DATA PROCESSING AGREEMENT

BETWEEN

NORTH CENTRAL LONDON PARTNERS

and

HARINGEY CLINICAL COMMISSIONING GROUP

and

CERNER HEALTHCARE SOLUTION PRIVATE LTD

and

CERNER CORPORATION

THIS DATA PROCESSING AGREEMENT ("Data Processing Agreement") is made:

BETWEEN:

(1) **NORTH CENTRAL LONDON PARTNERS** (the **"Partners"**) (Listed in SCHEDULE 3)

(2) **NHS HARINGEY CLINICAL COMMISSIONING GROUP** whose address is River Park House, 225 High Road, Wood Green, London, N22 8HQ (the "**Data Processor**");

(3) Cerner Corporation whose registered office is 2800 Rockcreek Parkway, North Kansas City, MO 64117, United States of America (**"Cerner US"**); and

(4) Cerner Healthcare Solutions Private Ltd whose principal place of business is Ground Floor, Wing B, Block H2, Mountain Ash, Manyata Embassy Business Park, Outer Ring Road, Nagawara, Bangalore 560 045, India (**"Cerner India"**)

each referred to in this Data Processing Agreement as a "Party" and collectively as the "Parties".

BACKGROUND

(A) The Data Processor has procured certain IT services from **"Cerner Limited"** on behalf of the Partners, under an Agreement (as defined in paragraph 1.1 below) and pursuant to which the Partners are deemed **"Service Recipients"**.

(B) The purpose of this Data Processing Agreement is twofold:

a. to ensure that the Processing of Partners' Personal Confidential Data carried out by the Data Processor in connection with the Agreement complies with the Data Protection Legislation; and

b. to ensure compliance by the relevant Partners to the mandatory Standard Contractual Clauses which ensure an adequate level of protection for the Processing of Partners' Personal Confidential Data by the Sub-Processor and for the transfer of Partners' Personal Confidential Data outside the European Economic Area for the purposes of the services to be performed by Cerner US and Cerner India pursuant to the Agreement.

(C) For absolute clarity and completeness, it is expressly recognised that the Partners enter into this Agreement further to the Data Sharing Agreement version 1, by approval of the Data Sharing Agreement through the Data Controller Console by each individual Partner. The Partners do so in their capacity as Joint Data Controllers as further set out in that Data Sharing Agreement. This Data Processing Agreement also takes account of the wider relationship involving Partners and use of their Personal Confidential Data by the Data Processor in relation to provision of the Health Information Exchange (HIE) solution set out in the Agreement.

(D) With respect to the Parties' rights and obligations under this Contract, the Parties acknowledge that the Partners are Data Controllers and that Haringey Clinical Commissioning Group is a Data Processor (on behalf of the Partners and to the extent required in connection with the delivery of the Services) in relation to the Partners' Personal Data.

(E) It is expressly recognised by the Partners that the Data Processor will further enter into a Sub-Data Processing Agreement with Cerner Limited in connection with the Services to be delivered under the Agreement.

THE PARTIES AGREE AS FOLLOWS:

1. Definitions and Interpretation

1.1. In this Data Processing Agreement the following defined terms shall apply. Any other defined terms used in this Data Processing Agreement or applicable to its interpretation shall be as defined in Schedule 1 of the Agreement:

"**Agreement**"	means the Call off Terms and Conditions for the Supply of Services relating to A Health Information Exchange and Population Health Management & Analytics between NHS Haringey Clinical Commissioning Group and Cerner Limited dated 28 March 2018.
"**Partners' Personal Data**"	means Personal Confidential Data Processed by the Data Processor on behalf of the Partners under or in connection with the Agreement.
"**Controller"**	shall have the meaning set out in the Data Protection Legislation.
"**Data Protection Legislation"**	means all applicable data protection and privacy legislation including Regulation (EU) 2016/679 the "General Data Protection Regulation" or "GDPR") or, in the event that the UK leaves the European Union, all legislation enacted in the UK in respect of the protection of personal data, the Privacy and Electronic Communications (EC Directive) Regulations and the Data Protection Act 2018 (all as amended, updated or re-enacted from time to time).
"**Data Subject**"	shall have the meaning set out in the Data Protection Legislation.
"Data Sharing Agreement"	means the Data Sharing Agreement defined in Recital (C) above.
"**Personal Confidential Data**"	shall have the meaning set out in the Data Protection Legislation.
"**Processing"**	shall have the meaning set out in the Data Protection Legislation ("**Process**", **"Processing"** and "**Processed**" shall be construed accordingly).
"Processor(s)"	shall have the meaning set out in the Data Protection Legislation.
"**Regulator**"	shall mean the Information Commissioner's Office and the European Data Protection Board or any successor body to either regulator from time to time and any other supervisory Partners with jurisdiction over either Party.
"Partners"	shall have the meaning given in the Agreement.
"**Standard Clauses**"	means the standard contractual clauses for Data Processors approved by the EU Commission for transfer of Personal Confidential Data outside the EEA, and as further set out in Schedule 2.

"Sub-Data Processing Agreement"	means the further data processing agreement between Haringey Clinical Commissioning Group and Cerner Limited dated 31 January 2019.

1.2. The headings are to be ignored in construing this Data Processing Agreement.

1.3. Words or phrases importing the singular are to be interpreted to include the plural and vice versa, unless the context otherwise requires.

1.4. To the extent any other provision of the Agreement conflicts with this Data Processing Agreement, the terms of the Data Processing Agreement shall prevail.

2. General

2.1. The Data Processor and Cerner Limited previously entered into the Agreement, as defined above, for the provision of IT services and pursuant to which the Data Processor has procured the Data Processing from Cerner Limited on behalf of the Partners. This Data Processing Agreement shall apply to the services under that Agreement, and in particular the details contained therein outlining the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Partners' Personal Confidential Data and categories of Data Subjects.

2.2. The Parties to this Data Processing Agreement hereby agree with respect to each Party performing their respective obligations hereunder in order for the Partners and Partners to benefit from the services under the Agreement the Data Processor and Partners shall perform their respective obligations set out in this Data Processing Agreement.

3. General Obligations

3.1. This Data Processing Agreement applies to any Processing undertaken by the Data Processor (or any of its sub-Processors, appointed from time to time), on behalf of the Partners.

3.2. The Parties acknowledge that the Partners instruct the Data Processor as Joint Data Controllers of the Partners' shared Personal Data, as further set out in the Data Sharing Agreement. The Data Processor shall be entitled to rely on the instructions of the Partners, such instructions to be given in writing, only. The Data Processor shall process Partners' Personal Confidential Data on their behalf. The details of such Processing by the Data Processor are set out in Schedule One which is appended to this Data Processing Agreement.

