

**INFORMATION PROCESSING AGREEMENT**

between

**DEEPMIND TECHNOLOGIES LIMITED**

and

**ROYAL FREE LONDON NHS FOUNDATION TRUST**

**THIS AGREEMENT** is made as the Effective Date

**BETWEEN**

- (1) **ROYAL FREE LONDON NHS FOUNDATION TRUST** having its registered address at Pond Street, London, NW3 2QG (the “**Controller**”)
- (2) **DEEPMIND TECHNOLOGIES LIMITED** a company incorporated in England and Wales (registered number 07386350) whose registered offices is at 5 New Street Square, London, EC4A 3TW (the “**Processor**”)

each a “**Party**” and together the “**Parties**”.

**BACKGROUND**

- A. The Controller has entered into a Services Agreement with the Processor (as defined below) under which the Processor will provide certain Services (as defined below) to the Controller. In order to provide the Services, the Processor will need to process Personal Data, including patient data, on behalf of, and in accordance with the instructions of, the Controller.
- B. This Agreement exists to govern the relationship between the Parties during the term of the Services Agreement, to ensure that there are guarantees in place to protect data processed under this Agreement and to ensure that such processing meets the requirements of the 7th Data Protection Principle contained in the Data Protection Act 1998, and any replacement legislation in force from time to time.
- C. The Parties agree that the Information Sharing Agreement entered into on or around 24 September 2015 by or on behalf of the Parties is terminated with effect from the Effective Date. The Information Sharing Agreement is hereby superseded by this Agreement.

**THE PARTIES AGREE:**

**1. DEFINITIONS AND INTERPRETATION**

1.1 In this Agreement, unless the context indicates otherwise:

- Agreement** means this agreement comprising its clauses, schedules and any appendices that may be attached to it;
- Authorisations** means any permissions, consents (including without limitation consents from Data Subjects), approvals, certificates, permits, licences, agreements and authorities (whether statutory, regulatory, contractual or otherwise);
- Data** means data to made available by the Controller to the Processor for the purposes of providing the Services, as described in Schedule 1;

<b>Data Protection Legislation</b>	means the Data Protection Act 1998 as amended, extended, re-enacted and/or any replacement legislation therefor from time to time;
<b>Data Subject</b>	has the meaning given to it in the Data Protection Legislation;
<b>Effective Date</b>	the date on which this Agreement is signed by the Parties or, if signed on separate dates, the date on which the last Party signs.
<b>ICO</b>	means the Information Commissioner's Office or any successor thereto from time to time;
<b>N3 Network</b>	means the New National Network (or any replacement network), being the broadband network for England's National Health Service ("NHS");
<b>Personal Data</b>	means personal data (as defined under the Data Protection Legislation) which forms part of the Data;
<b>processing</b>	has the meaning given to it in the Data Protection Legislation;
<b>Processor Software</b>	means the software applications to be licensed to the Controller as part of the Services outlined in Clause 6 of the Services Agreement being the Streams: Results Viewing and Alerting application and the Streams: Task Management application, each as further specified in the Services Agreement;
<b>Project Governance Board</b>	means the governance board to be established in accordance with Clause 13 of the Services Agreement;
<b>Roadmap</b>	has the meaning given to it in the Services Agreement;
<b>Security Incident</b>	has the meaning given to it in Clause 4.10;
<b>Sensitive Personal Data</b>	means sensitive personal data or special categories of personal data (as defined under the Data Protection Legislation) which forms part of the Data;
<b>Services</b>	means the services to be provided by the Processor pursuant to the Services Agreement, as defined in the Services Agreement;
<b>Services Agreement</b>	means the Services Agreement between the Parties with an effective date of 2016; and
<b>Working Day</b>	means a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

- 1.2 Where the context so admits or requires, words denoting the singular include the plural and vice versa and words denoting any gender include all genders.
- 1.3 Any reference to a statutory provision, code or guidance shall be deemed to include reference to any subsequent modification or re-enactment of it.
- 1.4 Clause headings are for ease of reference only and do not form part of or affect the interpretation of this Agreement.
- 1.5 In the event of any inconsistency between the provisions of any Schedule and the provisions of the main body of this Agreement, the latter shall prevail to the extent of the inconsistency.
- 1.6 Capitalised terms not defined in this Agreement shall have the meaning given to them in the Services Agreement.

## **2. COMMENCEMENT AND DURATION**

- 2.1 This Agreement shall commence on the Effective Date and shall continue in force unless and until terminated in accordance with Clause 10 of this Agreement.

