Dated 17 May 2018

An addendum was added to the end of this Report on 7 June 2018 to address the implications of the General Data Protection Regulation and the Data Protection Act 2018.

Audit of the acute kidney injury detection system known as Streams

The Royal Free London NHS Foundation Trust

Linklaters

Linklaters LLP
One Silk Street
London EC2Y 8HQ

Telephone (+44) 20 7456 2000
Facsimile (+44) 20 7456 2222

Ref Peter Church

A summary for the patients of the Royal Free

In 2015, the Royal Free started a project with DeepMind to help detect acute kidney injury. This is a very serious condition estimated to cause 40,000 deaths, and costs the NHS over £1 billion, a year. A range of options to detect acute kidney injury were considered initially, including the use of artificial intelligence. However, the project eventually resulted in the development of a much simpler solution known as Streams.

The project started to attract public interest in early 2016. This led to an investigation by the National Data Guardian and the Information Commissioner. The Information Commissioner raised a number of concerns. They include that the agreement between the Royal Free and DeepMind was not sufficiently robust, that the Royal Free had not conducted a privacy impact assessment at the start of the project and that the Royal Free had not done enough to tell patients about these arrangements.

The Royal Free accepted the Information Commissioner's findings and took a number of remedial steps to address them. They include putting a much stronger agreement in place with DeepMind and providing more information on the Royal Free's website about the arrangements with DeepMind.

The Information Commissioner wanted to confirm if these steps were sufficient to ensure the Royal Free was now complying with data protection law and respecting the privacy and confidentiality rights of its patients. She therefore ordered the Royal Free to carry out a third party audit into Streams. The Royal Free instructed us, Linklaters LLP, to conduct that audit.

This report sets out our conclusions. We have reviewed the use of Streams and the remedial steps taken by the Royal Free. We consider the Royal Free's use of Streams is lawful. However, the audit has identified some areas in which further improvements should be made. For example, the Royal Free needs to do more to tell patients who visit its hospitals about how their information will be used. The Royal Free has accepted our recommendations and is working to implement them.

While there is still room for improvement, we do not think patients should be concerned about the use of Streams. Most importantly:

- **DeepMind only uses patient information for the purpose of providing Streams**. It does so under the direction of the Royal Free and in strictly controlled conditions. DeepMind is not permitted to use patient information for any other purpose.
- **Streams does not use artificial intelligence**. Instead, it implements a simple decision tree used across the whole of the NHS.
- **We have seen nothing to cast doubt on the safety and security of the patient information used in Streams**. There are systems and controls used to protect patient information. The teams at both the Royal Free and DeepMind clearly understand the confidential and sensitive nature of health information and act accordingly.

Further information is set out in the body of this report. It provides an overview of the operation of Streams, the relationship between the Royal Free and DeepMind and an analysis of data protection and confidentiality laws.

Finally, the clinicians we spoke to said Streams made a real difference to patient care. Proposals to further develop Streams have been put on hold while we carried out our audit. We hope the completion of this report means these proposals can finally proceed.

Linklaters LLP
17 May 2018

Table of Contents

Contents **Page**

Executive Summary

1 Acute kidney injury & Streams

1.1 What is acute kidney injury?

Acute kidney injury or AKI is sudden damage to the kidneys that causes them to not work properly. It can range from minor loss of kidney function to complete kidney failure.

It is a very serious condition and is estimated to cause 40,000 deaths, and costs the NHS over £1 billion, a year (see paragraph 9).

It is essential that AKI is detected early and treated promptly. Without quick treatment, abnormal levels of salts and chemicals can build up in the body, which affects the ability of other organs to work properly. If the kidneys shut down completely, this may require temporary support from a dialysis machine or lead to death.

1.2 How does Streams help?

Streams is used by the Royal Free to help manage AKI. Clinicians in the Royal Free's renal team and acute care team are provided with iPhones preloaded with the Streams App. That App performs two important functions:

- Firstly, it provides a real time alert to clinicians if a patient is at risk of, or has developed, AKI. It does this by analysing blood tests carried out on the patient in the last 12 months using a decision tree developed by the NHS (see paragraph 11.2). This is a significant improvement on the previous process which relied on clinicians logging into the Royal Free's system to obtain the patient's results.
- Secondly, it provides details of patient's previous medical history. This history is needed by the clinician to diagnose and treat the patient. This history is available on the Royal Free's other information technology systems, but Streams draws this information into a single place (which saves time) and allows mobile access to that information, for example at the patient's bedside or by a consultant on call. Streams currently contains eight years of medical history (see paragraph 11.3).

