Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Sir David Sloman, Chief Executive
Royal Free NHS Foundation Trust
Pond Street
Hampstead
London
NW3 2QC

3 July 2017

Dear Sir David,

***RFA0627721 – provision of patient data to DeepMind***

I write to confirm that I have concluded my investigation into the above.

In summary, my investigation has determined that the processing of approximately 1.6 million patients' personal data by DeepMind Technologies Limited ('DeepMind') for the purpose of the clinical safety testing of the Streams application did not fully comply with the requirements of the Data Protection Act 1998 (the 'Act').

This letter explains how my investigation has reached that conclusion and highlights my key areas of concern. It explains the steps that I expect The Royal Free London NHS Foundation Trust ("Royal Free") to take as a result. As the letter goes on to explain, this includes Royal Free London NHS Trust's agreement to the signing of an undertaking.

## 1.1 Our investigation

First and foremost, my office has made our support for the appropriate use of personal data for the purpose of research, development and clinical improvements clear. As you may be aware from my recent outreach work and public statements, I see the Data Protection Act, transparency for individuals, and sound data protection practices as fundamental to innovation. The ICO is committed to supporting technological advances in a way that locks in good data protection practice by default. We recognise that data analytics has huge and varied potential, but we also want to ensure that good data protection practice is seen as the positive force for good that we believe it to be.

In relation to health data, my office recognises the benefits that can be achieved by using patient data for wider public good and, where appropriate, we support

the development of innovative technological solutions that use personal data to improve clinical care. I would like to make it clear that I have no desire to prevent or hamper the development of such solutions; however, such schemes and laudable ends must meet the necessary compliance mechanisms set out in the Act.

**1.2 Purpose and scope of investigation**

As set out in an agreement between the two parties effective 30 September 2015, the relationship between the Royal Free and DeepMind is one of a data controller to data processor.

It is my view that the Royal Free has retained its data controller responsibilities throughout my office's investigation, and continues to do so. For the avoidance of doubt, the investigation has proceeded on the basis that the Royal Free is the data controller under the Act. It is therefore the Royal Free who is required to take the steps we consider necessary to achieve compliance with the Act, with support from DeepMind as a data processor where appropriate.

The purpose of my investigation was to determine whether the Royal Free had complied with its responsibilities as a data controller under the aforementioned Act. I should explain that the investigation has primarily focused on the clinical safety testing phase of Streams, however and to some degree; my findings also have implications for the live version of the application now in operation.

The investigation, now concluded, determined that there were a number of shortcomings in the processing of patient records for the clinical safety testing of the Streams application. It is my view that these shortcomings amounted to non-compliance with the following data protection principles:

- Principle One: *Personal data shall be processed fairly and lawfully;*
- Principle Three: *Personal data should be adequate, relevant and not excessive;*
- Principle Six: *Personal data shall be processed in accordance with the rights of data subjects;*
- Principle Seven: *Appropriate technical and organisational controls shall be taken – this includes the need to ensure that appropriate contractual controls are in place when a data processor is used.*

I have considered each of the above principles within the scope of our enquiries and I have reached a conclusion in relation to each, as set out below.

## 2.0 Summary of events

The agreement set out between the two parties effective 30 September 2015, outlines the terms under which DeepMind would process partial patient records containing person identifiable information held by the Royal Free.

The identifiable information in question included information on persons who had presented for treatment in the previous five years for tests together with data from the Trust's existing radiology electronic patient record system. Under the terms of the agreement DeepMind would process approximately 1.6 million such partial records for clinical safety testing.

Our investigation has determined that the purpose of allowing DeepMind to process such information was to carry out clinical safety testing as part of the development of a new clinical detection, diagnosis and prevention application for the Trust in relation to Acute Kidney Injury ('AKI'). The platform was 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 Royal Free clinicians.

Data streaming between the Royal Free and DeepMind commenced on 18 November 2015. At that stage, it is understood that the data was processed for clinical safety testing and that the Streams application was not in active deployment. As reflected in the agreement effective 30 September 2015, patient identifiable data was not subject to pseudonymisation as the Royal Free believed that the data was being processed for the purpose of direct patient care.

As the project progressed, further written agreements including a privacy impact assessment were formalised. These agreements were put in place in January 2016 and in November 2016 respectively. As you will know, at the time these agreements were made, DeepMind had already processed patient data for clinical safety testing purposes.

## 3.0 Key Findings

I should explain that my investigation has primarily focused on the processing of data for the clinical safety testing of Streams, though my findings also have implications for the live version of the application now in operation.