## **3. ROLE OF THE PARTIES**

- 3.1 The Parties acknowledge and agree that the Data processed by the Processor in order to provide the Services will include Personal Data, some of which will be Sensitive Personal Data.
- 3.2 In respect of any Personal Data processed by the Processor on behalf of the Controller in performing the Services, the Parties agree that the Controller shall be the “data controller” and the Processor shall be the “data processor” as such terms are defined in the Data Protection Legislation.
- 3.3 The Controller and Processor each agree to comply with those provisions of the Data Protection Legislation which are applicable to their role as a data controller or data processor, respectively, in relation to the Personal Data.
- 3.4 The Parties have agreed the data flow map attached as Schedule 3, which sets out how the Data will be processed by the Controller and the Processor in relation to the Services.

## **4. DATA PROCESSING**

- 4.1 The Processor agrees to process the Data in accordance with the terms and conditions set out in this Agreement and, subject to the overriding requirements of applicable law, undertakes to:
  - (a) only process the Personal Data for and on behalf of the Controller, strictly in accordance with the written instructions of the Controller, unless required to do otherwise by UK law, in which case the Processor shall inform the Controller of that legal requirement before processing the Personal Data otherwise than in

- accordance with the Controller's instructions (unless that law prohibits such information on important grounds of public interest);
- (b) disclose the Personal Data only to its personnel and subcontractors who have a need to know such information in order to perform the Services under the Services Agreement, and who have undergone appropriate information governance training and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - (c) process the Personal Data only for the purposes of providing the Services under the Services Agreement;
  - (d) implement and maintain appropriate technical and organisational security measures to safeguard the Personal Data from unauthorised or unlawful processing or accidental loss, damage or destruction, as more fully set out in Schedule 2 and the Services Agreement;
  - (e) not engage any subprocessors without the Controller's prior written consent and, in the event of subprocessing, ensure the same data protection obligations as are imposed on the Processor under this Agreement are imposed on the subprocessor by way of a written contract with the Processor. The Processor shall remain fully liable to the Controller for the acts or omissions of any subprocessor;
  - (f) taking into account the nature of the processing and the information available to the Processor, assist the Controller (as reasonably requested by the Controller) in ensuring compliance with its obligations under the Data Protection Legislation in relation to security, data breach notification, data protection impact assessments and prior consultation, if and to the extent such obligations apply to the Controller under the Data Protection Legislation;
  - (g) not transfer the Personal Data outside of England without the prior written consent of the Controller;
  - (h) at the choice of the Controller, delete or return all Personal Data upon termination of this Agreement, and delete any existing copies unless UK law requires storage of the Personal Data; and
  - (i) make available to the Controller such information as the Controller may reasonably require to demonstrate compliance by the Processor with its obligations under this Agreement, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to: (i) any such audit being conducted during business hours and on reasonable advance notice by the Controller; (ii) the Controller and any third party auditor taking reasonable steps to minimise any disruption to the Processor's business; and (iii) the Controller and any third party auditor complying with any reasonable requirements imposed by the Processor to protect the safety and security of its premises and systems, and the confidentiality of any Processor or third party confidential information and/or personal data processed by the Processor on behalf of any third party.

- 4.2 The Processor shall not disclose the Personal Data to any third party without the express written consent of the Controller. Where the Controller instructs the Processor to make the Personal Data available to a third party (whether through an application programmable interface or otherwise), the Controller shall ensure that it has a lawful basis for such disclosure and, where required by the Data Protection Legislation, has provided notice to the relevant Data Subjects.

