent by email, at the time recorded by the delivery receipt, or otherwise (for all notices other than email) at 9:00 am on the second Working Day after posting or at the time recorded by the delivery service.

11.9 **Waiver**

No omission or delay on the part of any Party in exercising any right under this Agreement shall operate as a waiver by that Party of any right to exercise it in future or of any other rights of that Party under this Agreement. No waiver of any provision of this Agreement shall be effective except to the extent made in writing and signed by the Party giving the waiver.

11.10 **Invalidity**

In the event that any provision of this Agreement is determined by any court of competent jurisdiction to be invalid, unlawful or unenforceable to any extent, such provision shall, to that extent, be severed from the remainder of this Agreement, which shall continue to be valid to the fullest extent permitted by applicable law, and the Parties shall negotiate in good faith to amend the severed provision so that, as amended it is legal, valid and enforceable, and to the greatest extent possible achieves the Parties' original commercial intention.

11.11 **No Partnership or Agency**

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

11.12 **Execution in Counterparts**

This Agreement may be executed in counterparts, each of which shall be deemed to be an original document but all of which taken together shall constitute one single agreement between the Parties.

SIGNATURE PAGE

EXECUTED by the Parties

for and on behalf of

NHS BRENT CLINICAL COMMISSIONING GROUP

Signature .....

Name Jan Norman

Position Director of Quality.

(PLEASE COMPLETE IN CAPITALS)

EXECUTED by the Parties

for and on behalf of

APOLLO MEDICAL SOFTWARE SOLUTIONS LIMITED

Signature Tony Megaw

Name TONY MEGAW

Position MANAGING DIRECTOR

(PLEASE COMPLETE IN CAPITALS)

SCHEDULE 1

Definitions and Interpretation

1. DEFINITIONS

In this Agreement (including the Background), unless the context otherwise requires, the following words shall have the following meanings:

"Applicable Law"	means any court order or any common law, statute, statutory instrument, order or regulation issued by a governmental body with authority over any relevant party, applicable to any relevant Party from time to time in the context of its relevant rights and obligations under this Agreement or the Data Extraction Agreements, including the Data Protection Legislation;
"Auditor"	means a Regulator, the Governing Group or the Host (or any third party appointed by any of them to conduct an audit of the Subcontractor);
"CCG Partner"	means the Host, NHS Central London Clinical Commissioning Group, NHS Ealing Clinical Commissioning Group, NHS Hammersmith & Fulham Clinical Commissioning Group, NHS Harrow Clinical Commissioning Group, NHS Hounslow Clinical Commissioning Group, NHS West London Clinical Commissioning Group and NHS Hillingdon Clinical Commissioning Group.
"CESG"	means the group within the Government Communications Headquarters which deals with information security (with its website, as of the Effective Date, at www.cesg.gov.uk);
"Data"	means any information whatsoever which constitutes Personal Data or is capable of constituting Personal Data, and is provided to or made available to the Subcontractor by or on behalf of the Host or any other CCG Partner and is Processed in any manner whatsoever by the Subcontractor under or in connection with the Data Extraction Agreements, as well as any information which is provided to the Subcontractor by or on behalf of the Host or any other CCG Partner and which is designated as being confidential, is manifestly of a confidential nature, or reasonably ought to be treated as such and any records maintained by the Subcontractor in accordance with Clause 2.1.13;
"Data Controller"	shall have the meaning given to it under section 1(1) of the Data Protection Act;
"Data Extraction Agreements"	means the agreements entered into between the Subcontractor and various Provider Partners, pursuant to which the Subcontractor provides certain services that involve the Processing by the Subcontractor of Data;
"Data Protection Act"	means the Data Protection Act 1998;
"Data Protection Legislation"	means the Data Protection Act, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the

	Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner;
"Data Subject"	means any individual who is a 'data subject' (as that term is defined under the section 1(1) of the Data Protection Act) in respect of Data;
"De-Identified Dataset"	means a copy of the Whole Systems Integrated Care Record, which is de-identified to the Information Standards Board Standard for Health Data (ISB 1523), published at http://www.isb.nhs.uk/library/standard/128;
"Good Industry Practice"	means the exercise of that degree of skill, diligence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of business as the Subcontractor;
"Governing Group"	means the group appointed under clause 14 of the ISA and defined therein as the Governing Group, consisting of various nominees and representatives of the Provider Partners and the CCG Partners;
"HSCIC"	means the Health & Social Care Information Centre;
"IG Toolkit"	means the latest version Information Governance Toolkit maintained by the HSCIC, as updated from time to time;
"Intellectual Property Rights"	means patents, rights in trade secrets, copyright, database rights, design rights, rights in trademarks, rights in domain names, and all other analogous intellectual property rights (whether or not registered or capable of registration and including applications for registration or the right to apply for registration of any such right) and all rights or forms of protection of a similar nature (including the right to bring proceedings for infringement of such rights) that subsist anywhere in the world, for the full duration of such rights (including extensions and renewals);
"Personal Data"	shall have the meaning given to it under section 1(1) of the Data Protection Act;
"Personnel"	means, in relation to either Party, all personnel of that Party, including directors, officers, employees, and temporary staff, as well as of that Party's agents and subcontractors. For the avoidance of doubt, the Host's Personnel shall exclude the Subcontractor and the Subcontractor's Personnel;
"Processing"	shall have the meaning given to it under section 1(1) of the Data Protection Act, and permutations such as "Process" or "Processed" shall be interpreted accordingly;

"Provider Partners"	means the parties to the ISA, excluding the Host;
"Regulator"	means any governmental or public department, authority, or agency which has supervisory authority over any CCG Partner or Provider Partner in respect of the CCG Partner or Provider Partner's conduct of its business (or any aspect thereof);
"Security Incident"	means any incident whatsoever and howsoever caused which results (or could potentially result) in: (i) unauthorised or unlawful Processing of Data, including any unauthorised reproduction, alteration, disclosure, sale, or any other misuse or exploitation or Data; (ii) accidental loss, destruction, or corruption of, or damage to Data; (iii) the confidentiality, integrity, or availability of Data otherwise becoming compromised; or (iv) the Host or any Provider Partner breaching any Data Protection Legislation;
"Services"	means the services that are provided pursuant to the Data Extraction Agreements;
"Sub-subcontractor"	means a subcontractor engaged by the Subcontractor to perform any of the Subcontractor's obligations under this Agreement or the Data Extraction Agreements;
"Whole Systems Integrated Care Record"	means the electronic integrated care record being established pursuant to the ISA; and
"Working Day"	means a day which is not a Saturday or a Sunday or a public holiday in England.

2. INTERPRETATION

2.1 Unless the context otherwise requires, the singular includes the plural and vice versa.

2.2 The headings in this Agreement are for the convenience of the Parties only, and are in no way intended to affect, describe, interpret, define or limit the scope, extent, or interpretation of the Agreement of any provision thereof.

2.3 Any obligation in this Agreement not to do anything includes an obligation not to suffer, permit or cause that thing to be done.

2.4 The terms "**including**", "**includes**", and "**in particular**" shall not be construed as terms of limitation.

2.5 References to "this Agreement" shall include all Clauses and Schedules.

2.6 Clause, Schedule and paragraph headings shall not affect the interpretation of this Agreement. References to Clauses and Schedules are to the Clauses and Schedules to this Agreement and references to paragraphs are to paragraphs of a Schedule.

2.7 Reference in this Agreement to any directive, regulation, decision, statute, enactment, or other similar instrument shall be construed to include a reference to such instrument, as the same is from time to time amended, extended, re-enacted, replaced, or consolidated, and all subordinate legislation made from time to time under such instrument.

2.8 A reference to "**writing**" or "**written**" includes e-mail if a delivery receipt has been returned to the sender indicating successful delivery.

2.9 In case of any conflict or ambiguity between the Clauses and the Schedules, the Clauses shall take precedence.

SCHEDULE 2

Information Security Controls

1. SECURITY RESPONSIBILITIES

1.1 The Subcontractor shall maintain appropriate information security arrangements for all forms of Data held in any format and expressed or relayed in any communication (oral or written) in a manner consistent with the principles of the most current version of the IG Toolkit and ISO 27002 - Code of Practice for Information Security Management (with the principles of the IG Toolkit prevailing in case of any conflict). In particular:

1.1.1 The Subcontractor shall have management arrangements in place for the management of information security;

1.1.2 The Subcontractor shall comply with the IG Toolkit assessment, reporting and audit requirements relevant to its organisation type; and

1.1.3 The Subcontractor shall have appropriate operational risk assessment and management processes in place for the identification, mitigation and management of operational security risks.

