

DATA PROTECTION ACT 1998 UNDERTAKING

Data Controller: Royal Free London NHS Foundation Trust
Pond Street
Hampstead
London
NW32QG

The Royal Free London NHS Foundation Trust (the "Trust") hereby affirms the details set out below and undertakes to comply with the terms of the following Undertaking:

- (1) The Trust is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the Trust and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.
- (2) In response to media reports publicised in May 2016, the Information Commissioner (the 'Commissioner') was alerted to an arrangement between the Trust and DeepMind Technologies Limited ('DeepMind'), a UK company and data processor, under which DeepMind was engaged to develop and deploy a new clinical detection, diagnosis and prevention application for the Trust. The Commissioner launched an investigation which primarily focused on the data processing undertaken during the clinical testing phase of the application.
- (3) The investigation determined that on 30 September 2015, the Trust entered into an agreement with Google UK Limited (an affiliate of DeepMind) to develop and deploy a new clinical detection, diagnosis and prevention application and the associated technology platform for the Trust. In order to undertake clinical safety testing of this application and technology platform DeepMind, for this purpose and under the terms of the aforementioned agreement, processed approximately 1.6 million partial patient

records containing sensitive identifiable personal information held by the Trust.

- (4) The identifiable information in question included information on persons who had presented for treatment at the Trust in the previous five years for pathology tests together with data from the Trust's existing radiology and electronic patient record system. The purpose requiring DeepMind to process such information was to enable the clinical safety testing and deployment in live operation of a new application and associated technology platform that would provide the Trust with a mobile electronic patient record and an alert, diagnosis and detection system for acute kidney injury. The clinical safety testing of that platform was undertaken by the Trust, using the application and technology hosted and maintained by DeepMind.
- (5) The Trust explained to the Commissioner that Clinical safety testing at the relevant time was required by standards issued under the Health and Social Care Act 2012 and needed to be undertaken before new technology was deployed. The Commissioner has concluded however that these points need further exploration before a final view can be reached on them, and expect to find them considered more fully in the Privacy Impact Assessment that she is now requiring the Trust to complete.
- (6) The platform went on to be formalised into a mobile device application, known as 'Streams'. From February 2017, the Streams application moved to live deployment and it is now in active use by the Trust's clinicians. The Streams application is registered with the MHRA as a Class I non-measuring device and is CE marked.
- (7) The agreement of the 30 September 2015 set out the relationship between the Trust and Google UK Limited as one of a data controller to data processor, with the Trust retaining its data controller responsibilities throughout.
- (8) The Trust confirmed to the Commissioner that DeepMind was only provided access to patient records as a data processor. The Trust has also confirmed that DeepMind has never used that information for any purpose other than to conduct clinical safety tests and for the live operation of the application and associated

technology platform set out above.

- (9) Data streaming between the Trust and DeepMind commenced on 18 November 2015. At that stage, the data was processed for clinical safety testing purposes only, and the Streams application was not in live deployment. This is an important point to note in the context of the conditions for processing that the Trust sought to rely upon at that stage.
- (10) All development and functional testing of the application and the related technology platform was undertaken by DeepMind using synthetic, non-personally identifiable, data. Pseudonymisation of the patient identifiable data was not undertaken for clinical safety testing. This is because the Trust was (and remains) of the view that it needed access to patient records in the application and technology platform in order to undertake clinical safety testing. The Trust is of the view that it is not possible to demonstrate clinical safety of a new technology of this type without access to information about real patients. The Trust was therefore of the view that the data was being held and made available for the purpose of direct patient care.
- (11) The Commissioner has concluded that, having completed her investigation, there were a number of shortcomings in the way in which patient records were made available to DeepMind in support of the clinical safety testing of the Streams application by the Trust. These shortcomings amounted, in the Commissioner's view, to non-compliance with the First, Third, Sixth and Seventh Data Protection Principles. These Principles are set out in Part I of Schedule 1 to the Act. The Commissioner considers that the data controller is also processing 'sensitive' personal data as defined by section 2(e) of the Act.

Principle One

- (12) The Commissioner's investigation determined that DeepMind processed approximately 1.6 million partial patient records to enable the clinical safety testing of the Streams application by the Trust. However, it is the Commissioner's view that patients were not adequately informed that their records would be processed for the purpose of clinical safety testing.
- (13) The Commissioner has concluded that the data

controller did not provide an appropriate level of transparency to patients about the use of their personal data during the clinical safety testing phase and that this processing was not something that the patients might reasonably expect. Specifically the Commissioner has concluded that the fair processing information available to the patients was insufficient. Patients were not, in the Commissioner's view, provided with sufficient notice that their records would be processed in support of the clinical safety testing of the Streams application. The Commissioner notes the recent improvements that have been made by the data controller to improve transparency and that a revised notice regarding live clinical use is now available.

(14) Further the Commissioner is not satisfied that the Trust has, to date, properly evidenced a condition for processing that would otherwise remove the need for the Trust to obtain the informed consent of the patients involved for the processing of personal data for the clinical safety testing of the application prior to live deployment. As a result, during the Commissioner's investigation and to the Commissioner's satisfaction, the data controller has not been able to evidence a valid condition for processing personal data under Schedule 2 to the Act during the clinical safety testing phase of the application or to evidence a valid condition for processing sensitive personal data under Schedule 3 to the Act during the clinical safety testing phase of the application. The Commissioner has therefore required the Trust to provide evidence that any future testing arrangements with DeepMind will comply with a processing condition in Schedule 2 and 3 to the Act.