3.3. The Parties also acknowledge that, in accordance with Part A of the Data Sharing Agreement, the Partners act as sole Data Controllers when disclosing for transfer or accessing any Personal Data Processed by the Data Processor, including circumstances in which data is held on the HIE repository servers within the Sub-Data Processor's (Cerner) data center, in order to share data with other Partners. In such instances, those Partners are the sole Data Controller for their data until it is shared with other Partners, who will in turn also be acting as sole Data Controllers in respect of their access to the data in question.

3.4. The Data Processor shall comply with its obligations under the Data Protection Legislation in respect of any Partners' Personal Confidential Data it Processes in connection with the Agreement. The Partners hereby warrants and represents to the Data Processor that any instructions it issues in respect of the Partners' Personal Confidential Data are lawful and to the best of its knowledge any instructions issued on behalf of other Partners are also lawful.

3.5. Cerner Limited is an approved sub-Processor of the Data Processor and Cerner US and Cerner India are approved sub-sub-Processors of Cerner Limited, appointed in accordance with clause 7.5 of this Data Processing Agreement, subject to Cerner US and Cerner India entering into the Standard Contractual Clauses for Processors outside of the EEA as approved by the EU Commission, in accordance with clause 7.2.2 of this Data Processing Agreement.

3.6. The Data Processor shall, directly or through its permitted sub-Processors, enter into, manage and enforce the provisions of, the Agreement and this Data Processing Agreement as necessary to deliver the following purposes (hereafter referred to as the **"Purposes"**):

3.6.1. to integrate Personal Confidential Data concerning health and care needs from multiple electronic health and care systems in order to enable the Partners (health and care providers) access to 'real time' data and provide the best possible care for their patients **(the "Direct Care and Administration Purpose").** In instances where this is not possible, alternative approaches will be used to receive and hold the data sent from source systems within the HIE database. This will be securely held within the HIE data repository on servers within Cerner's data centre.

3.6.2. to maintain and administer the HIE system, including by human intervention where required to ensure the NHS numbers are matched accurately; patient data will not be amended to support matching **(the "Maintenance and Administration Purpose");**

3.7. The Data Processor shall carry out its obligations under this Data Processing Agreement in compliance with the Data Protection Legislation.

3.8. The Data Processor shall, directly or through its permitted sub-Processors, comply with its obligations as a Processor, and specifically shall (and shall, so far as possible, ensure that any sub-Processor shall):

3.8.1. Process Partners' Personal Confidential Data only in accordance with instructions from the Partners, which may be specific instructions or instructions of a general nature as set out in this Data Processing Agreement;

3.8.2. Process the Partners' Personal Confidential Data only to the extent, and in such manner, as has been approved by the Partners and as is necessary for the Purposes or, as is required by law or any Regulatory or Supervisory Body. For the avoidance of doubt this shall include:

3.8.2.1. acting as lead for the maintenance & configuration of the Health Information Exchange (HIE) system;

3.8.2.2. managing complaints or a potential/suspected unauthorised release, disclosure or access to Partners' Personal Confidential Data or any part thereof; and

3.8.2.3. conducting system audits when and where required.

3.8.3. ensure the reliability of any Data Processor, or sub-Data Processor, personnel who have access to Partners' Personal Confidential Data by imposing upon them an explicit duty of confidentiality, and will further ensure that all such personnel will comply with the obligations set out in this Data Processing Agreement;

3.8.4. implement appropriate technical and organisational measures to protect Partners' Personal Confidential Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, as further set out in clause 4 of this Data Processing Agreement. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the data and having regard to the nature of the Partners' Personal Confidential Data which is to be protected;

3.8.5. ensure that none of the Data Processor personnel publish, disclose or divulge any of the Partners' Personal Confidential Data to any third party unless directed in writing to do so by the Partners;

3.8.6. notify the Partners without undue delay within five (5) Working Day if it receives:

3.8.6.1. a request from a Data Subject to have access to their Personal Data; or

3.8.6.2. a complaint relating to the Data Processor's obligations under the Data Protection Legislation; or

3.8.6.3. receive any request from a Data Subject of the Partners' Personal Data, exercising its rights under the Data Protection Legislation.

3.8.7. provide the Partners with appropriate cooperation and assistance in relation to any complaint or request made, including by:

3.8.7.1. providing all available details of the complaint or request;

3.8.7.2. assisting the Partners to comply with a subject access request within one (1) calendar month timescale set out in the Data Protection Legislation or in accordance with the Partners' reasonable instructions; and

3.8.7.3. providing the Partners with any Partners' Personal Confidential Data it holds in relation to a Data Subject.

3.8.8. where required, provide a written description of the technical and organisational methods employed for Processing Partners' Personal Confidential Data within reasonable timescales; and

3.8.9. not transfer any Partners' Personal Confidential Data country outside the EEA or the UK unless instructed by the Controller to make the particular transfer or otherwise permitted in accordance with this Data Processing Agreement.

3.9. The Data Processor shall not make or permit the making of any further copies of the Partners' Personal Data, except for back-up copies as necessary, and except where de-identified/pseudonymised in accordance with this Data Processing Agreement or approved by the Partners.

3.10. The Data Processor shall maintain and implement a business continuity and disaster recovery plan to the reasonable satisfaction of the Partners

3.11. Where the Data Processor exceeds its role as a Data Processor by determining the purposes and means of Processing Partners' Personal Data, the Data Processor shall be considered to be a Data Controller in respect of that processing, and shall be liable to:

3.11.1. any right to compensation from a data subject who may have suffered material or non-material damage as a result of the infringement; and

3.11.2. imposition of administrative fines or penalty from the Information Commissioner.

3.12. The Data Processor shall ensure that on the expiry or termination of this Data Processing Agreement, the Partners' Personal Confidential Data is returned to the Partners, destroyed in accordance with Partners' instructions or migrated to an alternative system/software provider in accordance with instructions of the Partners and shall ensure that no Partners' Personal Confidential Data is retained by any sub-Processor or sub-sub-Processor.

3.13. The Data Processor shall ensure it is compliant with the standards and techniques of data protection by design and data protection by default. Such measures shall in include appropriate technical and organisational measures for pseudonymisation and data minimisation.

3.14. The Data Processor shall ensure that Partners' Personal Confidential Data that has had "right to object" or "right to restrict" exercised are not held longer than necessary in its data repository. Therefore, the Data Processor shall ensure it has a written policy and procedure for the archiving, retention and disposal of information which complies with the Records/ Management Codes of Practice for Health and Social Care 2016.

