

Dated _____ 2016

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

- and -

(2) **PATIENTS KNOW BEST LIMITED**

Data Processing Agreement

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

© DAC Beachcroft LLP 2015
Draft: 2015

S_4081154270

Table of contents

Clause heading and number	Page number
1. SPECIFIC OBLIGATIONS OF PKB	1
2. CONDITIONS OF PROCESSING	2
3. INFORMATION SECURITY	4
4. FREEDOM OF INFORMATION	6
5. AUDIT	7
6. RIGHTS IN THE DATA.....	8
7. RETURN OF DATA	8
8. SUBCONTRACTING.....	9
9. WARRANTIES AND LIABILITY.....	9
10. TERM AND TERMINATION	11
11. GENERAL PROVISIONS	12
SIGNATURE PAGE.....	15
SCHEDULE 1	16
DEFINITIONS AND INTERPRETATION.....	16
SCHEDULE 2	20
INFORMATION SECURITY CONTROLS	20

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) **PATIENTS KNOW BEST LIMITED** (company registration number 06517382) of St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS ("**PKB**")

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

BACKGROUND:

- (A) The Host has been appointed as host organisation entering into contracts with third party suppliers of technology and related infrastructure pursuant to the North West London Integrated Care Digital Information Governance Agreement dated 1 October 2014 (the "**ISA**") between the Host and the Provider Partners. The ISA was varied by agreement between the Partners with effect from 1 September 2015 and on _____ 2016.
- (B) Following completion of the ISA, one of the Provider Partners, Imperial College Healthcare NHS Trust ("**Imperial**") entered into a call-off contract under the Crown Commercial Service G-Cloud Services 6 Framework Agreement with PKB whereby PKB agreed to provide certain services for the creation of integrated care records to be used by the Provider Partners in North West London. This Agreement is the Underlying Commercial Agreement.
- (C) The obligations of PKB to Imperial under the Underlying Commercial Agreement and of PKB and Imperial to the ISA signatories under the Assurance Requirements shall not be affected by this Agreement.
- (D) Under the Underlying Commercial Agreement, PKB will provide services which enable the implementation of the CIE Care Record. In providing these services PKB is appointed as a sub-data processor of the Host who is in turn appointed as data processor of the Provider Partners on terms set out in the ISA.
- (E) The Underlying Commercial Agreement also provides that PKB will implement the facility for patients who explicitly consent to the creation of a personal account with PKB to access their own medical records online and to input into them. These are known as Patient Access Services. In providing Patient Access Services PKB acts as a data controller of the data in the patient accessible online record. This data includes data derived from data in the CIE Care Record.
- (F) This Data Processing Agreement is only concerned with PKB's activities and obligations to the Host, and through the Host to the Provider Partners, as a data processor of data populating the CIE Care Record. PKB's activities and obligations to the Provider Partners in respect of the Patient Access Services are addressed in Part B of the ISA and related Assurance Agreement entered into pursuant to the ISA.
- (G) The obligations of PKB to the Host under this Agreement shall not be affected by any agreement between PKB and Imperial.
- (H) This Agreement records the specific terms and conditions upon which Processing of Data provided by or on behalf of the Provider Partners to the Host is to be performed by PKB.

THE PARTIES AGREE as follows:

1. SPECIFIC OBLIGATIONS OF PKB

- 1.1 PKB shall, to the extent instructed to do so by the Host:
 - 1.1.1 provide technical support, implementation and set-up assistance for the CIE

Care Record in accordance with the Underlying Commercial Agreement;