The clinicians we spoke to found Streams extremely useful when treating patients. It helps ensure patients who might have AKI are seen promptly. The provision of contextual clinical information avoids the time-consuming process of extracting that information from the Royal Free's various other information technology systems (see paragraph 16.5).

A service evaluation is being carried out by academics to determine whether Streams delivers better outcomes for patients. However, that study had not been completed by the time we finalised our report.[1]

The Imperial College Healthcare NHS Trust, Taunton and Somerset NHS Trust and Yeovil District Hospital NHS Foundation Trust have also entered into agreements with DeepMind to use Streams.

[1] See https://f1000research.com/articles/6-1033/v1.

1.3 How many clinicians have access to the Streams App? Is it secure?

The Streams App is only used by the renal team and acute care team at the Royal Free. They can only use the Streams App on iPhones owned by the Royal Free. There are eight such iPhones.

The Streams App is subject to multiple layers of security. The iPhones are protected by PIN codes and encryption. Once the iPhone is unlocked, clinicians must use their username and password to access the Streams App. The username and password are verified on the Royal Free's LDAP servers (see paragraph 11). Information security specialists, First Base, reviewed the security of the Streams App last year and did not raise any significant concerns (see paragraph 11.8).

However, when we reviewed the LDAP access list, we discovered that some clinicians on that list are no longer working at the Royal Free. The Royal Free addressed this issue prior to the completion of our Report (see paragraph 16.5).

1.4 Why does <u>any</u> information need to be stored on Streams? Couldn't Streams just request that information from the Royal Free's systems as and when required?

We discussed this issue with the Royal Free. In summary, the Royal Free's technology does not support an alternative model in which Streams requests confidential patient information from the Royal Free's systems as and when required. The reasons for this are complex and are described in more detail in paragraph 26.1.

In any event, the clinicians at the Royal Free have access to all of this confidential patient information on the Royal Free's other systems. Thus, the question is not whether the Royal Free should store this information in Streams, but rather whether the Royal Free should store it in Streams as well as in the Royal Free's other systems.

1.5 If the purpose of Streams is to detect acute kidney injury, why doesn't it only contain blood tests for the last 12 months?

The purpose of the Streams App is not just to implement the NHS AKI algorithm to detect AKI, which would only require blood tests for the last 12 months. The Streams App also provides details of patients' previous medical history. This history is needed by the clinician to diagnose and treat the patient.

For example, if the patient has had a nephrectomy (removal of a kidney) or diabetes, they are more likely to be a priority if they trigger an AKI alert. Similarly, knowing the patient suffers from other conditions, such as kidney stones or hyperkalemia (elevated potassium levels), will help the management of the patient (see paragraph 11.3).

The clinicians could access confidential patient information from the Royal Free's other information technology systems. However, that information is spread across multiple other systems, so logging into them all to extract the information would be time-consuming. One of the clinicians we spoke to said that Streams saves an hour a day. Streams also allows mobile access to this information. This means a clinician can access it at a patient's bedside or a renal consultant can access when off-site but on call.

Again, the clinicians at the Royal Free have access to all of this information on the Royal Free's other systems in any event, so the question is not whether the Royal Free should store this information in Streams, but rather whether the Royal Free should store it in Streams as well as in the Royal Free's other systems.

1.6 Why does Streams store eight years of medical history? Wouldn't a shorter period be sufficient?

There is currently no retention period for confidential patient information on Streams. In other words, there is no process to delete a patient's medical history once it reaches a certain age. This means the information on Streams currently dates back eight years.

We discussed this with clinicians at the Royal Free. Whilst older information is not used to generate AKI alerts, it provides details of a patient's previous medical history. The clinicians suggested they would like to have as much information as possible and some information will be highly relevant even if it is 10 or even 20 years old. In addition, this information is retained for a longer period on the Royal Free's other systems so, again, the question is not whether the Royal Free should store this information in Streams, but rather whether the Royal Free should store it in Streams as well as in the Royal Free's other systems.

Having discussed this with clinicians, we do not think the current lack of a fixed retention period results in patient information being kept longer than is necessary for medical purposes. The information is currently approximately eight years old, a retention period that is within the guidelines from the Department of Health. However, the Royal Free should consider this issue in detail and set an upper limit on the age of the information contained in Streams (see paragraph 27).

1.7 Does Streams include information about patients who visit the Barnet and Chase Farm hospitals?

Yes. The Royal Free sends information about patients at the Royal Free, Barnet and Chase Farm hospital to Streams. This is despite the fact that only clinicians at the Royal Free hospital in London currently use the Streams App.

This is because the three hospitals operate as a single unit and a patient will move between the three hospitals as part of their treatment. We were informed by clinicians that access to information from all three hospitals is essential to the proper treatment of those patients (see paragraph 26.2). There is also a proposal to provide the Streams App to clinicians at the Barnet hospital (see paragraph 13.1).