3.15. The Data Processor warrants and undertakes to the Partners that:

3.15.1. it shall only Process Partners' Personal Confidential Data in accordance with the instructions of the Partners which are set out in Schedule One of

this Data Processing Agreement, or as provided in writing by the Partners to the Data Processor from time to time;

3.15.2. it shall comply with its obligations under the Data Protection Legislation when Processing Partners' Personal Confidential Data including, but not limited to, its obligations to ensure the secure transfer of Partners' Personal Confidential Data to its sub-Processors;

3.15.3. taking into account the nature of the Processing and the information available to it, the Data Processor shall provide reasonable assistance and co-operation to the Partners as requested by the Partners from time to time to ensure the Partners' compliance with its obligations under the Data Protection Legislation, including in respect of:

3.15.3.1. data protection impact assessments and prior consultation with the UK Information Commissioner's Office;

3.15.3.2. implementing appropriate measures to mitigate against any data protection risks; and

3.15.3.3. any other steps which the Partners are required to take in order to comply with its obligations under the Data Protection Legislation.

3.15.4. taking into account the nature of the Processing, implementing technical and organisational measures, insofar as is possible, to enable the Partners to respond to requests from Data Subjects exercising their rights under the Data Protection Legislation which shall include but not be limited to:

3.15.4.1. providing Partners' Personal Confidential Data and details of the Processing of Partners' Personal Confidential Data to the Partners in response to a subject access request, which may be done via the Data sub-Processor's audit tools known as 'P2 Sentinel' and "Cerner Sentinel"; and

3.15.4.2. deleting and/or rectifying Partners' Personal Confidential Data as requested by the Partners; and

3.15.4.3. providing reasonable assistance with any enquiries from Regulators.

3.15.5. it shall ensure that appropriate controls including Role Based Access Control ("RBAC") are implemented where access to HIE is via the web-portal or via a context sensitive link embedded in source systems, in order to ensure such access can be monitored and audited. Evidence of audit shall be made available on request by the Partners;

3.15.6. it shall ensure for all accesses of Partners' Personal Data, the audit trail shall identify the following information:

3.15.6.1. name of staff member accessing the system;

3.15.6.2. usage detailing date/time and location;

3.15.6.3. usage report;

3.15.6.4. snap shots of aggregated information viewed.

3.16. The Data Processor shall notify the Partners promptly should it:

3.16.1. receive notice of any complaint made to a Regulator or any finding by a Regulator in relation to its Processing of Partners' Personal Data;

3.16.2. be subject to any finding by a Regulator in relation to its Processing of any Personal Confidential Data which the Data Processor Processes on the same IT systems that are used to provide the services to the Partners under the Agreement; or

3.16.3. be under a legal obligation to Process the Partners' Personal Data, other than under the instructions of the Partners, in which case it shall inform the Partners of the legal obligation, unless the law prohibits such information on important grounds of public interest.

3.17. The Data Processor shall only transfer the Partners' Personal Confidential Data Processed under this Data Processing Agreement outside the European Economic Area ("**EEA**") and the UK to Cerner US and Cerner India in accordance with the Standard Contractual Clauses for Processors as approved by the EU Commission and as set out at Schedule 2 to this Data Processing Agreement or, where applicable, the Privacy Shield.

4. Security

4.1. When Processing Partners' Personal Confidential Data under this Data Processing Agreement the Data Processor shall take appropriate technical and organisational precautions and measures, as further set out under Schedule 1 and this clause 4 (together known as "the Security Measures"), to preserve the confidentiality and integrity of the Partners' Personal Confidential Data and prevent any unlawful Processing or disclosure, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects. These shall include, but not be limited to:

4.1.1. complying with the Data Protection Legislation

4.1.2. maintaining ISO 27001 accreditation;

4.1.3. encrypting Partners' Personal Confidential Data stored or transmitted between client and Cerner data center over public;

4.1.4. implementing and maintaining business continuity, disaster recovery and other relevant policies and procedures to ensure:

4.1.5. the confidentiality, integrity, availability and resilience of Processing systems and services;

4.1.6. the availability and access to Partners' Personal Confidential Data in a timely manner in the event of a physical or technical incident; and

4.1.7. backup of servers to the extent necessary to maintain the service and retain audit trails

4.1.8. completion of the Data Security and Protection (DSP) Toolkit introduced in the National Data Guardian review of data security, consent and opt-outs, and adhere to robust information governance management and accountability arrangements.

4.1.9. use of 'user access authentication' mechanisms to ensure that all instances of access to any Partners' Personal Confidential Data under the Health Information Exchange (HIE) system are auditable against an individual. The auditing process shall include:

4.1.9.1. Job role and name of staff member accessing the system;
4.1.9.2. Organisation name;
4.1.9.3. Usage detailing date/time, user information, role, and location
4.1.9.4. Usage report

4.1.10. ensuring that security measures such as, access log files, access controls, network security, monitoring and enforcement of user access are in place to ensure restricted/limited access to records on the HIE system;

4.1.11. demonstrating compliance with the standards and techniques of data protection by design and data protection by default. Such measures shall include appropriate technical and organisational measures for pseudonymisation data minimisation; and

4.1.12. ensuring that all employees and contractors who are involved in the Processing of Partners' Personal Confidential Data are suitably trained in maintaining the privacy and security of the Partners' Personal Confidential Data and are under contractual or statutory obligations of confidentiality concerning the Partners' Personal Data.

4.2. The Data Processor shall afford Partners' Personal Confidential Data the appropriate industry standards of storage including ensuring that hardware utilised for the Purposes is kept in a physically secure environment protected by a fully managed industry standard firewall.

4.3. The Data Processor shall use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of malicious software.

4.4. The Data Processor shall regularly audit access to the HIE system and provide reports to the Partners upon request.

4.5. The Security Measures shall be regularly tested by the Data Processor to assess the effectiveness of the measures in ensuring the security, confidentiality, integrity, availability and resilience of the Partners' Personal Confidential Data and shall maintain records of the testing.

4.6. Further to clause 4.3, the Data Processor will provide, a "Penetration Testing Attestation Letter," which shall describe the penetration testing that was performed,

confirm that an industry standard methodology, testing tools and national vulnerability database were used, and confirm that identified vulnerabilities have been remediated or are being addressed in a plan for remediation and actively monitored. These should occur at least once in every two (2) years, unless North London Digital Programme Board and/or North London Partners Information Governance Working Group decides otherwise.

5. Records of Processing

5.1. The Data Processor, and its sub-Processors and sub-sub-Processors where required, shall maintain accurate written records of the Processing it undertakes in connection with this Data Processing Agreement which shall contain at a minimum:

5.1.1. its details, the Partners' details, and the details of its data protection officers;
5.1.2. the categories of Processing carried out on behalf of the Partners;
5.1.3. the details of any transfers to any third countries, where applicable, and the safeguards in place for that transfer; and
5.1.4. an accurate record of the Security Measures it has in place.