### *3.1 Principle one*

Principle one of the Act requires that data be processed in a manner that is fair, lawful and transparent. At this point it is useful to turn to my office's published guidance regarding principle one which sets out that in practice, data controllers must:

- have legitimate grounds for collecting and using the personal data;

- not use the data in ways that have unjustified adverse effects on the individuals concerned;

- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

- handle people's personal data only in ways they would reasonably expect; and

- ensure they do not do anything unlawful with the data.

The requirement to ensure that processing is fair, lawful and transparent is key to all aspects of processing but takes on particular importance when the processing impacts on a large volume of individuals and when it involves the use of sensitive personal data.

Where sensitive personal data are to be used for a purpose that data subjects would not reasonably expect, or to which they have not directly consented, steps must be taken to engage with those affected. The exception to this is where an alternative condition for processing that does not require an individual's active consent applies.

My investigation has determined that under the terms of the agreement with the Royal Free, DeepMind processed approximately 1.6 million partial patient records for the purpose of clinical safety testing without those patients being informed of this processing. I was not satisfied that the Royal Free had properly evidenced a condition for processing that would otherwise remove the need to obtain the informed consent of the patients involved and our concerns in this regard remain.

It is also my view that, the Royal Free has not, during my investigation, and to my satisfaction, evidenced a valid condition for processing personal data under Schedule 2[1] to the Act during the clinical safety testing phase of the application.

I note that the Royal Free has, since my investigation began, made changes to improve transparency by way of additional information displayed on its website, including information on live clinical use.

### *3.1.1 Principle one – findings*

The processing of patient records by DeepMind significantly differs from what data subjects might reasonably have expected to happen to their data when presenting at the Royal Free for treatment. For example, a patient presenting at accident and emergency within the last five years to receive treatment or a person who engages with radiology services and who has had little or no prior engagement with the Trust would not reasonably expect their data to be accessible to a third party for the testing of a new mobile application, however positive the aims of that application may be.

The mechanisms to inform those patients that their data would be used in the clinical safety testing of the Streams application were inadequate. In short, the evidence presented to date leads me to conclude that data subjects were not adequately informed that the processing was taking place and that as result, the processing was neither fair nor transparent.

I have also considered whether the processing was lawful under the requirements of principle one. I have considered the arguments that have been advanced by the Royal Free in relation to confidentiality and 'direct care'. The question of direct care is inextricably linked to whether or not the Royal Free had implied consent and so had a basis for satisfying the common law duty of confidence. I have considered the advice supplied by the National Data Guardian (NDG) on this question. On the basis of my investigation, and having appropriate regard for the NDG's views, it is reasonable to conclude, as I do, that the Royal Free did not have a valid basis for satisfying the common law duty of confidence and therefore the processing of that data breached that duty.

In this light, the processing was not lawful under the Act.

[1] *Please see Appendix One*

Where the processing of sensitive personal data is taking place, data controllers must also be able to demonstrate that an appropriate Schedule 3 condition is met. It is our present opinion that the Royal Free is yet to evidence a valid Schedule 3 condition for processing for the clinical safety testing. I do however anticipate that the Royal Free will afford appropriate consideration to this as part of the proposed Privacy Impact Assessment.

### *3.2 Principle Three*

This requires that personal data be adequate, relevant and not excessive in relation to the purposes for which they are processed.

The Royal Free has explained that the records processed by DeepMind were required for clinical safety testing, and that the nature of the injury and the manner in which it may present gave the Royal Free cause to share a high volume of records. As it was explained to my office, this was partly to ensure that repeat incidences relating to the same patient were captured.

In respect of the estimated 1.6 million partial patient records processed by DeepMind, I have considered the Royal Free's representations as to why it was necessary for so many partial records to be used for the clinical safety testing of the Streams application.

Whilst high level explanations have been put forward by the Royal Free to explain why the processing of the sensitive personal data of 1.6 million patients was necessary – I have not yet been provided with sufficient evidence to support the case that so many partial records were absolutely and justifiably required for clinical safety testing.

#### *3.2.1 Principle Three – finding*

I am not persuaded that it was necessary and proportionate to process 1.6 million partial patient records in order to test the clinical safety of the application. The processing of these records was, in my view excessive and in contravention of principle three.

### *3.3 Principle six*

On page five of this letter I have set out my conclusions in relation to compliance with principle one of the Act. The lack of transparency and consent has also led me to determine that the majority of patients would not have been aware that

their personal data had been used for the clinical safety testing of the application and processed by DeepMind and that 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.