- 4.3 The Processor shall promptly amend or delete the Data, or restrict the processing of any Data, if requested to do so in writing by the Controller.
- 4.4 The Processor shall not combine or link the Data with any other data unless instructed to do so by the Controller.
- 4.5 The Processor shall be accountable for managing the Data as a responsible data processor compliant with the ICO's policies and procedures.
- 4.6 The Processor shall designate an individual as its custodian of the Data, who will be responsible for overseeing the Processor's compliance with the terms of this Agreement as they pertain to the Data and who shall act as the Controller's single point of contact in relation to any concerns the Controller may have regarding the Processor's compliance with the same. The Processor will identify its custodian to the Controller and will notify the Controller in the event of any change to that role.
- 4.7 The Processor shall ensure that all relevant personnel involved in the processing of the Data are aware of the legal obligations imposed on the Processor under this Agreement with respect to the Data and their respective responsibilities in discharging their duties.
- 4.8 The Processor shall ensure that appropriate training is provided to all relevant personnel in relation to information governance.
- 4.9 The Processor will permit Controller employees or other personnel authorised by the Controller to access the Data via the Processor's systems, such role-based access will be controlled by the Controller's Lightweight Directory Access Protocol ("LDAP") system. It remains the responsibility of the Controller to enable user accounts on the LDAP system only for users who have a legal right to access the Data.
- 4.10 In the event that the Processor becomes aware of any breach of security or other significant incident that affects the confidentiality, accuracy or integrity of the Data (a "Security Incident"), the Processor shall inform the Controller in writing without undue delay (and in accordance with any information governance process agreed pursuant to Clause 7), and shall promptly implement corrective action to seek to mitigate the impact of the Security Incident.
- 4.11 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations to respond to requests for exercising Data Subjects' rights. The Processor will notify the Controller within five Working Days of all communications the Processor receives from any Data Subject seeking to exercise the rights in relation to the Personal Data.
- 4.12 Under no circumstances shall the Processor sell or attempt to sell any Data to any third party.

## 5. OBLIGATIONS OF THE CONTROLLER

- 5.1 The Controller shall:

- (a) at all times comply with the Data Protection Legislation and any information governance requirements, and, in particular, ensure that its instructions and disclosures of the Data to the Processor are lawful and that it has at all times a lawful basis to provide the Data to the Processor and to instruct the Processor to process such Data in accordance with this Agreement;
  - (b) not disclose any Personal Data to the Processor save where this is lawful and in a form which is lawful;
  - (c) ensure that, where required under the Data Protection Legislation or for information governance reasons, appropriate information as to how the Data is to be used under the Services Agreement is made available to the Data Subjects and that any Data Subjects who object to the use of their Personal Data do not have Personal Data related to them included in the Data.
- 5.2 The Controller warrants and represents that it has assessed the technical and organisational security measures which the Processor has in place to comply with its obligation under Clause 4.1(d), and considers these to be appropriate to protect the Data, taking into account the state of the art, and the nature, scope, context and purposes of the processing, as well as the risks involved.
- 5.3 The Controller will provide the Processor with a connection to the Controller's LDAP servers.
- 5.4 The Controller remains responsible for any unauthorized access to Personal Data through the use of valid Controller LDAP credentials.
- 5.5 The Controller will ensure that:
- (a) it has obtained and maintains all necessary Authorisations to provide the Data to the Processor and for the Processor's use of the Data to perform the Services and other activities contemplated under this Agreement; and
  - (b) all relevant Authorisations are in place and are maintained for the Processor to provide the Services, including without limitation any ethical approvals required by a regulatory authority.

## 6. REGULATORY OVERSIGHT

- 6.1 Each Party will co-operate with, and provide reasonable assistance to, the other in the event of any enquiry or investigation by the ICO or any other regulatory authority in relation to processing of the Data pursuant to this Agreement.
- 6.2 Each Party will inform the other within two Working Days of receipt of any communication from the ICO or other regulatory authority in relation to the Services, and will provide the other Party with a reasonable opportunity to comment on and contribute to any response, prior to its being sent.

## 7. INFORMATION GOVERNANCE

- 7.1 In recognition of the seriousness with which the Parties view their respective responsibilities in respect of the Data, the Parties shall establish an information governance board consisting of two individuals, comprising one representative of each Party (the "**Information Governance Board**"). The initial representatives of the

Parties shall be notified by each Party to the other within ten (10) days of the Effective Date.

- 7.2 Each Party may from time to time change its representative on the Information Governance Board by notifying the other Party with the name of its new representative.
- 7.3 The Information Governance Board will co-operate to establish and implement the following information governance processes in relation to the Services, and in doing so shall bear in mind the Caldicott Principles:
- (a) monthly audit reports to contain information on some or all of the following: spot checks (assets, code, physical storage, policy adherence), incident simulation, auditing logs and pager testing;
  - (b) new starter training in relation to HSCIC certification and internal policy training;
  - (c) data and infrastructure access approval including submission of access tickets to the Information Governance Board as required and the requesting of review and approval;
  - (d) review of access requests and access control lists, new processes & information assets, security planning/proposals, and policy updates by the Information Governance Board;
  - (e) risk management processes for agreed incident management procedures;
  - (f) procedures for auditing of access to Data; and
  - (g) procedures for reviewing the information governance and data processing arrangements under this Agreement on a regular basis.
- 7.4 The Information Governance Board shall meet at least once every month.
- 7.5 All material decisions of the Information Governance Board shall be recorded in writing.
- 7.6 Each Party shall be entitled to convene a meeting of the Information Governance Board on giving not less than fourteen (14) days' notice to the other Party.
- 7.7 The quorum for a meeting of the Information Governance Board shall be two individuals, one representing each Party. No valid meeting of the Information Governance Board may be held unless a quorum is present. All decisions of the Information Governance Board must be unanimous.
- 7.8 The Information Governance Board shall consult with the Project Governance Board in relation to approval of Service Schedules and any changes to any Service Schedule which are relevant to this Agreement.
- 7.9 For the avoidance of doubt, the Information Governance Board shall not have the power to make any changes to the provisions of this Agreement, but may recommend to the Parties changes to this Agreement to be made in accordance with Clause 12.8.
- 8. INDEMNITY**
- 8.1 The Processor shall indemnify and keep the Controller indemnified in respect of any losses, liabilities, fines, charges, damages, actions, costs and expenses (including