5.2. The Data Processor shall provide the records set out in clause 3 and clause 4 to the Partners or a Regulator on request.

6. Security Breach Notification

6.1. The Data Processor shall notify the Partners without undue delay (and in any event no later than 24 hours of discovery) if it becomes aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Partners' Personal Confidential Data or any damage to, corruption of or destruction of such Personal Confidential Data("**Security Incident**").

6.2. The notification in clause 6.1 shall include:

6.2.1. the nature of the breach, including the categories and approximate number of Data Subjects and records concerned (to the extent known at the time of the report);
6.2.2. the contacts at the Data Processor who will liaise with the Partners concerning the breach; and
6.2.3. the remediation measures being taken to secure the affected Partners' Personal Data, mitigate and contain the breach,

and the Data Processor shall provide regular updates to the notification, as more facts become known and to set out the effects of the remediation measures.

6.3. In the event of a Security Incident, the relevant Partner shall at its sole discretion determine whether to provide notification to the Data Subject, any third party or Regulator and the Data Processor shall not notify the Data Subject, any third party or Regulator unless such disclosure by the Data Processor is required by law or is otherwise approved by the relevant Partner as applicable. The relevant Partner shall

approve all notifications to Data Subjects, third parties or Regulators which it determines are required or appropriate.

7. Sub-Processing

7.1. The Data Processor shall not provide any third party with access to the Partners' Personal Confidential Data or engage any sub-Processors or sub-sub-Processors to perform its obligations under this Data Processing Agreement without the prior written approval of the Partners and a written contract for sub-Processing or sub-sub-Processing. A written contract shall not be required for sub-sub-Processors within Cerner Limited`s group of companies insofar as the sub-sub-Processors are otherwise legally bound to comply with the obligations of a Processor under this Data Processing Agreement and applicable law.

7.2. Where authority has been granted by the Partners to the Data Processor to engage any sub-Processor or sub-sub-Processor in accordance with clause 7.1, the Data Processor shall:

7.2.1. undertake reasonable due diligence on the sub-Processor or sub-sub-Processor to ensure their ability to comply with the obligations of this Data Processing Agreement; and

7.2.2. put in place contractual data processing, information security and confidentiality provisions equivalent to those in place between the Data Processor and the Partners under this Data Processing Agreement, unless the sub-sub-Processor is part of Cerner Limited's group of companies.

7.3. The Data Processor shall remain liable for the acts and omissions of its sub-Processors and sub-sub-Processors, including the Processing activities of such sub-Processors or sub-sub-Processors. For the avoidance of doubt this includes, but is not limited to, any breach of the sub-Processors' or sub-sub-Processors' obligations under Schedule 1 of this Data Sharing Agreement.

7.4. At the Partners's request, the Data Processor will provide information as to which sub-Processors or sub-sub-Processors are operating on its behalf, and provide reasonable information to demonstrate how those sub-Processors or sub-sub-Processors have ensured compliance with the Data Protection Legislation.

7.5. With effect from the Commencement Date, the Data Processor is authorised to appoint the following sub-Processors and sub-sub-Processors in order to fulfil its obligations under this Data Processing Agreement, such obligations may include, but are not limited to, Processing Partners' Personal Confidential Data on behalf of the North London Health and Care Partners:

7.5.1. Cerner Limited;
7.5.2. Cerner US;
7.5.3. Cerner India; and
7.5.4. Cerner's affiliated Group companies established in the EEA, e.g. Ireland.

7.6. The Data Processor must assess the sub-Processor's and sub-sub-Processor's compliance with those obligations on a regular basis.

8. Audit

8.1. The Data Processor shall provide all reasonable necessary information and assistance to the Partners in order for the Partners to verify the Data Processor's compliance with its obligations under this Data Processing Agreement and the Data Protection Legislation including:

8.1.1. submitting to the Partners all information, and documentation reasonably necessary to demonstrate compliance with the Data Processing Agreement, Data Protection Legislation and Security Measures; and

8.1.2. allowing access to the Data Processor premises on reasonable notice and provide all reasonable assistance to the Partners to enable the Partners (or a third party appointed by the Partners and bound by appropriate obligations of confidentiality) to audit the Data Processor's compliance with the Data Processing Agreement, Data Protection Legislation and Security Measures, provided the Partners shall not (apart from in reasonable circumstances) be permitted to inspect and audit the Data Processor's Data Processing activities on more than one occasion in any Agreement Year and upon reasonable and timely advance agreement. The Partners shall bear the costs of any such on-site audit.

8.2. In relation to its obligations under this clause 7, the Data Processor shall immediately inform the Partners if, in its opinion, an instruction received from the Partners infringes the Data Protection Legislation.

9. Term and Termination

9.1. Unless otherwise required by law, the Data Processor shall, upon termination or expiry of the Agreement for whatever reason, at the option of the Partners, either, securely delete or return all Partners' Personal Confidential Data to the Partners or the relevant Partners and comply with all other applicable provisions set out in the Agreement with respect to Partners' Personal Confidential Data on expiry or termination. If required by law to retain a copy, the Data Processor shall inform the Partners what it is retaining and the legal reason why it needs to be retained.

10. Liability

10.1. Subject to clause 10.2 below, the liability of each Party under or in connection with this Data Processing Agreement, including: (a) under the Standard Clauses; and/or (b) to any Service Recipient exercising their right as a third party beneficiary under the Agreement, shall be limited to £5 million per annum in aggregate. For the avoidance of doubt, the Data Processor, Cerner Limited, Cerner India and Cerner US shall be deemed a 'Party' for the purposes of this clause 10.1, and the limit of liability set out in this clause for a Party shall be an aggregate figure between them.

10.2. No Party limits its liability: (a) for death or personal injury caused by its negligence; or (b) for fraud or fraudulent misrepresentation by it or its employees; or (c) owed directly by the Party to a Data Subject under Clause 3 of the Standard Clauses; or (d) any other liability which cannot be excluded or limited by law.

10.3. Subject to clause 10.2, no Party will be liable for: (a) any indirect, special or consequential loss or damage; or (c) any loss of profits, turnover, business opportunities or damage to goodwill (whether direct or indirect).

10.4. The Data Processor, Cerner Limited, Cerner India and Cerner US shall remain independently liable for complying with their respective obligations under this Data Processing Agreement, including the Standard Clauses, and nothing herein shall be considered to constitute joint and several liability between the Parties towards the Partners.

11. Governing law

11.1. Without prejudice to clauses 7 and 9 of the Standard Clauses, this Data Processing Agreement shall be governed and interpreted in all respects by the law of England and Wales and the Parties hereby submit to the exclusive jurisdiction of the courts of England.