1.2 The Parties shall agree, and the Subcontractor shall have in place, an information security policy that is supported by appropriate organisational, security and technical security standards (the "**Security Policy**").

1.3 The Subcontractor shall propose changes to the Security Policy on an on-going basis to reflect Good Industry Practice or changes necessitated by any changes in Applicable Law. Material changes to the management of information relating to the Host's business shall be agreed in writing by both parties, and the requirement for all such changes shall be promptly notified to the other party.

1.4 The Subcontractor shall create, design, establish, provide, implement, manage and maintain safeguards (including security architecture) that reflect the Security Policy and shall ensure that any changes to the Security Policy from time to time are reflected in the secure environment provided to Host as soon as practicable.

1.5 The Subcontractor shall be equally responsible for managing information security risk should the Data, or access to the Data, be made available to any third parties or subcontractors (as may be permitted elsewhere). Such engagements will be preceded by a satisfactory due diligence process, contractual documentation being signed, and the establishment of monitoring, auditing and incident handling procedures so that the Data is no less secure under the third party's management.

1.6 The Subcontractor shall ensure that all transfers of the Data undertaken by it or on its behalf will be in accordance with Secure File Transfer Protocols within the N3 network and/or in accordance with the HSCIC Good Practice Guidelines (which are, as of the date of this Agreement, published at http://systems.hscic.gov.uk/infogov/security/infrasec/gpg).

2. SECURITY MANAGEMENT

2.1 The Subcontractor shall plan, determine, create, implement, manage, review and maintain security control over the technology and physical storage infrastructure, and respond appropriately to security events. This includes the implementation of secure technical infrastructures, technologies and physical controls (including firewalls, encryption, authentication services and swipe access) appropriate to the UK public health sector.

2.2 The Subcontractor shall implement control, technologies and procedures to limit the risk of unauthorised access to the environment used to provide the Services (the "**Services Environment**"), Host applications and Data appropriate to the UK public health sector.

2.3 The Subcontractor shall inform and make recommendations to the Host if it becomes aware of any products, methods or services that would result in required improvements to the security procedures in operation.

2.4 The Subcontractor shall create, acquire, provide, install, implement, manage and maintain any such improvements reasonably requested by Host that reflect Good Industry Practice.

3. SECURITY ADMINISTRATION

3.1 The Subcontractor shall track, co-ordinate, implement, manage and maintain all security changes across the Services Environment.

3.2 The Subcontractor shall limit the risk of unauthorised access to the Services Environment including content filtering to prevent objectionable material, virus protection, password controls and physical security. The Subcontractor shall have regard to the confidentiality and sensitivity contained within the Services Environment and shall ensure that measures applicable to the UK public health sector are in place to prevent unauthorised access.

4. SECURITY AUDIT

The Subcontractor shall provide to the Host any information that the Host reasonably requires for the purpose of allowing the Host to investigate the Subcontractor's compliance with the provisions of this Schedule 2 within a reasonable time from the Host's request. The Subcontractor shall provide this information in such format as the Host may reasonably require.

5. NON-COMPLIANCE REPORTING

5.1 The Subcontractor shall monitor, on an ongoing basis, computer and network security configurations.

5.2 The Subcontractor shall create and issue reports to the Host on incidents of non-compliance with the Security Policy according to their severity within a reasonable time after such incidents occur.

6. SYSTEM ACCESS CONTROL

6.1 The Subcontractor shall administer the provision of access to the Services Environment (by both the Host's Personnel and the Subcontractor's Personnel), Data and any other applicable data in accordance with Good Industry Practice.

6.2 The Subcontractor shall restrict access to the Services Environment to appropriately identified authenticated and authorised personnel, and shall keep records of which personnel have access to the Services Environment and the reasons for such personnel being given such access. The Subcontractor shall also keep records of which personnel have accessed the Services Environment (including details of login and logout times).

6.3 The Subcontractor shall restrict user access to information and data held on external networks.

7. CRYPTOGRAPHY MANAGEMENT

7.1 The Subcontractor shall ensure that Data is encrypted as appropriate in accordance with Good Industry Practice and the most current version of the IG Toolkit and ISO 27002 - Code of Practice for Information Security Management (with the principles of the IG Toolkit prevailing in case of any conflict).

7.2 The Subcontractor shall manage all processes and procedures pertaining to the administration of the encryption keys, including secure key storage, periodic changing of keys, destruction of old keys, and registration of keys with the appropriate authorities.