reasonable legal expenses actually incurred) and costs of investigation, litigation, settlement, judgment, interest and penalties that are suffered or incurred by the Controller as a direct result of a breach of this Agreement by the Processor, including without limitation in connection with any claim or proceeding brought against the Controller by a Data Subject or any competent regulatory agency, provided that this indemnity shall not apply if and to the extent that any such losses, liabilities, fines, charges, damages, actions, costs and expenses (including reasonable legal expenses actually incurred) and/or costs of investigation, litigation, settlement, judgment, interest and penalties that are suffered or incurred by the Controller arise as a result of or were exacerbated by any breach by the Controller of its obligations under the Data Protection Legislation and/or under this Agreement and/or as a result of the Processor processing any Data in accordance with the Controller's instructions.

- 8.2 The Controller shall indemnify and keep the Processor indemnified in respect of any losses, liabilities, fines, charges, damages, actions, costs and expenses (including reasonable legal expenses actually incurred) and costs of investigation, litigation, settlement, judgment, interest and penalties that are suffered or incurred by the Processor as a direct result of a breach by the Controller of this Agreement, including without limitation in connection with any claim or proceeding brought against the Processor by a Data Subject or any competent regulatory agency, provided that this indemnity shall not apply if and to the extent that any such losses, liabilities, fines, charges, damages, actions, costs and expenses (including reasonable legal expenses actually incurred) and/or costs of investigation, litigation, settlement, judgment, interest and penalties that are suffered or incurred by the Processor arise as a result of or were exacerbated by any breach by the Processor of its obligations under this Agreement.
- 8.3 Each of the indemnities in Clauses 8.1 and 8.2 respectively is subject to: (i) the indemnified Party promptly notifying the indemnifying Party of any third party claim or regulatory proceeding in respect of which indemnification is sought; (ii) the indemnified Party giving the indemnifying Party the right to defend any such third party claim and settle such third party claim with the prior written consent of the indemnified Party (such consent not to be unreasonably withheld or delayed), and to participate in the defence of any enforcement action by the ICO or other regulatory proceeding by any other regulatory body, in each case with the indemnified Party providing assistance and information in relation to such defence as reasonably requested; and (iii) the indemnified Party not making any statement or taking any action or refraining from taking any action that is or may be prejudicial to the defence of such third party claim, or regulatory proceedings. The indemnified Party shall take all reasonable steps to mitigate any loss and/or damage.

## **9. LIABILITY**

- 9.1 The Parties' liability whether based on a claim in contract, tort (including negligence), breach of statutory duty or otherwise arising out of, in relation to, or in connection with this Agreement and/or the Services Agreement, including under the indemnities set out in Clause 8, shall be limited and excluded in accordance with and subject to the terms of Clause 28 of the Services Agreement.

## **10. TERMINATION**

- 10.1 This Agreement shall automatically terminate upon termination or expiry for any reason of the Services Agreement. Termination of this Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry. Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect.

## 11. DISPUTE RESOLUTION

- 11.1 The Parties shall attempt, in good faith, to resolve any dispute arising out of, in connection with or in relation to this Agreement promptly in accordance and on and subject to the terms of with Clause 32 of the Services Agreement, save that the Parties' representatives on the Information Governance Board shall take the place of the Parties' Services Managers.