Specifically, as patients were not fully aware that DeepMind would be processing the information on the Royal Free's behalf, they could not fully exercise their rights to opt-out or to otherwise prevent processing. For example, and whilst the Royal Free has put forward the possibility of patients opting out of the processing in its responses to our enquiries, given the lack of awareness and the limitations of the information available to patients at the time the information was first streamed in November 2015, I do not believe that patients could fully exercise their right to prevent processing or to otherwise opt-out of inclusion within the data sets which DeepMind processed. Put plainly, if the patients did not know that their information would be used in this way, they could not take steps to object.

### *3.3.1 Principle six – finding*

The Royal Free has failed to demonstrate compliance with principle six as the circumstances under which personal data was processed by DeepMind on its behalf did not allow those individuals to fully exercise their rights as data subjects.

## *4.0 Principle Seven*

This principle requires that appropriate technical and organisational measures be taken to protect personal data.

Principle Seven also 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 were some controls in place at the time the patient records were used in the testing of the Streams application, my office's investigation has revealed that these controls were deficient in some areas and that the documentation in place at the initial stages of the agreement did not go far enough to ensure that the processing was undertaken in compliance with the Act. Specifically, it is my view that the information sharing agreement effective 30 September 2015 did not contain enough detail to ensure that only the minimal possible data would be accessible to DeepMind and that the processing would only be conducted for limited means. As such the requirements DeepMind must meet and maintain were not clearly stated. I am also concerned to note that the

processing of such a large volume of records containing sensitive health data was not subject to a full privacy impact assessment ahead of the project's commencement.

### *4.0.1 Principle Seven – finding*

Royal Free has failed to demonstrate compliance with principle seven as the initial agreement between the two parties and under which personal data was processed by DeepMind did not go far enough to fully comply with the Act.

I do however recognise that the Royal Free has since improved the documentation in place between the Trust and DeepMind and has increased patient visibility of the use of data for the Streams application.

### *4.0.2 – Other considerations*

In terms of the technical security of the dataset, it is understood that the data is subject to encryption at rest and whilst in transit. It is also understood that the Royal Free has received confirmation from the appropriate body that approval had been obtained for the Logical Connection Architecture for the transfer of data, and that the hosting location has been confirmed as compliant with two relevant Information Security Standards[2]. On this basis, I accept that there is no current evidence that the data has or will be at risk of processing by an unauthorised third party.

However, in line with the ICO's role to promote best practice, and taking into account our experience in investigating data security incidents and recognising the common pitfalls associated with these incidents, I advise the Royal Free as follows:

- It would appear that the information relayed as a result of a positive hit on the algorithm will be broadcast to dedicated portable devices held by Royal Free clinicians. The Royal Free should ensure that the security of these devices, and of the transmission of data to these, is adequate. In particular, it should ensure that any potential 'Bring Your Own Device' (BYOD) issues are carefully scoped and considered. Further guidance in this respect is enclosed;

[2] ISO9001 and ISO27001

- It is understood that access to the data set made available to DeepMind is on a real time basis and that DeepMind employees will only have access to it in a very narrow set of circumstances and specifically where they would need to investigate a software problem.

- It is further understood that all access to raw patient-identifiable data by DeepMind staff as part of the system administration is carefully logged in an audit trail, and is only carried out under the instruction of the Royal Free as part of the data processing. My office would like to make it clear that for as long as the data remains in DeepMind's or indeed any third parties possession, appropriate audit trails, logs and restrictive access provisions should be in place;

- Deletion of data should be undertaken in line with the appropriate standards (as already confirmed to me).

### *5.0 Live and ongoing use of patient data*

During the latter stages of my investigation and in early 2017, the use of patient data for Streams moved from clinical safety testing into the live use of the Streams application in the clinical environment.

The Royal Free has told my office that some early successes have already been achieved and that positive clinical outcomes have resulted from this for the patients concerned. As I have previously explained, it is not my wish to prevent or hamper such progress.

However, my concerns regarding the necessity and proportionality of the use of the sensitive data of 1.6 million patients remain despite the live deployment of the application. As you will note from the enclosed undertaking we have not reached a conclusion on this point and we believe it requires additional consideration.

### *6.0 Industry and sector awareness and support*

I acknowledge that the Royal Free and DeepMind have contended that the definition and application of 'direct care' is wide. I also acknowledge that the care of patients is of utmost importance, as is health research. My investigation has nonetheless identified the above compliance issues under the Act, which the Royal Free must address. I can, however, confirm that, in collaboration with the NDG, the Commissioner is committed to examining this matter further in order to

explore ways in which the ICO can support sectoral guidance in this area.

## 7.0 The Undertaking

In order to bring the aforementioned data processing into compliance with the Act I propose that the Royal Free agree to the terms set out in the enclosed undertaking.