- 1.1.2 receive the transfer of Data from Provider Partners and host it on the system provided under the Underlying Commercial Agreement.
- 1.2 PKB shall not when acting as a data processor hereunder:
 - 1.2.1 do anything that may materially damage the reputation of a CCG Partner and/or any Provider Partner (and PKB acknowledges that PKB's use of the Data for clinical research purposes or for sale to third parties 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 Subject to clause 2.2 below, where PKB undertakes any Processing of Data in connection with the CIE Care Record under this Agreement (whether during the term of this Agreement or following termination), PKB shall:
 - 2.1.1 only Process such Data in accordance with the Provider Partners' instructions, which may be given directly to PKB or relayed to PKB by the Host from time to time, for the purposes of fulfilling this Agreement and the Underlying Commercial Agreement. These instructions may be set out in this Agreement and/or the Underlying Commercial Agreement or be in the form of standing instructions of a general nature. PKB 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 Provider Partners;
 - 2.1.2 only Process such 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 Underlying Commercial Agreement or as required by Applicable Law or a Regulator;
 - 2.1.3 not itself determine or seek to determine the purposes for which and the manner in which any Data in the CIE Care Record are, or are to be, Processed;
 - 2.1.4 not Process any such Data in any way which results or might result in a Security Incident;
 - 2.1.5 ensure the reliability of any of PKB's Personnel who have access to the CIE Care Record;
 - 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 PKB'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 in the CIE Care Record to any third party other than to permit the Provider Partners to access the CIE Care Record without obtaining the prior written consent of the Governing Group and the Host;
 - 2.1.8 not transfer any Data in the CIE Care Record outside England unless at the instruction of and with the explicit consent of a patient as instructed by the

Governing Group and the Host;

- 2.1.9 ensure that all of its Personnel who will have access to the Data in the CIE Care Record 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 in the CIE Care Record to any third party unless directed in writing to do so by the Governing Group;
- 2.1.11 the following provisions of clause 2.1.12 shall be read and construed on the basis that the technical system employed by PKB for the processing of Data hereunder does not enable PKB to access or read the Data;
- 2.1.12 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 PKB 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 PKB receives, which does not fall within the ambit of Clause (a) above but nevertheless concerns the Underlying Commercial Agreement, or otherwise concerns PKB's dealings with the CCG Partners, any Provider Partner or Data and which, for the avoidance of doubt, includes any communication relating to the transfer or processing of data from any organisation within PKB Sharing Network;
 - (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 Governing Group or relevant Provider Partner's reasonable instructions;
 - (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); 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) save where PKB is compelled to do so by court

order;

- 2.1.13 notify the Host via the following email address _____ and copied to Imperial at the following _____ of any investigation being initiated by any Regulator that PKB has breached any Data Protection Legislation 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;
- 2.1.14 ensure that the system maintains a record of all Processing of Data and ensure that such record at all times enables the Provider Partners to identify:
- (a) (i) the Data that is Processed and by whom; (ii) the nature, date and time of such Processing; (iii), any Data Subjects; and is
 - (b) kept up-to-date and fully auditable; and
 - (c) is accessible to the Provider Partners (or a representative acting on their behalf) in so far as it relates to individuals with whom a Provider Partner has a legitimate care relationship;
- 2.1.15 not make further copies of the Data except as necessary for the delivery of services to the Host pursuant to the Host's instructions under this Agreement or pursuant to the Underlying Commercial Agreement;
- 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 Data Protection Legislation. Such assistance shall include the granting of access to PKB'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 such Applicable Laws; and
- 2.1.17 comply with all Data Protection Legislation and refrain from doing anything or failing to do anything which results or may result in the Host or any Provider Partner breaching any Data Protection Legislation.
- 2.2 The Host acknowledges for itself and on behalf of the Provider Partners that in the provision of Patient Access Services, PKB acts as a data controller. The provisions of clause 2.1 shall not affect the obligations of PKB as a data controller in respect of the data it accesses or processes as a data controller under the Underlying Commercial Agreement or Part B of the ISA.

