CONFIDENTIAL

EXECUTIVE SUMMARY OF SERVICES AGREEMENT
Royal Free London NHS Trust (the "Trust")

Date	10 November 2016
Term	5 years, with each of the Services (defined below) being provided for any specific period which may be set out in the Roadmap. DeepMind and the Trust will, prior to 12 months before the end of the 5 year period, discuss and agree in good faith whether to extend the agreement depending upon progress and fulfillment of the Roadmap.
Services	DeepMind will provide the following services to the Trust (the "Services"): • **FHIR API Development** - DeepMind will design, develop and maintain a generalised, open application programmable interface (FHIR DSTU2 with agreed local extensions) to support application access to the Data (as defined below). The API will be designed to provide the Trust with a scalable and extensible mobile environment to support a range of services from third party providers (including the DeepMind Software), and shall include the development of extensions to support those by the Trust, as required. • **Data Management** - DeepMind shall, acting only as a data processor for the Trust, provide and maintain at least two secure data centres in England for the storage and maintenance of the Data (including any patient confidential information) with ISO27001 accreditation and at all times in compliance with NHS Digital IG and ISMS requirements. • **DeepMind Software** - DeepMind shall provide the following proprietary software applications to the Trust. Users of the software will be given instructions on its appropriate use and the Trust will notify DeepMind of any issues regarding the use or functioning of the Software as soon as possible. In all cases processing outputs from the DeepMind Software will be developed to be compatible with outputs already delivered or planned in existing Trust systems, and built on top of the FHIR API: ○ Streams: Results Viewing and Alerting - a Class 1 non-measuring medical device provided in the form of a standalone mobile software application that can presently assess the real-time detection of AKI with patients and which is extensible generally to (i) patient safety alerts, and (ii) real time detection and decision support to support treatment and avert clinical deterioration across a range of diagnoses and organ systems; and ○ Streams: Task Management - a comprehensive clinical task management and text based messaging platform provided in the form of a mobile software application. This application is not a medical device. • **Software and API Support** - DeepMind shall provide the Trust with remote maintenance and support for the Software and the API in accordance with the support guide provided to the Trust. • **Audit** - DeepMind shall develop and provide the Trust with a service to allow the Trust (or other authorised party) to obtain an accessible audit history of all actions taken on any Data to be made available subject to, and as provided for on, the Roadmap. • **Exit migration** - where agreed by the parties on a notice of termination, DeepMind shall provide exit migration services to enable the orderly cessation of Data Management Services by the Transfer of data to the Trust

	in a format that allows the Trust to enable a suitably qualified service provider to provide services similar to the Data Management Services
Service Charges	[redacted]
	DeepMind will share with the Trust information related to the support costs incurred by DeepMind in the first 2 months of the term to enable the Trust to better understand at what point they may reach their £15,000 monthly threshold

Intellectual Property	The Trust and DeepMind will each retain their own rights in pre-existing intellectual property (including rights in third party software which may be developed during the Term for the Trust, or developed by the Trust independently). The Trust will grant DeepMind a licence to such rights as may exist in the Data solely for the purpose of the provision of the Services by DeepMind. Trust also grants to DeepMind a perpetual licence to Trust's background IP (excluding Data) to the extent that it is incorporated into the DeepMind Software/FHIR API/Documentation DeepMind will retain all intellectual property rights that may be created by DeepMind in the development and deployment of the FHIR API. DeepMind shall grant the Trust a non-exclusive, royalty-free internal use license in respect of any such rights created by DeepMind in the development and deployment of the FHIR API. In the event that DeepMind terminates the agreement before the Term or the Trust terminates the Agreement before the Term on account of DeepMind's material breach, the license shall convert to a perpetual license to facilitate the Trust's ongoing internal use and development of the API. DeepMind will retain all intellectual property rights in the DeepMind Software and any developments or modifications made to such software by DeepMind during the Term.
Devices	Unless agreed otherwise with DeepMind, clinicians working for the Trust will use their own device or Trust owned devices to use the DeepMind Software. The Trust shall: ● maintain a Mobile Device Policy to be agreed with DeepMind that is consistent with currently accepted best practice and in line with relevant guidance issued by the Centre for the Protection of National Infrastructure,