12. Disputes and Changes

12.1. Any dispute or change to this Data Processing Agreement shall be governed by Clause 27 or Schedule 8.2 of the Agreement respectively.

SIGNED for and on behalf of

NHS Haringey Clinical Commissioning Group by

Name	Karl Thompson
Position	SIRO for Haringey and Islington CCGs
Date	14/11/2019

NCL Partners by individual Partners entering into the Data Sharing Agreement through the Data Controller Console

SCHEDULE ONE

Information required	**Response**
The precise nature of the services provided by the Data Processor to the Partners and the purposes of processing	• Provide the software for the HIE system • Provide implementation systems services and hardware infrastructure • Provide ongoing support and maintenance of the hardware and Data Processor software • Providing a population health solution
Please describe the data flows between the Partners and the Partners	Partners shall transfer their Personal Confidential Data to the Data Processor, in accordance with the terms of a separate data sharing agreement between the Partners.  HIE Data Flows Diagram.pdf
Please describe the data flows (i) between the Partners and the Data Processor; and (ii) between the Data Processor and Cerner US and Cerner India which are going outside of the UK	(i) The Partners shall transfer their Personal Confidential Data directly to Cerner Limited, as Sub-Processor, pursuant to the Agreement and Sub-Data Processing Agreement between the Data Processor and Sub-Processor, and on the terms further set out in the Data Sharing Agreement." (ii) This data may be accessed by Cerner India and Cerner US. The Standard Clauses entered into between the Partners and Cerner US and Cerner India at Schedule 2 to this Data Processing Agreement, as well as the Privacy Shield in respect of data flowed to Cerner US, govern the transfer of Partners' Personal Confidential Data outside of the EEA by the Data Processor in its performance of certain IT services for the Partners.
The Partners' Personal Data	<u>Patient data</u> • name, work and home contact details (email, phone numbers, physical address) including emergency contact details for next of kin • language(s) spoken • gender • date of birth • Patient identifier e.g. NHS and Hospital numbers; • marital/civil partnership status • practice name and contact details of patient GP • domestic partners • dependants

	• specific patient encounter transaction details <u>Sensitive category data of patients:</u> • Disability status • Ethnic origin • Allergies and safeguarding alerts • Known pre-existing medical conditions • Safeguarding alerts • Diagnostic test results • Inpatient, day case and outpatient attendances • Future patient appointments • Diagnosis and treatment plans • Prescribing and drug administration record • Clinical and pre-operative assessments <u>The Partners' staff data</u> • Name • Job role • Contact details • Log in details.
Who the Partners' Personal Confidential Data relates to ie categories of data subjects (e.g. customers, employees)	• Patients being treated by or population members leveraging services delivered by the Partners and/or Partners • The Partners staff • Data Processor staff
Who owns the Partners' Personal Data? Who was it collected by? And for what purpose (e.g. was consent for marketing obtained?)	The Partners' Personal Confidential Data will belong to the Partners in their roles as the Data Controllers and it was collected for the purpose of Data Subjects' health care management and also for the wider purposes of the being used in the population health solution.
The nature of the processing (e.g. storing, analysing)	• Storing Partners' Personal Confidential Data on the project portal (SharePoint) to enable to configuration of the system. • Viewing Partners' Personal Confidential Data within the data exporter's Solution(s) for support, maintenance and troubleshooting purposes via technical remote access. • Viewing Partners' Personal Confidential Data by the data importer's support personnel in the execution of service requests through the centralised service ticketing system. • Viewing Partners' Personal Confidential Data on the tracking tool in order to perform certain build activities. • Analysing through the population health solution
The duration of the processing	For the duration of the Agreement

The organisational security measures put in place to protect the information processed for the Partners (e.g. retention periods, training, audits, business continuity and disaster recovery plans) The Partners need to ensure adequate security measures are in place. Are there any bespoke measures the Partners would like to impose?	The Data Processor will ensure it is possible to retrospectively check and determine whether and by whom Partners' Personal Confidential Data was entered into data processing systems, modified or deleted. **Measures:** The Data Processor shall only allow authorized users on the basis of a role-based authorization concept to access Partners' Personal Data. Accesses to Partners' Personal Confidential Data shall be recorded in log files and their creation, modification and deletion shall be correspondingly recorded. The Data Processor shall ensure that Partners' Personal Confidential Data is protected against accidental damage or loss. **Measures:** If Partners' Personal Confidential Data is stored, it shall be secured in state of the art redundant systems for recovery depending on its security rating. Additionally, Cerner US and Cerner India shall use uninterrupted power supplies (e.g. UPS, batteries, generators) for securing data centers. A comprehensive emergency concept shall be drawn up in writing. Emergency procedures and systems shall be regularly tested. Cerner US and Cerner India shall use firewalls and other technologies to ensure network security. Furthermore, regularly updated antiviruses and spyware filters shall be provided on the network and on all DP systems. The Data Processor shall ensure that the Partners' Personal Confidential Data which has been collected for different purposes can be processed separately. **Measures:** The Data Processor shall make sure that the Partners' Personal Confidential Data for intended purposes shall be processed as separately as possible by means of a role-based authorization concept for regulating access to the Partners' Personal Data. Furthermore, there shall be client separation on hardware and software. Partners' Personal Confidential Data shall be appropriately encrypted when stored. Test systems and productive systems shall be logically separated.
The technical security measures put in place to protect the information processed for the Partners (e.g. encryption, pseudonymisation, passwords,	The Data Processor will not allow unauthorized persons to use data processing systems and will train authorized users to only access Partners' Personal Confidential Data to the

back ups, security software, complying with security standards e.g. ISO 27001) The Partners need to ensure adequate security measures are in place. Are there any bespoke measures the Partners would like to impose?	extent strictly necessary to perform the services in the Agreement. **Measures:** Access to data processing systems (DP systems) shall only be granted to authorized users on the basis of a role-based authorization concept by means of the following measures: • Data encryption to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256 encryption for data at rest), • for HIE authentication to access data is managed through the native source system; • intrusion detection systems and intrusion prevention systems, • regularly updated anti-viruses and spyware filters on the network, on individual PCs and back up tapes • No other form of portable storage e.g. DVDs and USB sticks shall be used. The Data Processor will ensure that those who are authorized to use DP systems can only access Partners' Personal Confidential Data that they are authorized to access, and that Partners' Personal Confidential Data is not read, copied, altered or deleted without authorization after having been processed, used and stored. **Measures:** Cerner US and Cerner India shall only permit access to Personal Confidential Data on the basis of a role-based authorization concept. Furthermore, unauthorized access to Personal Confidential Data shall be prevented with appropriate data encryption to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256 encryption for data at rest). The Data Processor will ensure that Partners' Personal Confidential Data is not read, copied, altered or deleted without authorization during electronic transmission, during transportation or while stored on data carriers, and that it is possible to examine and determine where a transmission of Personal Confidential Data via data transmission facilities is intended. **Measures:** Cerner US and Cerner India shall protect electronic paths of communication through facilities, closed networks and data encryption processes to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256