## 12. GENERAL PROVISIONS

- 12.1 Any notices under this Agreement shall be in writing, signed by the relevant Party to this Agreement and delivered personally, by courier or by recorded post to the addresses specified below:
- (a) The Processor: 5 New Street Square, London, EC4A 3TW
  - (b) The Controller: Royal Free  
London NHS Foundation Trust, Royal Free Hospital, Pond Street, London,  
NW3 2QG
- 12.2 Neither Party shall assign, transfer, subcontract, or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the other Party (such consent not to be unreasonably withheld or delayed).
- 12.3 A person who is not a Party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.
- 12.4 This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.
- 12.5 This Agreement (including the Schedules) constitutes the entire agreement between the Parties in connection with its subject matter and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations (other than fraudulent misrepresentations but including negligent misrepresentations) and understandings between them, (in each case whether written or oral), relating to its subject matter. Each Party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently but excluding any fraudulent misrepresentation) that is not set out in this Agreement.

- 12.6 No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy.
- 12.7 Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control. The Party claiming to be affected by the event of force majeure shall notify the other Party of the nature and extent of the circumstances as soon as practicable. In such circumstances the affected Party shall be entitled to a reasonable extension of the time for performing such obligations.
- 12.8 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties.
- 12.9 Nothing in this Agreement is intended to, or shall be deemed to, establish any legal partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party.
- 12.10 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.
- 12.11 Each Party irrevocably agrees that the courts of England and Wales shall, subject to Clause 11, have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

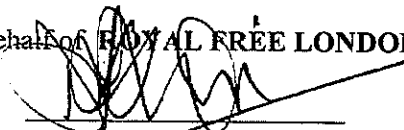
Signed for and on behalf of ~~ROYAL FREE LONDON NHS TRUST~~ by:

Signature:

Print Name:

Position:

Date:

  
\_\_\_\_\_  
DAVID SLOMAN  
\_\_\_\_\_  
CHIEF EXECUTIVE  
\_\_\_\_\_  
10 NOVEMBER 2016

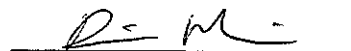
Signed for and on behalf of **DEEPMIND TECHNOLOGIES LIMITED** by:

Signature:

Print Name:

Position:

Date:

  
\_\_\_\_\_  
DEMIS HASSABIS  
\_\_\_\_\_  
C.E.O  
\_\_\_\_\_  
10 NOVEMBER 2016

**SCHEDULE 1: Data**

1. The Controller will provide the following Data on the dates and in the manner specified in the Roadmap:
  - (a) HL7 feeds: and live data via HL7 MLLP (Minimal Lower Layer Protocol);
  - (b) HL7 message types (eg. ADT, ORU, ORM) and sources required on the feed will be determined by the roadmap of resources to be provided by the API in the Project roadmap;
  - (c) text files exported from existing hospital systems defining fixed (non-patient) resources (eg. Consultants, General Practitioners, Beds);
  - (d) Historic encounter, procedure, diagnostic information in an agreed format (eg. HES-APC 6.2 single line fixed width);
  - (e) Renal System reporting database;
  - (f) radiology images through Query & Retrieve access to the Picture Archiving and Communication System; and
  - (g) FHIR messages as developed through the Controller or from existing hospital systems.

## SCHEDULE 2: Security Measures

The Processor shall implement and maintain the following security measures whilst it continues to process the Data on behalf of the Controller:

- (i) **Data Centre** - Data is stored at an ISO27001 accredited colocation facility.
- (ii) **Encryption** - Data will be delivered to the Processor over an encrypted channel. Where required by the Controller, connections will be limited to the Controller's N3 Network and/or encapsulated, for example in an encrypted Internet Protocol Security tunnel. The API will be accessible from the Controller via an encrypted HTTPS connection, secured via an authentication and authorisation system linked to the Controller LDAP servers. Data is secured on disk with AES-256 encryption and in-transit at the colocation facility with TLS v1.2.
- (iii) **Backup** - The Processor will use an encrypted file-based backup with full and incremental backups daily.
- (iv) **Resilience** - The Processor will use reasonable measures to seek to ensure that there is sufficient additional server and other hardware capacity to continue operations of the systems. Where technically feasible, failover mechanisms will be in place to ensure that in the event of hardware or software failure the Services will transition to other available systems.
- (v) **Disaster Recovery** - The Processor has undertaken and continuously undertakes disaster recovery planning exercises. The Processor and the Controller will agree a formal service level agreement to cover any deployment with critical clinical dependencies on or prior to the relevant date in the Roadmap.
- (vi) **Incident Notification** - The Processor will promptly inform the Controller of any Security Incident in accordance with the Information Governance process to be established pursuant to Clause 7.

**SCHEDULE 3: Data Flow Map**  
(redacted for commercial sensitivity)