3. INFORMATION SECURITY

- 3.1 PKB 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, PKB shall:

- 3.1.1 implement and at all times maintain an information security management system within its business and organisation which complies with the highest appropriate industry standards of storage (and is, in any case, is compliant with the requirements set out in of Schedule 2 (Information Security Controls)) and conduct regular penetration testing to verify the security of the system;
 - 3.1.2 ensure that all Data which is Processed by PKB and its Personnel (including any Data that is commercially sensitive) is subjected to the controls of the information security management system PKB 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 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;
 - 3.1.4 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
 - 3.1.5 (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 PKB shall use reasonable commercial 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, Provider Partners and CCG Partners and the Data Subjects are kept to an absolute minimum.
- 3.3 PKB 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 Without prejudice to the generality of Clause 3.2, if PKB discovers or has any reason whatsoever to suspect that a Security Incident has taken place, or is likely to take place, PKB shall:
- 3.4.1 immediately notify the Host, the Governing Group and the relevant Provider Partners;
 - 3.4.2 assign appropriate resources (which must as a minimum include at least one senior Personnel of PKB who is a director) to oversee and manage the actual or suspected Security Incident through to resolution to the satisfaction of the Host;
 - 3.4.3 provide all assistance and cooperation as may be reasonably requested by the Host in assessing and responding to such Security Incident;

- 3.4.4 undertake a full investigation to identify the cause, effect, and impact of such Security Incident, as well as steps PKB proposes to take so as to avoid, contain, or mitigate the adverse impact of such Security Incident;
 - 3.4.5 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;
 - 3.4.6 promptly implement the remedial plan of action devised further to Clause 3.4.5 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
 - 3.4.7 keep the Host informed of the status of such Security Incident and its resolution by providing the Host with regular interim reports, as well as a final report once such Security Incident is resolved, detailing the status and/or outcome of investigation undertaken pursuant to Clause 3.4.4 and the plan of action PKB devises and implements pursuant to Clause 3.4.5, as appropriate.
- 3.5 The Host has appointed a Senior Information Risk Owner ("**SIRO**") in relation to its obligations under the ISA, and PKB shall implement any information security requirements reasonably required by the SIRO.

4. **FREEDOM OF INFORMATION**

- 4.1 PKB 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 Host to enable the CCG Partners to comply with their disclosure obligations under the FOIA. PKB agrees:
- 4.1.1 that this Agreement and any other recorded information held by PKB 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 PKB receives a request for information under FOIA and PKB 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 PKB receives a request for information under FOIA and PKB 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 PKB and this Agreement either without consulting with PKB, or following consultation with PKB 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, PKB 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 PKB 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, PKB 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 PKB's business to review PKB's compliance with this Agreement.
- 5.2 In respect of any audit conducted pursuant to Clause 4.1, PKB shall comply with all reasonable requests and directions by an Auditor to enable the Auditor to verify and/or procure that PKB is in full compliance with its obligations as such under this Agreement and/or the Underlying Commercial Agreement. In particular, PKB shall permit an Auditor to:
 - 5.2.1 inspect and/or take copies of all records made or maintained by PKB under this Agreement; 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 PKB 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 subcontractor engaged by PKB, and this Clause 4 shall apply mutatis mutandis to any such audit of a subcontractor of PKB undertaken by or on behalf of an Auditor.
- 5.4 PKB shall conduct audits of its subcontractors' compliance with the equivalent obligations to those under this Agreement at reasonable intervals or as and when reasonably required by the Host, and shall provide the Host with a detailed report of such audit.
- 5.5 PKB 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 report to the Host no less than

once every twelve months. To the extent that such audits are arranged by the Host, PKB 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 4 may be exercised independently of and in addition to any right of audit under the Underlying Commercial Agreement.

6. RIGHTS IN THE DATA

Each Party acknowledges and agrees that nothing in this Agreement or the Underlying Commercial Agreement grants or shall be deemed to grant to the other Party any right, title, or interest whatsoever (including any Intellectual Property Right whatsoever) in or to the Data or any part thereof, except:

- 6.1 the limited right for PKB to Process the Data for the purpose of the performance of its obligations under, and in accordance with, this Agreement and the Underlying Commercial Agreement; and
- 6.2 a non-exclusive licence for the Host to use the Services during the continuance of the Underlying Commercial Agreement,

to the extent necessary to enable the Host to receive the benefit of this Agreement and as stipulated in the Underlying Commercial Agreement.