On its return, the undertaking will be signed by me and the text will be published on the ICO's website. This document will be made public. A copy of the signed document will be returned to you for your records. You should note that any significant breach of a signed undertaking will likely to lead to enforcement action being taken.

Further, I will follow up the undertaking to gain assurance that the agreed actions have been implemented and embedded within the timeframe agreed.

If the Royal Free agrees to the undertaking, and commits to executing the steps within the stated timeframes, I will allow the data provided to DeepMind to continue to be used for the Streams application whilst the compliance measures required are put in place.

Should Royal Free London NHS Foundation Trust decline to sign the undertaking I will consider what formal steps are needed to secure compliance.

## 8.0 Third Party Audit

Recent communications between the Royal Free and me indicate that the Royal Free and DeepMind are committed to a third party audit of the processing arrangements. I welcome this, but wish to stress that the audit process should cover all of the compliance concerns detailed in this letter and enclosed undertaking. The results of the audit are to be presented to me. As you will see, I have referenced the proposed audit in the enclosed undertaking.

I recognise that this case has wide implications for the health care sector and that my findings will necessitate additional work for both the Royal Free and DeepMind. My office is available to discuss these findings, and the actions identified, further. Please do indicate if this is something either or both of you would like to take forward when responding to this letter.

## 9.0 Information to be placed in the public domain

As previously mentioned, my office will publish the undertaking once signed and this is likely to be accompanied by a press release or similar public statement. Given the interest in this matter, wider public and sector interest is anticipated and so it is likely that my office will undertake a proactive approach to sharing the details of our investigation, including the publication of this letter. Any commercial confidentiality concerns or similar should therefore be notified to me at the earliest possible opportunity.

## 10. Next steps

Please confirm at the earliest possible convenience and in any event by **3 July** whether the Royal Free London NHS Foundation Trust will agree to the enclosed undertaking and if so, provide a signed copy by that date.

Yours Sincerely,

Elizabeth Denham
**Information Commissioner**

## Appendix One

**http://www.legislation.gov.uk/ukpga/1998/29/schedule/2**

***SCHEDULE 2 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA***

*1The data subject has given his consent to the processing.*
*2The processing is necessary—*
*(a)for the performance of a contract to which the data subject is a party, or*

*(b)for the taking of steps at the request of the data subject with a view to entering into a contract.*

*3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*
*4The processing is necessary in order to protect the vital interests of the data subject.*
*5The processing is necessary—*
*(a)for the administration of justice,*

*(b)for the exercise of any functions conferred on any person by or under any enactment,*

*(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or*

*(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.*

*6(1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.*
*(2)The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.*

## Appendix Two

**http://www.legislation.gov.uk/ukpga/1998/29/schedule/3**

*SCHEDULE 3. Conditions relevant for purposes of the first principle: processing of sensitive personal data*

*1The data subject has given his explicit consent to the processing of the personal data.*

*2(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.*

*(2)The Secretary of State may by order—*

*(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or*

*(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.*

*3 The processing is necessary—*

*(a)in order to protect the vital interests of the data subject or another person, in a case where—*

*(i)consent cannot be given by or on behalf of the data subject, or*

*(ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or*

*(b)in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.*

*4 The processing—*

*(a)is carried out in the course of its legitimate activities by any body or association which—*

*(i)is not established or conducted for profit, and*

*(ii)exists for political, philosophical, religious or trade-union purposes,*

*(b)is carried out with appropriate safeguards for the rights and freedoms of data subjects,*

*(c)relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and*

*(d)does not involve disclosure of the personal data to a third party without the consent of the data subject.*
*5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.*
*6 The processing—*
*(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),*
*(b)is necessary for the purpose of obtaining legal advice, or*
*(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.*
*7 (1)The processing is necessary—*
*(a)for the administration of justice,*
*(aa)for the exercise of any functions of either House of Parliament,*
*(b)for the exercise of any functions conferred on any person by or under an enactment, or*
*(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department.*
*(2)The Secretary of State may by order—*
*(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or*
*(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.*
*7A(1)The processing—*
*(a)is either—*
*(i)the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or*
*(ii)any other processing by that person or another person of sensitive personal data so disclosed; and*
*(b)is necessary for the purposes of preventing fraud or a particular kind of fraud.*
*(2)In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to*

*prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.*

*8 (1)The processing is necessary for medical purposes and is undertaken by—*

*(a)a health professional, or*

*(b)a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.*

*(2)In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.*

*9 (1)The processing—*

*(a)is of sensitive personal data consisting of information as to racial or ethnic origin,*

*(b)is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and*

*(c)is carried out with appropriate safeguards for the rights and freedoms of data subjects.*

*(2)The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.*

*10The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.*