	CESG and the ICO; ● maintain technical controls to remotely secure (including remote deletion of information), manage and support the personally-owned devices, to the highest level of security available, offering only approved employees controlled and time-limited access to an encrypted shell of relevant clinical data to be confirmed and audited by DeepMind prior to deployment; ● ensure that each clinician or employee is made aware of the Mobile Device Policy and has signed a copy of the Mobile Device Policy to show that they acknowledge and understand their obligations; ● inform DeepMind on becoming aware that any device using the DeepMInd Software has been lost, stolen, damaged or accessed in an authorised manner; and ● *ensure that only appropriate trained and qualified clinical staff have access to the DeepMind Software and that appropriate restrictions on use are reflected in the Mobile Device Policy and enforced by the Trust.*
Freedom of Information	DeepMind shall provide assistance and co-operation as reasonably requested by the Trust to enable the Trust to comply with its disclosure obligations under the FOIA. The Trust must give not less than 48 hours notice to DeepMind of any FOIA request it receives which relates to DeepMind and/or this agreement. DeepMind accepts that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under FOIA is a decision solely for the Trust to whom the request is addressed, but may, in providing information to the Trust preemptively mark information that in DeepMind's reasonable view would be exempt from any subsequent FOIA request (for example, due to reasons of commercial confidentiality) and the Trust shall have due regard to such markings in making any determination.
Data Types	

Data Security	DeepMind shall ensure that the following security processes are in place to protect the Data: ● **Encryption** - Data will be delivered to DeepMind over an encrypted channel. Where required by the Trust, connections will be limited to the N3 network and/or encapsulated, for example in an encrypted Internet Protocol Security tunnel. The API will be accessible from the Trust via an encrypted HTTPS connection, secured via an authentication and authorisation system linked to the Trust LDAP servers. Data will be encrypted both in transit and at rest within DeepMind data centres. ● **Backup** - DeepMind will use an encrypted file-based backup with full and incremental backups daily (once every 24 hours). The database will be fully replicated and will fail-over in the event of a failure. ● **Resilience** - DeepMind will ensure, for all Services, 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. ● **Disaster Recovery** - DeepMind has undertaken and continuously undertakes disaster recovery planning exercises. DeepMind and the Trust will agree a formal service level agreement to cover any deployment with critical clinical dependencies on or prior to a the relevant date in the Roadmap. ● **Incident Notification** - DeepMind will promptly inform the Trust of any information security incident or suspected information security incident involving the Data in accordance with the Information Governance process (see below, and which process shall include appropriate mutual protocols for handling of confidential or embargoed information from third parties on reported issues, and restrictions on internal use of sensitive information relating to any actual or potential incident). ● **Penetration testing** - DeepMind and the Trust will conduct penetration testing on an annual basis NOTE: no change from the original template
Data Protection	DeepMind and the Trust recognize and agree that the Trust is a registered data controller that is commissioning data processing services from DeepMind to support the direct care of Trust patients. Accordingly, wherever personal data forms part of the Data, the Trust shall at all times act as the data controller and DeepMind as the data processor. As data controller, the Trust undertakes to: ● consistently ensure that it has a lawful basis to provide the data to DeepMind and to instruct DeepMind to process such data; ● indemnify and keep DeepMind indemnified in respect of any losses and penalties that are suffered or incurred by DeepMind as a result of a breach of its obligations as a data controller in relation to the Data, including in connection with any claim or proceeding brought against DeepMind by a data subject or any regulatory body as a result of a breach of the Trust's obligations as a data controller. As data processor DeepMind undertakes to: ● use the Data only for the purposes of providing the Services; ● only process the Data for and on behalf of the Trust, strictly in accordance with the instructions of the Trust;