7. RETURN OF DATA

- 7.1 Subject to clause 7.4 and subject also to the terms of the Underlying Commercial Agreement, 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 PKB to facilitate the migration of 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 PKB for the Host to contact within a specified timeframe.
- 7.2 On termination of this Agreement for any reason PKB shall, as soon as reasonably practicable, 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.
- 7.3 Where the Host makes a request under Clause 6.1, PKB shall, promptly and in any event no later than thirty (30) days after receipt of such request:
- 7.3.1 comply with such request;
 - 7.3.2 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
 - 7.3.3 certify in writing that, where the Host has requested the secure destruction of Data, PKB has securely destroyed (or procured the secure destruction of) the relevant Data.
- 7.4 For the avoidance of doubt, the provisions of Clauses 7.1 to 7.3 above shall not affect any obligations of PKB as a data controller in respect of data it accesses or processes as a data controller pursuant to the Underlying Commercial Agreement in order to provide the Patient Access Services.

8. SUBCONTRACTING

- 8.1 PKB 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. This clause 8 shall not apply to the appointment of suppliers appointed by PKB for the provision of services to PKB including suppliers of IT infrastructure which is used to host or process Data.
- 8.2 Where the Host and the Governing Group consent pursuant to clause 8.1 above to the use of subcontractors by PKB, in respect of each and every subcontractor PKB engages (each a "**Sub-subcontractor**"), PKB 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 PKB); and
 - 8.2.3 ensure that a suitable written agreement between PKB 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 4 above, is executed before the Sub-subcontractor is allowed to commence performance of any of the subcontracted obligations of PKB, 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 LIABILITY

- 9.1 PKB warrants to the Host that:
- 9.1.1 PKB 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 Underlying Commercial Agreement;
 - 9.1.2 there is no proceeding pending or, to the knowledge of PKB, threatened, which has or may have a material adverse effect on this Agreement or on the ability of PKB to perform its obligations under this Agreement and the Underlying Commercial Agreement;
 - 9.1.3 PKB 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 Underlying Commercial Agreement.
- 9.2 The Host warrants to PKB that it has authority to act on behalf of and to bind the Partners under and for the purposes of this clause 9.
- 9.3 If PKB becomes aware of:
- 9.3.1 any Court proceedings being commenced against PKB in England or

Wales; or

9.3.2 any other matter which will or might reasonably be expected to have a material adverse effect on the ability of PKB to perform its material obligations under this Agreement and/or the Underlying Commercial Agreement and/or the Assurance Agreement,

and PKB shall notify the Host as soon as it is reasonably practicable following PKB becoming aware of these matters.

9.4 The Host acknowledges and agrees for itself and on behalf of the Provider Partners and CCG Partners that PKB has limited its liability to Imperial for any losses incurred in the provision of services or in connection to the provision of services pursuant to the Underlying Commercial Agreement, and the Assurance Agreement and as set out in more detail below.

9.5 The Host acknowledges and agrees for itself and on behalf of the Provider Partners and CCG Partners that PKB shall have no liability to any person under or in connection with this Agreement (including to any Provider Partner or CCG Partner) other than the Host.