1.8 How does the technology behind Streams work?

The Royal Free provides information to Streams primarily through a secure stream of messages in an industry standard format known as HL7 (see paragraph 10.2). The Streams system is also fed with other information, such as HES data which provides additional contextual information needed by clinicians to treat patients (see paragraph 10).

When a HL7 message containing a blood test is received, it will be processed by Streams using the NHS AKI algorithm to determine if it should trigger an AKI alert. That algorithm does not use artificial intelligence or machine learning. Instead, it uses a simple decision tree developed by the NHS (see paragraph 12).

2 DeepMind

2.1 What is DeepMind's role?

DeepMind developed Streams. It provides the Streams App to the Royal Free and hosts Streams.

However, DeepMind is only able to use confidential patient information for the purposes of providing Streams to the Royal Free. DeepMind is not permitted to use that information for any other purpose.

Under data protection law, the Royal Free is a data controller (and so decides what confidential patient information is used for) and DeepMind is a data processor (and so can only use that confidential information on the Royal Free's instructions). We have reviewed the relationship between the Royal Free and DeepMind (see paragraph 20). We can see no reason to categorise DeepMind as anything other than a data processor.

2.2 Are the arrangements with DeepMind set out in a contract?

Yes. The Royal Free has an Information Processing Agreement and a Services Agreement with DeepMind.

The Information Processing Agreement imposes strict controls on DeepMind's use of confidential patient information and only permits DeepMind to use confidential patient information in accordance with the Royal Free's instructions. It also contains a number of other provisions, such as a prohibition on DeepMind disclosing confidential patient information to third parties without the Royal Free's consent, and an obligation to delete that information if instructed by the Royal Free. It also obliges DeepMind to implement various security measures.

We consider that the Information Processing Agreement imposes suitable obligations on DeepMind. However, we have recommended one minor change in light of the upcoming EU General Data Protection Regulation (see paragraph 19.2).

2.3 Does DeepMind have appropriate security measures in place?

DeepMind hosts Streams in a datacentre in England. The datacentre is owned by a third party who provides space to DeepMind under a co-location arrangement (see paragraph 10.10). Information security specialists, First Base, reviewed the security of the datacentre last year and did not raise any significant concerns (see paragraph 10.12).

Only eight DeepMind employees have access to the "live" Streams servers containing confidential patient information. All have a direct need to access those servers and their access rights are renewed regularly. Their access to Streams is logged and reviewed periodically (see paragraph 17.5).

3 Development and testing

3.1 Is patient information used in the design and development process?

No. The design and development of modifications to Streams would be carried out by DeepMind using synthetic data. This is manufactured data that does not relate to an individual. Its use does not affect the privacy or confidentiality of any patient.

3.2 Is patient information used for testing?

DeepMind will test modifications to Streams using synthetic data to check those modifications work property. Once DeepMind is satisfied with its testing, the Royal Free will need to carry out clinical safety and effectiveness testing of that modification prior to deployment (with technical assistance from DeepMind).

Clinical safety and effectiveness testing must be carried out with confidential patient data to assure the safe operation of Streams in accordance with the NHS' information technology standards (see paragraph 14).

This testing may require the Royal Free to use a full set of confidential patient information. For example, clinical safety testing is likely to require side-by-side use of Streams with the existing system so that the output from Streams can be compared to that of the existing system. That side-by-side testing may well only work if Streams is loaded with a full data set to ensure it contains the relevant confidential patient information to compare with the existing system (particularly given that Royal Free's systems do not allow Streams to request that information as and when required, see paragraph 1.4).

We have concluded that the use of confidential patient information for testing is lawful, provided that it is genuinely necessary for that purpose (see paragraphs 24.4 and 33.3). We recommend the Royal Free confirms this to be the case as part of the privacy impact assessment for any future modifications. The Royal Free should clearly document: (a) the justification for using confidential patient information, rather than synthetic data; (b) the justification for the volume of confidential patient information being used in testing including a consideration of whether a smaller amount would suffice; and (c) the controls used to protect that confidential patient information.

3.3 What projects are currently under consideration?

The Royal Free is considering a range of potential developments to Streams, including providing Streams-enabled iPhones to clinicians at its Barnet hospital. However, these plans have been put on hold pending the finalisation of this Report.

A privacy impact assessment should be completed for these projects before they proceed, other than the extension to Barnet, for which a privacy impact assessment has already been completed (see paragraph 13).