	encryption for data at rest). If a transportation of data on a physical data carrier occurs, there shall be verifiable transport procedures, which shall prevent unauthorized access to data or consequential loss of data. Data carriers shall be disposed of in a way that complies with Data Protection Legislation. Care must be taken that Partners' Personal Confidential Data that is being processed as part of the assignment is only processed according to the Partners' instructions. **Measures:** The Data Processor should make use of standardized procedures to assess compliance with the Partners' instructions. The Data Processor shall implement technical precautions including intrusion detection, and segregation of Partners' Personal Confidential Data for the identification of persons giving and receiving instructions.
The physical security measures put in place to protect the information processed for the Partners (e.g. locking server rooms, CCTV) The Partners need to ensure adequate security measures are in place. Are there any bespoke measures the Partners would like to impose?	The Data Processor shall protect its buildings with sufficient entry control systems based on a security rating of the building and corresponding to a defined concept of authorized access. All buildings shall be secured by means of entry control measures. Properties, buildings or single areas shall be secured through additional means according to their security rating. This shall include special access profiles, pin pads, video surveillance and security personnel. Access rights for authorized persons shall be granted individually according to set criteria. This also applies to external persons.
Please confirm the relationship between the Data Processor, Cerner Limited, Cerner US and Cerner India	The Data Processor has procured the Services from Cerner Limited, and Cerner India and Cerner are subsidiaries of Cerner Limited.
On termination or expiry of the agreement – what would the Partners like to happen to Partners data. Returned or deleted?	At the option and request of the Partners, the Data Processor will either return or delete Partners' Personal Confidential Data in the event of termination or expiry of the Agreement (5 years from March 2018).

SCHEDULE TWO

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of Personal Confidential Data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation(s):

Name:	North Central London Partners (Listed in SCHEDULE 3)
Address:	**Available on Data Controller Console**
Tel	Available on Data Controller Console
e-mail	-Available on Data Controller Console

Other information needed to identify the organisation

Cerner client mnemonics: TBC

(the **data exporter**)

And

Name of the data importing organisation:

Name:	Cerner Corporation
Address:	World Headquarters
	2800 Rockcreek Parkway
	North Kansas City, MO 64117
	United States of America
Tel	+1-816-221-1024
Fax	-
e-mail	-

And

Name:	Cerner Healthcare Solutions Private Ltd.
Address:	Ground Floor, Wing B, Block H2, Mountain Ash
	Manyata Embassy Business Park
	Outer Ring Road
	Nagawara
	Bangalore 560 045
	India

Tel	+91 80 3301 0400
Fax	-
e-mail	-

(each a **data importer**)

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the Personal Confidential Data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Confidential Data and on the free movement of such data[1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter Personal Confidential Data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer Personal Confidential Data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of Personal Confidential Data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting Personal Confidential Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of Personal Confidential Data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the Personal Confidential Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the Personal Confidential Data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect Personal Confidential Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the Personal Confidential Data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the Personal Confidential Dataonly o n behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the Personal Confidential Data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the Personal Confidential Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the Personal Confidential Data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the laws of England and Wales.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the laws of England and Wales.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the Personal Confidential Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Confidential Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Confidential Data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the Personal Confidential Data transferred

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporters:

Name (written out in full): ……

Position: ……

Address: ……

Signature ……

On behalf of the data importer (Cerner Corporation):

Name (written out in full): ……

Position: ……

Address: ……

Signature ……

On behalf of the data importer (Cerner Healthcare Solutions Private Ltd):

Name (written out in full): ……

Position: ……

Address: ……

Signature ……

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporters are the North Central London Partners.

The data exporter are providers of health care services for certain part of the population in the United Kingdom. As the provider of health care services, the data exporters are the controllers of or may process the Personal Confidential Data(including personal health information) of the population for which the data exporters provides health care services, as well as Personal Confidential Data it has received from the Service Recipients.

Data importer

The data importers are :

(1) Cerner Healthcare Solutions Private Ltd of is Ground Floor, Wing B, Block H2, Mountain Ash, Manyata Embassy Business Park, Outer Ring Road, Nagawara, Bangalore 560 045, India ("**Cerner India**"); and

(2) Cerner Corporation of 2800 Rockcreek Parkway, North Kansas City, MO 64117, United States of America ("**Cerner US**").

The data importers are providers of health care information technology solutions and services provide outsourced services on behalf of its group company Cerner Limited The Point, 37 North Wharf Road, Paddington, London W2 1AF who is contracted to provide services to the data exporter.

The Standard Contractual Clauses shall apply as between (1) the data exporter and Cerner India; and (2) the data exporter and Cerner US and the Standard Contractually Clauses shall apply severally in respect of Cerner India and Cerner US.

The data exporter has acquired the license and right from Cerner Limited (an affiliate of data importer) to use certain electronic medical record solutions ("Solution(s)"). The data exporter purchases support, maintenance and build services for the Solution(s) from Cerner Limited under the Agreements.

The data importer will perform certain parts of the support, maintenance and build services for the Solution(s) on behalf of Cerner Limited under the Agreements as described in more detail below in section "Processing operations" of this Appendix 1.

Data subjects

The Personal Confidential Data transferred concern the following categories of data subjects (please specify):

1) *Patients being treated by the data exporters; and*
2) *Staff of the data exporters.*

Categories of data

The Personal Confidential Data transferred concern the following categories of data:

Patient data

- name, work and home contact details (email, phone numbers, physical address) including emergency contact details for next of kin
- language(s) spoken
- gender
- date of birth
- Patient identifier e.g. NHS and Hospital numbers;
- marital/civil partnership status
- practice name and contact details of patient GP
- domestic partners
- dependants
- specific patient encounter transaction details

Data exporter's staff data

- Name
- Job role
- Contact details
- Log in details

Special categories of data

The Personal Confidential Data transferred concern the following special categories of data belonging to patients:

- Disability status
- Ethnic origin
- Allergies and safeguarding alerts
- Known pre-existing medical conditions
- Safeguarding alerts
- Diagnostic test results
- Inpatient, day case and outpatient attendances
- Future patient appointments
- Diagnosis and treatment plans
- Prescribing and drug administration record
- Clinical and pre-operative assessments

Processing operations

The Personal Confidential Data transferred will be subject to the following basic processing activities:

- Storing Authority Personal Confidential Data on the project portal (SharePoint) to enable to configuration of the system.
- Viewing Authority Personal Confidential Data within the data exporter's Solution(s) for support, maintenance and troubleshooting purposes via technical remote access.
- Viewing Authority Personal Confidential Data by the data importer's support personnel in the execution of service requests through the centralised service ticketing system.
- Viewing Authority Personal Confidential Data on the tracking tool in order to perform certain build activities.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER (CERNER CORPORATION)

Name: .....