9.6 The Host for itself and on behalf of the Provider Partners and CCG Partner acknowledges and agrees that PKB's aggregate liability arising under or in connection with this Agreement and the Underlying Commercial Agreement and the Assurance Agreement to the Host and in respect of any Provider Partner or other CCG Partner:

9.6.1 including liability arising out of or in connection with PKB's (which includes any of PKB's employees, consultants, agents, sub-contractors or associates) acts and/or omissions under or in connection with this Agreement and/or the Underlying Commercial Agreement and/or the Assurance Agreement; and

9.6.2 including any and all claims, liens, actions, suits, causes of action, debts, fines, losses, liabilities, penalties, costs or expenses of whatever kind or nature (including legal fees, expenses, damages, judgments and/ or orders), arising out of any demand, claim or action, or breach of contract, equity, negligence, misconduct, breach of statutory duty or non-compliance with any Applicable Law and

9.6.3 which have existed or may have existed, or which do exist or which shall or may exist, based on any facts, circumstances, events, actions or omissions occurring prior to the date of this Agreement (or the Underlying Commercial Agreement and/or the Assurance Agreement) which concern or relate in any way to, or arise out of, or are pursuant to this Agreement (or the Underlying Commercial Agreement and/or the Assurance Agreement),

brought by any person against PKB (which includes any of PKB's employees, agents, consultants, sub-contractors or associates) shall not exceed a sum equivalent to five million Pounds (£5 million) in the aggregate.

9.7 The aggregate liability of the Host to PKB under or in connection with this Agreement or the Assurance Agreement arising out of or in connection with the Host's or any Provider Partner or CCG Partner (or any of their respective employees, consultants, agents, sub-contractors or associates) acts or omissions under this Agreement or the Assurance Agreement shall not exceed a sum equivalent to five million pounds (£5m) in the aggregate including all claims, liens, actions, suits, cases of action, debts, fines, losses, liabilities, penalties, costs or expenses of whatever kind or nature (including legal fees, expenses, damages, judgments and/or orders) arising out of any demand, claim or action, or breach of contract, equity, negligence, misconduct, breach of

statutory duty or non-compliance with any Applicable Law which has existed or may have existed, or which do exist or which shall exist, based on any facts, circumstances, events, actions or assurances occurring prior to the date of this Agreement (or the Assurance Agreement), which relate in any way to, or arise out of, or are pursuant to this Agreement or the Assurance Agreement.

9.8 Without prejudice to the limits on PKB's liability in clause 9.6 above, and subject to clause 9.8 below, PKB agrees that the following shall be deemed to be direct losses for the purpose of this Agreement:

9.8.1 any final award by a court of competent jurisdiction against any Provider Partner who is an original signatory to the ISA;

9.8.2 any settlement of any claim agreed by any Provider Partner who is an original signatory to the ISA provided that such settlement is approved by PKB (such approval not to be unreasonably withheld or delayed) before it is agreed; and

9.8.3 evidenced costs and expenses incurred by any Provider Partner who is an original signatory to the ISA; and

9.8.4 [any fine imposed by the Information Commissioner's Office where the fine is final and rights of appeal have been exhausted,

in each case where reasonably incurred as a consequence of a breach of this Agreement (or the Underlying Commercial Agreement and the Assurance Agreement) by PKB.

9.9 The Host shall not bring or threaten a claim against PKB in relation to any actual or alleged breach of this Agreement without first obtaining the approval of the Governing Group. Each of PKB and the Host shall (and the Host shall, for the purposes of direct losses which fall within clause 9.6 above, ensure that each Provider Partner and/ or each CCG Partner shall) use its reasonable endeavours to mitigate all of its and their losses, liabilities, claims, costs, expenses and other sums and detriments incurred under or in connection with this Agreement as a result of any act or omission (or alleged act or omission) of either Party.

9.10 In no event shall the Host or PKB be liable to the other for any: loss of profits; loss of business; loss of revenue; loss of or damage to goodwill; loss of savings (whether anticipated or otherwise); and/or any indirect, special or consequential loss or damage.

9.11 Nothing in this Agreement shall be construed to limit or exclude either Party's liability for:

9.11.1 death or personal injury caused by its negligence or that of its staff;

9.11.2 bribery, fraud or fraudulent misrepresentation by it or its staff;

9.11.3 any other matter which, by Applicable Law, may not be excluded or limited.