4 Governance and accountability

4.1 What steps has the Royal Free taken to look after patient information?

The Royal Free has structures and processes in place to manage its use of confidential patient information. The Royal Free has an Information Governance Group that meets quarterly to discuss data protection and confidentiality issues (see paragraph 16.1). The senior leadership team confirmed that respecting patient confidentiality is fundamental to the operation of the hospital.

The Royal Free has a data protection officer and an information governance manager to manage data protection and confidentiality issues. Both have significant experience and have been at the Royal Free for a number of years (see paragraphs 16.3 and 16.4). The Royal Free intends to appoint its data protection officer as the statutory data protection officer under the General Data Protection Regulation. We have some concerns this might create a conflict of interest given the data protection officer is also responsible for parts of the Royal Free's information technology estate.

The Royal Free has policies and training addressing data protection and confidentiality (see paragraph 16.6). We had some concerns about whether all of the clinicians are repeating their training annually (see paragraph 16.5). However, all the clinicians whom we spoke to clearly understood their duties in relation to confidential patient information.

4.2 What steps has DeepMind taken to look after patient information?

DeepMind has structures and processes in place to manage its very limited use of confidential patient information. DeepMind has an Information Governance Management Framework setting out its approach to information governance and an Information Governance Board to address these issues (see paragraph 17.1). The senior leadership team at DeepMind expressed strong support for proper information governance.

DeepMind has an information governance lead who has significant experience in that role, having previously worked in an information governance role for a number of NHS trusts (see paragraph 17.4).

DeepMind has information governance policies and requires that its employees take annual information governance training. All the DeepMind employees we interviewed, including the senior leadership team, had taken that training annually (see paragraph 17.6).

All the DeepMind employees whom we spoke to clearly understood their duties in relation to confidential patient information.

5 Data protection laws

5.1 Are these arrangements subject to data protection law?

Yes. These arrangements are subject to the Data Protection Act 1998 (see paragraph 22).[2] As data controller, the Royal Free must comply with the eight data protection principles in respect of confidential patient information.

5.2 Is the operation of Streams lawful under the Data Protection Act 1998?

Yes. The Royal Free is under an obligation to process confidential patient information fairly and lawfully (see paragraph 23). We consider that processing for the operation of Streams is fair and lawful. It satisfies:

- a processing condition on the basis that it is necessary to protect the vital interests of patients (see paragraph 4, Schedule 2, Data Protection Act 1998) and that it is necessary for the exercise of the Royal Free's statutory functions (see paragraph 5(b), Schedule 2, Data Protection Act 1998);[3] and
- a sensitive personal data processing condition on the basis that it is necessary for medical purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (see paragraph 8, Schedule 3, Data Protection Act 1998) and that it is necessary for the exercise of the Royal Free's statutory functions (see paragraph 7(1)(b), Schedule 3, Data Protection Act 1998).[4]

[2] The Royal Free will need to comply with the General Data Protection Regulation from 25 May 2018, see paragraph 22.2.

[3] The General Data Protection Regulation contains equivalent conditions in: (a) article 6(1)(d); and (b) article 6(1)(e), read in light of section 8 of the Data Protection Bill.

[4] The General Data Protection Regulation contains equivalent conditions in: (a) article 9(2)(h), read in light of sections 10 and 11 and Schedule 1, para 2 of the Data Protection Bill; and (b) article 9(2)(g), read in light of sections 10 and Schedule 1, para 6 of the Data Protection Bill. Paragraph 6 contains an additional requirement that the processing be in the substantial public interest, which we consider would be satisfied here.

5.3 Is the testing of Streams lawful under the Data Protection Act 1998?

Yes. The Royal Free's future use of confidential patient information for the testing of Streams will be fair and lawful so long as it is genuinely necessary for that purpose, minimised as far as possible and appropriate controls are in place (see paragraph 24). It would satisfy:

- a processing condition on the basis that it is necessary to protect the vital interests of patients (see paragraph 4, Schedule 2, Data Protection Act 1998) and that it is necessary for the exercise of the Royal Free's statutory functions (see paragraph 5(b), Schedule 2, Data Protection Act 1998)[5]; and
- a sensitive personal data processing condition on the basis that it is necessary for medical purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (see paragraph 8, Schedule 3, Data Protection Act 1998). We understand the testing of Streams using confidential patient information would be carried out in a clinical environment, so would be done for the treatment of patients. Such testing is also "necessary" for the live deployment of that system and subsequent treatment of future patients. Alternatively, we consider this to be necessary for the exercise of the Royal Free's statutory functions (see paragraph 7(1)(b), Schedule 3, Data Protection Act 1998).[6]

We recommend that the Royal Free documents its approach to this issue as part of the privacy impact assessment for any future modifications (see paragraph 3.2).