	• not transfer the Data outside of England without the prior written consent of the Trust; • not combine or link the Data with any other data held by DeepMind unless instructed to do so by the Trust; • disclose the Data only to its personnel and subcontractors who have a need to know such information in order to perform the Services; • designate an individual as its custodian of the Data, who will be the Trust's single point of contact in relation to any concerns the Trust may have regarding DeepMind's compliance data protection requirements. DeepMind will identify its custodian to the Trust and will notify the Trust in the event of any change to that role; • implement appropriate technical and organisational safeguards to prevent unauthorised use or disclosure of the Data; • provide written notice to the Trust promptly on becoming aware of any unauthorised use or disclosure of the Data following an investigation; • not sell nor attempt to sell the Data to a third party under any circumstances; • manage the Data as a responsible data processor compliant with the Information Commissioner's Office's policies and procedures; • maintain technical and organisational security measures to safeguard the Data; and • promptly inform the Trust on becoming aware of any breach or suspected breach of the Data Protection Act involving personal data.
Data Subjects	DeepMind will: • assist the Trust promptly with all subject access requests which may be received from individuals whose personal data DeepMind is processing on behalf of the Trust; • promptly amend, transfer or delete any personal data that DeepMind is processing for the data controller if the data controller requires DeepMind to do so; • notify the Trust immediately of all communications DeepMind receives from any data subject or regulatory agency in connection with personal data processed by DeepMind as part of the Services which suggests non-compliance with the Data Protection Act and DeepMind will not do anything with regard to such communication unless the Trust expressly authorises DeepMind to do so.
Information Governance	DeepMind will work with the Trust Information Governance lead to ensure that the following information governance processes are in place: • **Monthly audit reports** - which will contain information on some or all of the following: spot checks (assets, code, physical storage, policy adherence), incident simulation, auditing logs and pager testing; • **New starter training** - HSCIC certification and internal policy training; • **Data/Infrastructure access approval** - submission of access tickets to IG Board as required and the requesting of review and approval; • **IG Board meeting** (separate to project board) - review access requests & access control lists, new processes & information assets, security planning/ proposal, and policy updates; • **Risk Management** - DeepMind will ensure that agreed incident management procedures are followed, and that in the event of an incident the Trust is briefed without delay and any corrective action reasonably required by the Trust is taken to redress any failures within a reasonable period of time; • **Auditing of access** - DeepMind will allow access to Data only on a 'need to know' basis by appropriately trained individuals and will use appropriate

	technical and organisational controls to ensure that this requirement is satisfied in accordance with the Caldicott Principles.
Project Governance	The parties shall establish a Project Governance Board, consisting of 2 representatives from each party which will be meet at least monthly. The Project Governance Board will be responsible for manage the management of the Services, including monitoring progress, reviewing and signing off on completed milestones. DeepMind may recover costs from the Trust for failing to meet a particular milestone, if the delay is caused by the Trust failing to carry out its responsibilities. Any changes to the roadmap (project delivery roadmap) will be need to be agreed in writing by the Project Governance Board.
Announcements	Any publicity must be in accordance with the Trust's prevailing communications policy. DeepMind and the Trust will take all reasonable steps to consult with the other over all press or public activity relating to the Services. Neither DeepMind or the Trust shall, without the other's prior written approval: ● issue any previously unreleased information or statement to the press or public relating to the Services; or ● use the names or logos of the other in any publicity, advertising or news release without the other's prior written approval.
Publications	Each of the Trust or DeepMind may present results relating to the use of the Services at symposia and/or publish in academic journals or other media of their choosing. Any publication must be in accordance with the Anonymisation Standard for Publishing Health and Social Care Data - ISB 1523. Prior to any publication the draft will be subject to sign off by the project managers.
Termination	Both the Trust and DeepMind may terminate the agreement on not less than 12 months notice. The Information Sharing Agreement (24 Sep 2015) is terminated from the Effective Data and the IPA supersedes the Information Sharing Agreement
Insurance	DeepMind shall maintain all the insurance cover as laid out in the original template; Trust will maintain its membership of the indemnity schemes run by the NHS Litigation Authority
Maximum liability	£5m