Authorised Signature .....

DATA IMPORTER (CERNER HEALTHCARE SOLUTIONS PRIVATE LTD)

Name: .....

Authorised Signature .....

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Technical and organizational measures (TOM)

1. Introduction

This document contains a description of the technical and organizational measures which have been taken by the Data Importer to protect Personal Confidential Data within the scope of the Data Importer's activities.

Personal Confidential Data shall be processed by the Data Importer in compliance with the relevant laws for Personal Confidential Data protection.

2. The Data Importer's Technical and Organizational Measures

The Data Importer shall form the internal organization within their sphere of responsibility in a way that satisfies the special requirements of data protection. The Data Importer shall preserve **confidentiality** (only those authorized to do so may gain access), **integrity** (only those entitled to do so may make modifications) and **availability** (should Personal Confidential Data be stored by the Data Importer due to contractual stipulations, this data shall remain available as is stipulated in the contract). Employees shall be regularly trained in matters of data protection. There shall be a continuous procedural directory.

2.1 Physical access control

Unauthorized access to data processing systems which process and use Personal Confidential Data will be denied by the Data Importer.

Measures:

The Data Importer shall protect their buildings with sufficient entry control systems based on a security rating of the building and corresponding to a defined concept of authorized access. All buildings shall be secured by means of entry control measures. Properties, buildings or single areas shall be secured through additional means according to their security rating. This shall include special access profiles, pin pads, video surveillance and security personnel. Access rights for authorized persons shall be granted individually according to set criteria. This also applies to external persons.

2.2 System access control

Data Importer will not allow unauthorized persons to use data processing systems and will train authorized users to only access Personal Confidential Data to the extent strictly necessary to perform the services in the Agreement.

Measures:

Access to data processing systems (DP systems) shall only be granted to authorized users on the basis of a role-based authorization concept by means of the following measures: Data encryption to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256 encryption for data at rest), individualized password allocation with min. of 8 characters, which shall automatically expire every 90 days, password protected screen saver after a 10 minute period of inactivity, intrusion detection systems and intrusion prevention systems, regularly updated anti-viruses and spyware filters on the network, on individual PCs and back up tapes No other form of portable storage e.g. DVDs and USB sticks shall be used.

2.3 Data access control

Data Importer will ensure that those who are authorized to use DP systems can only access data that they are authorized to access, and that Personal Confidential Data is not read, copied, altered or deleted without authorization after having been processed, used and stored.

Measures:

Data Importer shall only permit access to Personal Confidential Data on the basis of a role-based authorization concept. Furthermore, unauthorized access to Personal Confidential Data shall be prevented with appropriate data encryption to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256 encryption for data at rest).

2.4 Disclosure control

Data Importer will ensure that Personal Confidential Data is not read, copied, altered or deleted without authorization during electronic transmission, during transportation or while stored on data carriers, and that it is possible to examine and determine where a transmission of Personal Confidential Data via data transmission facilities is intended.

Measures:

Data Importer shall protect electronic paths of communication through facilities, closed networks and data encryption processes to NHS standards (utilizing at least TLS V1.2 encryption for data in transit and AES-256 encryption for data at rest). If a transportation of data on a physical data carrier occurs, there shall be verifiable transport procedures, which shall prevent unauthorized access to data or consequential loss of data. Data carriers shall be disposed of in a way that complies with data protection laws.

2.5 Input control

The Data Importer will ensure it is possible to retrospectively check and determine whether and by whom Personal Confidential Data was entered into data processing systems, modified or deleted.

Measures:

The Data Importer shall only allow authorized users on the basis of a role-based authorization concept to access personal data. Accesses to Personal Confidential Data shall be recorded in log files and their creation, modification and deletion shall be correspondingly recorded.

2.6 Job control

Care must be taken that Personal Confidential Data that is being processed as part of the assignment is only processed according to the Authority's instructions.

Measures:

The Data Importer should make use of standardized procedures to assess compliance with the Authority's instructions. Data Importer shall implement technical precautions including intrusion detection, and segregation of data, for the identification of persons giving and receiving instructions.

2.7 Availability control

Data Importer shall ensure that Personal Confidential Data is protected against accidental damage or loss.

Measures:

If Personal Confidential Data is stored, it shall be secured in state of the art redundant systems for recovery depending on its security rating. Additionally, the Data Importer shall use uninterrupted power supplies (e.g. UPS, batteries, generators) for securing data centers. A comprehensive emergency concept shall be drawn up in writing. Emergency procedures and systems shall be regularly tested. The Data Importer shall use firewalls and other technologies to ensure network security. Furthermore, regularly updated antiviruses and spyware filters shall be provided on the network and on all DP systems.

2.8 Separation control

Data Importer shall ensure that data which has been collected for different purposes can be processed separately.

Measures:

The Data Importer shall make sure that Personal Confidential Data for intended purposes shall be processed as separately as possible by means of a role-based authorization concept for regulating access to personal data. Furthermore, there shall be client separation on hardware and software. Personal Confidential Data shall be appropriately encrypted when stored. Test systems and productive systems shall be logically separated.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER (CERNER CORPORATION)

Name: .....

Authorised Signature .....

DATA IMPORTER (CERNER HEALTHCARE SOLUTIONS PRIVATE LTD)

Name: .....

Authorised Signature .....