5.4 Has the Royal Free done enough to tell patients about Streams?

The Royal Free provides a range of information about Streams on its website, including a number of videos about the operation of Streams. We consider the information on the website to be more than sufficient to describe Streams, given DeepMind's limited role as a data processor (see paragraphs 20.3 and 25).

However, we think that the Royal Free could do more to bring this information (and information about its processing more generally) to the attention of patients when those patients attend the Royal Free in person. For example, the Royal Free could include a signpost to this information on the electronic registration terminals (see paragraph 25).

The information that the Royal Free provides to patients will also need to be amended in light of the EU General Data Protection Regulation from late May 2018.

5.5 What rights do I have if my information is on Streams?

Patients have a right to make a subject access request to obtain copies of any personal data stored on Streams, and the right to object to the processing of their personal data on Streams.

We reviewed the Royal Free's processes to deal with subject access requests from patients for information in Streams and requests not to be included in Streams. We also sampled redacted copies of correspondence addressing these rights.

We consider that the Royal Free has appropriate procedures in place to deal with these rights, albeit we have made some minor recommendations about the way the Royal Free responds to patients (see paragraph 28).

---

[5] See footnote 3 for the relevant condition under the General Data Protection Regulation.

[6] See footnote 4 for the relevant condition under the General Data Protection Regulation

6 Confidentiality

6.1 Has the Royal Free breached its duty of confidence by using Streams? Would it breach that duty of confidence if it used patient information for testing in the future?

The application of the law of confidence to modern health care is not straightforward. Many patients no longer have a simple bilateral relationship with a single doctor. Instead, they are treated in a complex multi-agency environment with support from different specialists using a range of information technology systems.

We have considered how these issues apply to the Royal Free and consider that its duty of confidence arises in equity (see paragraph 31.3). The equitable duty is derived from the patient's relationship with the health professional and the private and confidential nature of information about a patient's health. As such, the key question to determine whether there is a breach of confidence is: would the use trouble the conscience of a reasonable health professional (see paragraph 31.4)?

We consider that the use of confidential patient information for the purposes of testing and operating Streams is compatible with this equitable duty of confidence. This use should not offend the "conscience test" (as described in the body of this Report at paragraphs 31.4 and 33).

If we are wrong about the duty of confidence arising in equity, we consider that the duty would be based around Article 8 of the European Convention. This requires a consideration of whether the use is an infringement of the patient's privacy, including if the use would be in accordance with the "reasonable expectations" of patients. If there is an infringement, there must be an assessment of whether that infringement is in accordance with law, proportionate and for a legitimate aim. We consider use of confidential patient information for the purposes of testing and operating Streams would also be compatible with this alternative test (see paragraph 31.8).

6.2 Has the Royal Free complied with professional guidance on the use of patient information?

Compliance with professional guidance will have a significant bearing on whether the "conscience test" is met. We have therefore considered whether the use of confidential patient information for the purposes of testing and operating Streams is consistent with that guidance. We consider that the proposed use of confidential patient information is compatible with professional guidance (see paragraph 32).

7 Recommendations

Our audit has identified some areas in which further improvements should be made. These are set out at the end of this Report (see paragraph 34).

8 Scope of the Report

8.1 Scope and reliance

This Report contains an assessment of the data protection and confidentiality issues associated with the data protection arrangements between the Royal Free and DeepMind. It is limited to the current use of Streams, and any further development, functional testing or clinical testing, that is either planned or in progress. It is not a historical review. It includes

consideration as to whether the transparency, fair processing, proportionality and information sharing concerns outlined in the Undertakings are being met.

Important information about the scope of this Report, the process of preparing the Report and any reliance that can be placed on it is set out in Annex 3.

8.2 Glossary

We have included a glossary of terms in Annex 1.

8.3 No access to confidential patient information

In preparing this Report, we have not sought access to, nor been provided with, any confidential patient information. Instead, we asked to be provided with redacted or synthetic data (see paragraph 14.7). We have also only used the Streams App in DeepMind's development environment, which is loaded with synthetic data.

Access to real confidential patient information might have been helpful. For example, we could have reviewed details of the actual HL7 messages sent to Streams to confirm their contents (though they are all based on a standardised format) or used the Streams App in the live environment (to confirm the operation is the same in the development environment). However, we felt access to confidential patient information was inappropriate and also unnecessary in order to finalise this Report.