(15) The Commissioner has worked closely with the Office of the National Data Guardian (the 'NDG') on the issue of whether the processing of the patient records during the clinical safety testing phase was in breach of the common law duty of confidentiality. The Trust maintains that the clinical safety testing of the application amounted to direct care so that it had the implied consent of its patients for confidentiality purposes, in accordance with the NDG's guidance. The Commissioner has considered the advice given by the NDG on this issue earlier this year and in light of the NDG's view on the matter, and her own review, the Commissioner considers it is likely that the processing of the records during the clinical safety testing phase was in breach of confidence and therefore not compliant with the First Data Protection Principle under

the Act. The Commissioner has therefore required the Trust to provide evidence that any future development or testing arrangements with DeepMind are not in breach of its duty of confidence, as it relates to the First Data Protection Principle.

- (15A) The Commissioner also notes that the Trust has adopted a revised notice and opt out approach, in line with the recent guidance of the NDG in order to enable compliance with patient confidentiality. Patients should also note that the Commissioner has not, in her investigations to date, found grounds for concern regarding the data processing in the live use of the Streams application.

Principle Three

- (16) An estimated 1.6 million partial patient records were processed by DeepMind on the Trust's behalf. The Commissioner has considered the Trust's representations as to why it was necessary for so many records to be used to support the clinical safety testing of the application. The Commissioner is not persuaded that proper consideration was given to the necessity of processing so many patients' records. As such the Commissioner is of the view that the Trust has failed to demonstrate that the processing of such a large number of partial records was both necessary and proportionate to the purpose pursued by the data controller and that the processing was potentially excessive. The Commissioner did not receive evidence of whether lower volumes of records could have been used during the testing phase. Whilst the rationale for using the full range of records in the live clinical setting is now clearer, the Commissioner emphasises the importance of assessing the proportionality in future iterations of the application for testing or clinical purposes.

Principle Six

- (17) The Commissioner's investigation has determined that as patients were not provided with sufficient information about the processing and as a result those patients would have been unable to exercise their rights to prevent the processing of their personal data under section 10 of the Act. As set out above, the Trust has now taken further steps to ensure patients are aware of the use of their data for clinical safety testing and of their ability to opt out from such testing. In the

Commissioner's view, this was not the case in 2015 and early 2016.

Principle Seven

- (18) Principle Seven requires that where a data processor carries out processing on behalf of a data controller, a contract evidenced in writing must be in place. Although there was a written information sharing agreement in place at the time DeepMind was given access to the data that set out the parties roles and imposed security obligations on the processor, the Commissioner's investigation has determined that this agreement did not in the Commissioner's view go far enough to ensure that the processing was undertaken in compliance with the Act. Specifically, it is the Commissioner's view that the information sharing agreement of 30 September 2015 did not contain enough detail to ensure that only the minimal possible data would be processed by DeepMind and that the processing would only be conducted for limited purposes. It is the Commissioner's view that, the requirements DeepMind must meet and maintain in respect of the data were not clearly stated. The Commissioner is also concerned to note that the processing of such a large volume of records containing sensitive health data was not subject to a privacy impact assessment ahead of the project's commencement.
- (19) The Commissioner does however recognise that the Trust has since replaced and improved the documentation in place between the Trust and DeepMind and has increased patient visibility of the use of data for the Streams application.
- (20) Following consideration of the remedial action that has been taken by the data controller and as detailed in this undertaking, it is agreed that in consideration of the Commissioner not exercising her powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the First, Third, Sixth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

1. The data controller will, within two months, complete a privacy impact assessment explaining how the data controller will demonstrate compliance with the Act in relation to the arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, during any future (a) application development and functional testing and (b) clinical safety testing that in either case is either planned or already in process. The privacy impact assessment should contain specific steps to review and (where necessary) ensure transparency and the provision of the fair processing information to affected individuals;
2. The data controller will, within one month of the date of the completion of the privacy impact assessment set out in (1) above, provide evidence that a condition for processing personal data under Schedule 2 to the Act applies in relation to its arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, to the use of such data for any further (a) application development and functional testing and (b) clinical safety testing which in either case uses patient data, and which in either case is either planned or currently in process;
3. The data controller will, within one month of the date of completion of the privacy impact assessment set out in (1) above, provide evidence that a condition for processing sensitive personal data under Schedule 3 to the Act applies in relation to its arrangement with DeepMind, if and to the extent such arrangement involves the processing of personal data relating to patients, to any future (a) application development and functional testing; and (b) clinical safety testing, which in either case is either planned or currently in process;
4. The data controller will, within one month of the completion of the privacy impact assessment set out in (1) above, provide the Commissioner with details of about how it will comply with its duty of confidence to patients as it relates to compliance with the First Data Protection Principle, in any future (a) application development and functional testing; and (b) clinical safety testing in relation to its arrangement with DeepMind if and to the extent such arrangements will use patient data and which in either case is either planned or in process;

5. The data controller will commission, within three months of the date of this undertaking, a third party audit of the current processing arrangements between the data controller and DeepMind, including an audit of how the data processing agreement between the data controller and DeepMind is operating, in practice in order to ensure compliance with Act, and disclose the findings to the Commissioner. The audit scope should assess both the current live clinical use of the Streams application and (a) any future application development and functional testing and (b) clinical safety testing that in either case is either planned or already in process. It should also include consideration as to whether the transparency, fair processing, proportionality and information sharing concerns outlined in this undertaking are now being met. The Commissioner will first approve the data controller's choice of auditor and agree the terms of reference. The Commissioner will, in the interests of transparency and in acknowledging the wider public interest in this case, retain the discretion to publish parts or all of the audit findings as appropriate.

Sir David Sloman (Chief Executive)
For and on behalf of the Royal Free London NHS Foundation Trust

Signed
Dated

Elizabeth Denham
Information
Commissioner

Signed
Dated