9.12 This clause 9 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 Underlying Commercial Agreement has been terminated and PKB has ceased to Process the Data in any manner whatsoever; and

- 10.1.2 PKB has ceased to have any Data under its custody or control.
- 10.2 PKB may not terminate this Agreement except where it has given notice to terminate the Underlying Commercial Agreement. The Host may terminate this Agreement at any time by giving at least thirty (30) days' notice in writing to PKB.
- 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 PKB if PKB commits a material breach of this Agreement or the Assurance Requirements 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 Underlying Commercial Agreement and/or the Assurance Requirements.
- 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, 4, 6 and 9) 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).
- 10.6 For the avoidance of doubt, where PKB is providing Patient Access Services, those services and any processing of data PKB performs as data controller in the provision of those services shall be terminated in accordance with any express terms agreed with relevant service users.

11. GENERAL PROVISIONS

11.1 Consideration

In consideration of PKB entering into this Agreement, the Host shall pay PKB the sum of £1.00 (one pound sterling), the receipt and sufficiency of which PKB 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 first approved by the Governing Group and evidenced in writing, signed by the Parties.

11.5 Third Party Rights

A person who is not a Party to this Agreement shall have no right under or pursuant to the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

11.6 Assignment

PKB 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

Without prejudice to clause 9 ("Warranties and Liability") this Agreement contains the entire understanding and agreement of the Parties in respect of the Processing of the Data on behalf of the Host and supersedes all prior oral or written communications and agreements between the Parties. This Agreement may not be amended except in writing signed by authorised representatives of both the Host and PKB. 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. For the avoidance of doubt, the ISA, the Assurance Agreement and the Underlying Commercial Agreement are separate agreements for the purposes of this clause 11.7.

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.

Email addresses for service are as follows:

For Imperial [] copied to []

For PKB []

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 Jan Norman
Jan Norman (Jun 29, 2016)
Name Jan Norman
Position Director of Quality & Safety

(PLEASE COMPLETE IN CAPITALS)

EXECUTED by the Parties
for and on behalf of
PATIENTS KNOW BEST LIMITED

Signature Mohammad Al-Ubaydli
Mohammad Al-Ubaydli (Jun 16, 2016)
Name Mohammad Al-Ubaydli
Position CEO

(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 Underlying Commercial Agreement 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 PKB);
"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);
"CIE Care Record"	means the Care Information Exchange (CIE) Shared Record which is the interoperable real time information transferred direct from NHS and social care provider systems for the purposes of direct care to be implemented by PKB in North West London in accordance with the Underlying Commercial Agreement;
"Data"	means any information in the dataset to be agreed by the parties from time to time which constitutes Personal Data or is capable of constituting Personal Data, and is provided to or made available to PKB by or on behalf of the Host or any other CCG Partner or Provider Partner and is Processed in any manner whatsoever by PKB in connection with the CIE Care Record in PKB's capacity as sub-processor;
"Data Controller"	shall have the meaning given to it under section 1(1) of the Data Protection Act;
"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;
"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 PKB;
"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 and other Confidential Information, copyright, database rights, design rights, rights in trademarks, rights in domain names and website addresses and other rights in trade names, know-how, rights in software and rights in inventions, semi-conductor topography rights, and all other analogous intellectual property rights (whether or not registered or capable of registration in any jurisdiction 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);
"Patient Access Services"	means the patient accessible record provided by PKB pursuant to the Underlying Commercial Agreement;
"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 PKB and PKB's Personnel;
"PKB Sharing Network"	means the network of healthcare providers sharing Data and information through the CIE Care Record;
"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 (including, for the avoidance of doubt, any incident emanating from or within PKB Sharing Network) 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 of 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 Underlying Commercial Agreement;
"Underlying Commercial Agreement"	means the call-off contract entered into on 27 March 2015 between PKB and Imperial College Healthcare NHS Trust under the framework agreement entered into on or around the same date between PKB and the Minister for the Cabinet Office (acting through Crown Commercial Service), pursuant to which PKB is to provide certain services that involve the Processing by PKB of Data;
"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 the Schedule.
- 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 PKB's obligations under this Schedule relate only to the provision of services relating to the implementation and maintenance of the CIE Care Record.
- 1.2 PKB 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:
 - 1.2.1 PKB shall have management arrangements in place for the management of information security;
 - 1.2.2 PKB shall comply with the IG Toolkit assessment, reporting and audit requirements relevant to its organisation type; and
 - 1.2.3 PKB shall have appropriate operational risk assessment and management processes in place for the identification, mitigation and management of operational security risks.
- 1.3 PKB shall also ensure that systems used to carry out processing under this Agreement are certified under ISO 27001 – Information Security Management. PKB shall provide a copy of the relevant ISO certificate upon request.
- 1.4 The Parties shall agree, and PKB shall have in place, an information security policy that is supported by appropriate organisational, security and technical security standards (the “**Security Policy**”).
- 1.5 PKB 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.
- 1.6 PKB 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.
- 1.7 PKB 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.
- 1.8 PKB 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 PKB 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 financial services industry.