8.4 Exclusions

The following issues fall outside the scope of this Report:

- Any technical assessment of the security of Streams, which was instead recently assessed by First Base (see paragraphs 10.12 and 11.8). However, the Report does consider operational security measures.
- The data protection and confidentiality issues associated with the processing of personal data about the clinicians at the Royal Free using the Streams App.
- Any assessment of the effectiveness of the Streams App, save to the extent directly related to data protection and confidentiality. In particular, we have not reviewed the current medical research to conduct a service evaluation of the efficacy of Streams.[7]
- Any area of law apart from data protection and confidentiality. The Undertakings and this Report do not extend to issues such as medical negligence, employment law, administrative law, intellectual property law, medical device regulation, telecoms law, network and information systems law, competition law or public procurement law.
- A historical review of issues arising prior to the date of our appointment, save to the extent relevant to current live clinical use of Streams, and any further development, functional testing or clinical testing, that is either planned or in progress. Instead, our audit focuses on whether the steps taken by the Royal Free are sufficient to address the Information Commissioner's concerns and bring the Royal Free into compliance with data protection and confidentiality laws.
- A detailed review of compliance with the EU General Data Protection Regulation, which will not apply to the United Kingdom until 25 May 2018, or the Data Protection Bill which has not yet been passed by Parliament. However, we note issues that are

[7] See https://f1000research.com/articles/6-1033/v1.

likely to arise under the General Data Protection Regulation and the Data Protection Bill where relevant to Streams.

- A general review of the Royal Free's compliance with data protection and confidentiality law, save to the extent directly relevant to the current live clinical use of Streams, and any further development, functional testing or clinical testing of Streams, that is either planned or in progress.

Part A: Acute kidney injury & Streams

9 Clinical need

9.1 Acute kidney injury

Acute Kidney Injury (AKI) is sudden damage to the kidneys that causes them to not work properly. It can range from minor loss of kidney function to complete kidney failure.

AKI is not the result of a physical blow to the kidneys. Instead, most cases of AKI are caused by reduced blood flow to the kidneys, usually in someone who is already unwell with another health condition. AKI can also be caused by a problem with the kidney itself or a blockage affecting the drainage of the kidneys.

9.2 Diagnosing acute kidney injury

AKI can be diagnosed using urine and blood tests. Blood levels of creatinine – a chemical waste product produced by the muscles – are measured. Healthy kidneys filter creatinine and other waste products from the blood and these are excreted in the form of urine. Higher levels of creatinine in the blood indicate poorer kidney function.

The NHS AKI algorithm is used to analyse those creatinine readings (see paragraph 12.1).

9.3 Need for urgent treatment

It is essential that AKI is detected early and treated promptly. The kidneys perform a number of vital functions, including filtering and cleaning blood, keeping the bones healthy, managing blood pressure and stimulating the bone marrow to make blood.

Without quick treatment, abnormal levels of salts and chemicals can build up in the body, which affects the ability of other organs to work properly.

If the kidneys shut down completely, this may require temporary support from a dialysis machine or lead to death.[8]

9.4 Frequency and effect of acute kidney injury

AKI is one of the most serious and common complications affecting hospital inpatients. AKI was recorded in approximately 2.5% of hospital admissions in Hospital Episode Statistics, but estimates derived from laboratory data suggest the true prevalence may be more than five times as high (approximately 14%).

Studies have estimated that the annual number of excess in-patient deaths associated with AKI in England may be above 40,000. The annual cost of AKI-related inpatient care in England is estimated at £1 billion, just over 1% of the NHS budget. The lifetime cost of post-discharge care for people who had AKI during hospital admission is estimated at approximately £175 million.[9]

[8] See Acute Kidney Injury, https://www.nhs.uk/conditions/acute-kidney-injury/

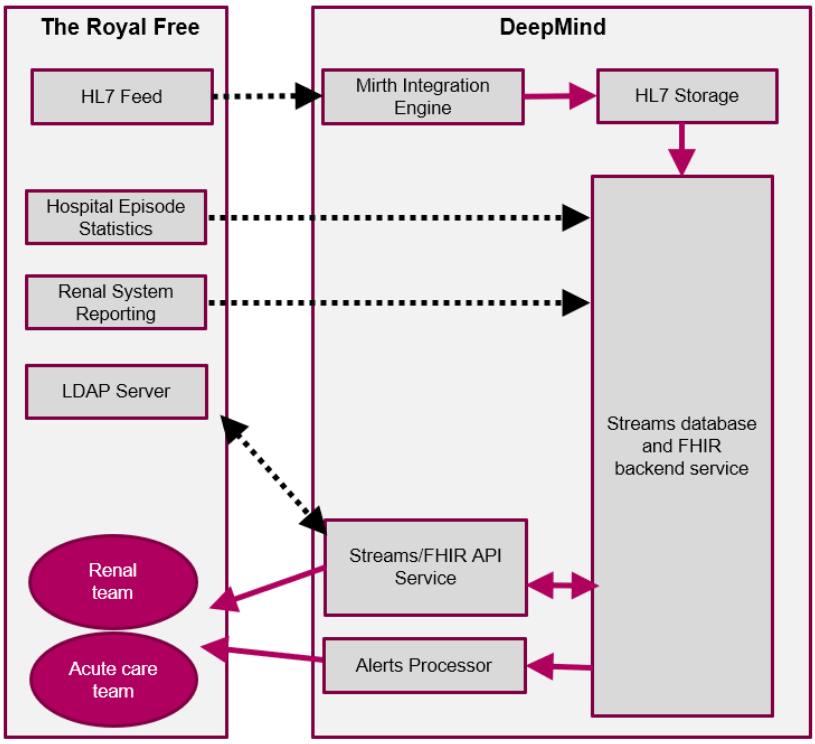
[9] See Kerr M, Bedford M, Matthews B, *et al*.: The economic impact of acute kidney injury in England. *Nephrol Dial Transplant*. 2014; 29(7): 1362–1368.