SCHEDULE 3

LIST OF NCL PARTNERS - DATA CONTROLLERS AND EXPORTERS

Barnet GP Partners (Controllers)
Brunswick Park Medical Practice
Greenfield Medical Centre
Lane End Medical Group
Longrove Surgery
Oak Lodge Medical Centre
Penshurst Gardens
PHGH Doctors
St Andrews Medical Practice
St George's Medical Centre
The Clinic (Oakleigh Rd North)
The Everglade Medical Practice
The Old Courthouse Surgery
The Speedwell Practice
The Village Surgery
Wakeman's Hill Surgery
Wentworth Medical Practice
Addington Medical Centre
Adler & Rosenberg (682 Finchley Road)
Cherry Tree Surgery
Cornwall House Surgery
Cricklewood Health Centre(Barndoc Healthcare Ltd)
Deans Lane Medical Centre
Derwent Medical Centre
Doctors Surgery
Dr Azim & Partners
Dr SL Datoo
East Barnet HC (Dr Peskin/Syed/Hussain)
East Barnet HC (Dr Weston & Dr Helbtitz)
East Barnet HC (Monkman)
East Finchley Medical Practice
Friern Barnet Medical Centre
Gloucester Road Surgery
Heathfielde
Hendon Way Surgery
Hillview Surgery
Hodford Road Surgery
Holly Park Clinic
Jai Medical Centre
Langstone Way Surgery
Lichfield Grove Surgery
Millway Medical Practice
MK Lamba
Mountfield Surgery
Mulberry Medical Practice
Parkview Surgery
Pennine Drive Surgery
Ravenscroft Medical Centre
Rosemary Surgery
Squires Lane Medical Practice

Supreme Medical Centre
Temple Fortune Health Centre
The Phoenix Practice **(Boyne Ave (E83656) has now merged with this practice)**
The Practice @ 188
Torrington Park Group Practice
Vale Drive Medical Practice
Watling Medical Centre
Woodlands Medical Practice
Camden GP Partners (Controllers)
Abbey Medical Centre
Adelaide Medical Centre
Ampthill Practice
Belsize Priory Medical Centre
Bloomsbury Surgery
Brondesbury Medical Centre
Brookfield Park Surgery
Brunswick Medical Centre
Caversham Group Practice
Camden Health Improvement Practice
Chomley Gardens
Daleham Gardens
Fortune Green Surgery
Gower Street Practice
Grays Inn Road Medical Centre
Hampstead Group Practice
Holborn Medical Centre
James Wigg Practice
The Keats Group Practice
Kings Cross Road Surgery
Museum Practice
Park End Surgery
Parliament Hill Surgery
Primrose Hill Surgery
Prince of Wales Group Practice
Prince of Wales (Dr Matthewman)
Queens Crescent Practice
Regents Park Practice
Rigdmount Practice
Rosslyn Hill Surgery

Somers Town Medical Centre
St Phillips Medical Centre
Swiss Cottage Surgery
West Hampstead Medical Centre
Camden GP Federation
Enfield GP Partners (Controllers)
Carlton House Surgery
Abernethy House
Willow House Surgery
White Lodge MC
Bincote Road Surgery
Southbury Surgery
Town Surgery
Cockforsters MC
Highlands Practice
Oakwood MC
Freezywater PCC
Ordnance Road Surgery
Enfield Island Surgery
Riley House Surgery
Moorfield Road HC
Brick Lane Surgery
Green Street Surgery
East Enfield Practice
Eagle House Surgery
Lincoln Road Medical Practice
Curzon Avenue Surgery
Dean House Surgery
Nightingale House Surgery
Southgate Surgery
Winchmore Practice
The Woodberry Practice
Gillian House Surgery
Connaught Surgery
Grovelands & Grenoble MC
Park Lodge MC
The North London HC

Arnos Grove MC
Trinity Avenue Surgery
Bush Hill Park Medical Centre
Bounces Road Surgery
Boundary House Surgery
Forest Road Group Practice
Keats Surgery
Latymer Road Surgery
Evergreen Surgery
Rainbow Practive
Chalfont Road Surgery
Morecambe Surgery
Edmonton MC
Green Cedars Medical Centre
Dover House Surgery
Angel Surgery
Boundary Court Surgery
Haringey GP Partners (Controllers)
157 Medical Practice
Alexandra Surgery
Arcadian Gardens Medical Centre
Bounds Green Group Practice
Bridge House Medical Practice
Bruce Grove Castle View branch
Bruce Grove Primary Care Health Centre
Charlton House Medical Centre
Cheshire Road Surgery
Christchurch Hall Surgery
Crouch Hall Road Surgery
Dowsett Road Surgery
Fernlea Surgery
Grove Road Surgery
Havergal Surgery
Highgate Group Practice
Hornsey Park Surgery
JS Medical Park Lane branch
JS Medical Practice Phillip Lane

JS Medical Westbury Ave branch
Lawrence House Broadwater Farm branch
Lawrence House Surgery
Morris House Group Practice
Muswell Hill Practice
Myddleton Road Surgery
Old Surgery
Queens Avenue Surgery
Queenswood Medical Practice
Rutland House Surgery
Somerset Gardens Family Health Care
Spur Road Surgery
St Ann's Road Surgery
Staunton Group Practice, Morum House Medical Centre
Stuart Crescent Health Centre
Stuart Crescent High Road
Tottenham Hale Medical Practice
Tottenham Health Centre
Tynemouth Medical Practice
Vale Practice
West Green Surgery
Westbury Medical Centre
Islington GP Partners (Controllers)
Archway Medical Centre
Hanley Primary Care Centre
The Rise Group Practice
Stroud Green Medical Clinic
The Village Practice
Andover Medical Centre
The Beaumont Practice
The Northern Medical Centre
St John's Way Medical Centre
The Goodinge Group Practice
The Junction Medical Practice
Partnership Primary Care Centre
The Family Practice
The Miller Practice

Islington Central Medical Centre
Mitchison Road Surgery
Roman Way Medical Centre
Highbury Grange Medical Practice
The Medical Centre- Dr Edoman
Mildmay Medical Practice
Sobell Medical Centre - Dr Gupta
Elizabeth Avenue Group Practice
New North Health Centre - Dr Skelly
River Place Group Practice
St Peter's Street Medical Practice
Barnsbury Medical Practice - Dr Haffiz
Killick Street Health Centre
Ritchie Street Group Practice
Amwell Group Practice
City Road Medical Centre
Clerkenwell Medical Practice
Pine Street Medical Practice - Dr Segarajasinghe
Provider Partners (NHS Trust)
University College London Hospital
Central North West London NHS Foundation Trust
Tavistock and Portman NHS Foundation Trust
Royal Free London NHS Hospitals Foundation Trust
Camden and Islington NHS Foundation Trust
North Middlesex University Hospital NHS Trust
Whittington Health NHS Trust (incl Islington and Haringey Community)
Barnet Enfield and Haringey Mental Health NHS Trust (main sites, incl Enfield Community)
Central London Community Healthcare NHS Trust
Moorfields Eye Hospital NHS Foundation Trust
Royal National Orthopaedic Hospital NHS Trust
Local Authority Partners
London Borough of Islington
London Borough of Camden
London Borough of Enfield
London Borough of Haringey
London Borough of Barnet
CCG Partners

Islington Clinical Commissioning Group
Barnet Clinical Commissioning Group
Haringey Clinical Commissioning Group
Camden Clinical Commissioning Group
Enfield Clinical Commissioning Group