- 2.2 PKB 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 PKB 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 PKB 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 PKB shall track, co-ordinate, implement, manage and maintain all security changes across the Services Environment.
- 3.2 PKB 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. PKB shall have regard to the confidentiality and sensitivity contained within the Services Environment and shall ensure that measures applicable to a UK financial services company are in place to prevent unauthorised access.

4. **SECURITY AUDIT**

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

5. **NON-COMPLIANCE REPORTING**

- 5.1 PKB shall monitor, on an ongoing basis, computer and network security configurations.
- 5.2 PKB 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 PKB shall administer the provision of access to the Services Environment (by both Host Personnel and PKB Personnel), Data and any other applicable data in accordance with Good Industry Practice.
- 6.2 PKB 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. PKB shall also keep records of which personnel have accessed the Services Environment (including details of login and logout times).
- 6.3 PKB shall restrict user access to information and data held on external networks.

7. **CRYPTOGRAPHY MANAGEMENT**

- 7.1 PKB 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 PKB 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 PKB 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 PKB 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 To the extent the Services are hosted by PKB utilising its own services and infrastructure, PKB shall ensure that no-one, other than properly authorised PKB Personnel, has physical access to any servers in scope under this Agreement or used to deliver the Services, including any servers located at PKB's facilities without formal documented approval from the Host.
- 8.5 In relation to PKB's facilities, PKB 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 PKB 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 a UK Financial Services company.

9. SECURITY AWARENESS

PKB 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 PKB Personnel shall, as at the commencement of the Services, be deemed to be appropriately screened and trained to a level befitting a financial services company.

10. SECURITY INCIDENTS AND MATERIAL RISK REPORTING

- 10.1 PKB 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
 - 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, PKB 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 PKB 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**

PKB 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 4 of this Agreement.

12. **DOCUMENTATION AND RECORD PRESERVATION**


12.1 PKB shall protect all Data held by PKB 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 PKB shall ensure that any documentation or records relating to the Services being disposed of by or on behalf of PKB 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, PKB will work with the Host to ensure that Clause 6 of this Agreement is complied with in respect of any and all Data under PKB's custody or control.

12.4 PKB 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 7.2, PKB 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, PKB shall deliver all Records to the Host, unless otherwise instructed by the Host. Any return or destruction of any Records by PKB must be done securely and in compliance with the information security controls maintained by PKB under this Agreement and, in the case of destruction, in accordance with the then-current standard of CESC or any successor body.

Signature: 
Mohammad Al-Ubaydli (Jun 15, 2016)

Email: mohammad@patientsknowbest.com

Title: CEO

Company: Patients Know Best

Signature: 
Jan Norman (Jun 29, 2016)

Email: jan.norman2@nhs.net

Title: Director of Quality & Safety

Company: Brent CCG