10 The Streams infrastructure

This section provides a high-level description of the technology used in Streams. The description is intended to provide context to the rest of the Report but is not comprehensive.

10.1 Overview of Streams

The diagram below sets out how Streams operates:



The Royal Free transfers the following data to Streams:

- *HL7 messages* – The HL7 messages contain details about patients' treatment and are described in more detail in paragraph 10.2. These messages are transferred to Streams via the NHS's secure and encrypted N3 network;
- *Hospital Episode Statistics* – The HES data contains details about the patient's previous diagnosis and procedures (see paragraph 10.4). This data is transferred by SSH File Transfer Protocol;
- *Renal system reporting* – This contains a list of patients undergoing dialysis (see paragraph 10.5);
- *LDAP server* – When a Royal Free clinician logs into the Streams App, their username and password will be authenticated on the Royal Free's LDAP server (see paragraph 11.5); and
- *Hospital resource information* – The Royal Free also transfers non-patient information to operate Streams, such as information about consultants or beds. We do not consider this information in our Report.

10.2 HL7 message standard

Clinical and administrative information is transferred between many of the Royal Free's systems, and those of third parties, by sending Health Level-7 or HL7 messages.

HL7 is an international standard produced by the not-for-profit international standards body, Health Level Seven International. HL7 is recognised in various ISO standards. It is a very widely used standard; Health Level Seven International has more than 1,600 members from over 50 countries, including over 500 corporate members representing healthcare providers, government stakeholders and suppliers. HL7 is widely used in the NHS, and the NHS Interoperability Toolkit uses open international standards which are aligned with HL7.

HL7 messages are in a standardised format which allows interoperability between the many different computer systems used by most healthcare providers.

The HL7 message contains a range of datafields, separated by a delimiter character (such as a "|", "^", "&" or "~"). The exact datafields depend on the type of message. An example of an HL7 message is set out below:[10]

MSH|^~\&|RADIOLOGY|RAL|MILLENNIUM||20180105002000||ORU^R01|201801050020000|T|2.3|||AL||44|ASCII

PID||47591151516620216^^^^MRN|47591151536800321^^^^MRN~6024515707^^^^NHSNMBR||Browne^Melanie^^^MR^^CURRENT||19070426|F|||roadFitzgerald0^laneReed0^avenueParkinson0^^620 216Ingram^countyHardy0^HOME^^ |||||||^^^RAL^FINNBR ||||P||||||||

PV1|1|INPATIENT |RALWHDS^ WH^5^RAL WH^^BED^RFH^2^ ||||C1234567^Dr. A Consultant|||241||||19 ||||INPATIENT |26452762^^^^visited |||||||||||||||||||||||| 20180105002000|||||||| OBR|1 |47591151516891055|47591151516830961 |N623^RENAL DYNAMIC INJ.F-15 || 20180105002000|20180105002000||||||||| C1234567^DR. A Consultant |||||306360202|20180105002000 ||1|f||1^^^20180105002000^^r|^||

OBX |2|FT|N623^RENAL DYNAMIC INJ. F-15||Adenosine stress protocol: Adenosine stress protocol [12.345mg/kg/min adenosine infused over 4 minutes with stress perfusion imaging performed during the last minute of the adenosine infusion using an FGRE-ET sequence and a gadolinium dose of 0.123 mmol/kg. Rest perfusion imaging was performed was then performed after appropriate delay using additional gadolinium dose of 0.123 mmol/kg. Cine white blood imaging including short axis and two, three and four chamber long axis views was performed using a FIESTA sequence to evaluate cardiac morphology and function. Delayed enhanced imaging was performed using an Inversion recovery prepared gradient echo sequence. Images were postprocessed on a computer workstation to assess cardiac anatomy and ventricular function. W.]Q=ZILsuMH{`OJ*%En8Vn$?%}F-:t/}-dI>`FM||||||F|||||

[1010] This is not a real HL7 message. It is a sample taken from the synthetic data used by DeepMind. Hence, the unlikely nature of the information in the message such as the reference to "Mr" Melanie Brown, who lives in "Hardy, Ingram", is 110 years old and is undergoing myocardial stress imaging tests.