8. ASSET PROTECTION

8.1 The Subcontractor shall acquire, create, provide, manage and maintain mechanisms to prevent or mitigate destruction, loss, alteration, disclosure or misuse of equipment used within the Services Environment, Data and Host assets, having regard to Good Industry Practice.

8.2 All Data shall be appropriately backed up and stored in a secure facility which in line with industry practice would be off site.

8.3 The Subcontractor will ensure adequate business continuity services and disaster recovery services are in place and regularly tested. Evidence of this testing may be required as part of the Host's due diligence.

8.4 The Subcontractor shall ensure that no-one, other than properly authorised Subcontractor Personnel, has physical access to any servers in scope under this Agreement or used to deliver the Services, including any servers located at the Subcontractor's facilities without formal documented approval from the Host.

8.5 In relation to Subcontractor's facilities, the Subcontractor shall, at a minimum, acquire, create, provide, manage and maintain mechanisms to prevent or mitigate destruction, loss, alteration, disclosure or misuse of Host systems and/or Data, having regard to Good Industry Practice.

8.6 The Subcontractor will fully and regularly assess the physical security risk for all premises and ensure reasonable controls are in place to prevent inappropriate access as would be expected for the National Health Service.

9. SECURITY AWARENESS

The Subcontractor shall ensure that all its Personnel working on the Host account are screened and security checked to an appropriate standard, trained in the Security Policy and any other requirements of this Agreement, and are individually accountable for their actions. All Subcontractor Personnel shall, as at the commencement of the Services, be deemed to be appropriately screened and trained to a level befitting the UK public health sector.

10. SECURITY INCIDENTS AND MATERIAL RISK REPORTING

10.1 The Subcontractor shall:

10.1.1 maintain a procedure for responding to Security Incidents, and shall report any Security Incident to the Host in accordance with that procedure (the "**Security Incident Response Procedure**") and in any event within 24 hours of the occurrence of the Security Incident; and

10.1.2 monitor the use of the Data, Host systems and Services to verify that all access to them is authorised and to check for any actual or potential Security Incidents.

10.2 In the event of a Security Incident, the Subcontractor shall:

10.2.1 immediately notify the Host (including, where necessary, escalating such notification); and

10.2.2 respond in a timely and appropriate manner to such Security Incident, each in accordance with the Security Incident Response Procedure.

10.3 The Subcontractor shall:

10.3.1 at the Host's request, provide assistance to the Host and/or its authorised representatives into the investigation of a Security Incident and retain all documentation relating to any such investigations;

10.3.2 in the case of a Security Incident which materially and adversely affects Data and/or the security of the Services, provide immediate assistance (subject to instructions and/or approvals granted by the Host) to the Host and/or its authorised representatives in respect of the investigation of the Security Incident and retain all documentation relating to any such investigations.

11. RIGHTS OF ACCESS

The Subcontractor shall allow the Host access and fully cooperate in order to conduct any audit of compliance or to investigate specific incidents in accordance with Clause 5 of this Agreement.

12. DOCUMENTATION AND RECORD PRESERVATION

12.1 The Subcontractor shall protect all Data held by Subcontractor employees, agents or subcontractors in a physical form by adopting a "clear desk" policy in respect of such Data and disposing of such information securely by treating it as confidential waste.

12.2 The Subcontractor shall ensure that any documentation or records relating to the Services being disposed of by or on behalf of the Subcontractor are treated in an appropriate manner having regard to their confidentiality including, where appropriate, being securely destroyed or shredded prior to disposal.

12.3 Upon termination of this Agreement, the Subcontractor will work with the Host to ensure that Clause 7 of this Agreement is complied with in respect of any and all Data under the Subcontractor's custody or control.

12.4 The Subcontractor will classify the security of documentation and information to limit distribution and to ensure adequate controls are in place to protect more sensitive content.

12.5 Subject to Clause 7.3, the Subcontractor shall retain all records maintained by it under this Agreement ("**Records**") for a period of six years following the termination or expiry of this Agreement, provided that the Host may at any time require any such records to be returned or destroyed before the end of that six-year period. At the end of this six-year period, the Subcontractor shall deliver all Records to the Host, unless otherwise instructed by the Host. Any return or destruction of any Records by the Subcontractor must be done securely and in compliance with the information security controls maintained by the Subcontractor under this Agreement and, in the case of destruction, in accordance with the then-current standard of CESG or any successor body.