To take the various paragraphs of the message in turn:

- MSH is the message header. This indicates the message is an ORU^R01 type, which means “Observation Result”;
- PID is the “Patient Identification” segment. From this paragraph, it is possible to determine the patient’s MRN is 47591151516620216 and NHS number 6024515707. Her name is Mr Melanie Brown. Her date of birth is 26 April 1907. She is female. Her address is Fitzgerald, Reed, Parkinson, Ingram 620216, Hardy. The PID fields can include a range of other information such as ethnic origin and contact details but they are not present in this message;
- PVI is the “Patient Visit” segment. It includes information such as the bed the patient is in and the name of the doctor - “Dr A Consultant”; and
- the OBX paragraph contains a free text observation about the patient: “*Adenosine stress protocol: Adenosine … and ventricular function*”.

Various events during a patient’s journey through the Royal Free will trigger an HL7 message. The combination of those HL7 messages provides a medical record of the patients as they progress through the hospital.

The format for the various types of HL7 message are available from Health Level Seven International’s website.

10.3 Stream’s use of HL7 messages

The Royal Free feeds HL7 messages to Streams via the N3 network. The HL7 messages are sent for all patients visiting any of the three Royal Free hospitals, namely the Royal Free, Barnet and Chase Farm. We consider the proportionality of sending information about patients at Barnet and Chase Farm at paragraph 26.2.

Not all HL7 messages are transferred to Streams.[11] The HL7 feed is instead limited to the following message types (“**relevant HL7 messages**”):

- ADT – Admit discharge transfer;
- ORM – Order, e.g. for a blood test;
- ORR – Acknowledgement of an order; and
- ORU – Observation result (see example above).

Streams ingests the HL7 messages using the Mirth Connect software. This is an open source HL7 interface engine that runs on the Streams infrastructure. Mirth Connect filters out HL7 messages that relate to patients who have opted out of Streams (see paragraph 28.2).

The raw HL7 messages are stored in an HL7 database. We were informed the information in those HL7 messages is materially the same as the information in the Streams database. However, the raw HL7 messages are kept to debug Streams (e.g. if there was a problem transferring that information into the main Streams database). They are also needed to “recompile” the Streams database. For example, if the data format in Streams were to

[11] For example, the Royal Free does not provide SIU messages for scheduling appointments, RAS/RDE/RGV messages which relate to orders to a pharmacy or dispensing solutions or MDM, which is used to manage medical records.

change, the HL7 messages could be reprocessed in order to repopulate that Streams database.

10.4 HES data

The information in the HL7 messages does not contain coding for previous patient diagnosis or procedures. This is important contextual clinical information and is instead provided using HES data transferred from the Royal Free using SSH File Transfer Protocol.

The HES data transferred by the Royal Free just contains the patient's MRN and fields describing previous diagnosis or procedure codes and not other HES fields.

The HES data is coded using the NHS mandated standards ICD 10 2016 for diagnosis coding and OPCS 4.8 for procedure coding.

HES data is not loaded for patients who have opted out of Streams (see paragraph 28.2).

10.5 Renal system reporting

The Royal Free also transfers information about renal system reporting. This provides a list of patients currently undergoing dialysis. This information is important as these patients' creatinine levels tend to vary significantly during dialysis. This is not a source of immediate concern, hence AKI alerts for these patients are screened out to avoid false alarms.

The renal system reporting information the Royal Free transfers into Streams only includes the patient's MRN and the fact they are undergoing dialysis during that period.

10.6 Initial set of Streams' data

In addition to the ongoing HL7 message feed, Streams was initially loaded with five years' of patient history in late 2015. This was by way of transfer of historic HL7 messages and HES data. This means the records include any patient who was treated at the Royal Free from approximately 2010 onwards.

This historical information is primarily needed to provide contextual clinical information to allow the Royal Free's clinicians to properly diagnose and treat patients. We consider the proportionality of transferring this information further in paragraph 27.

10.7 Use of NHS numbers as patient identifiers

We asked the Royal Free if it would be possible to remove patient names from Streams and instead simply refer to patients using their NHS number. The Royal Free considered this to be impractical and clinically dangerous. In particular:

- not all patients will have an NHS number recorded on the Royal Free's systems. For example, tourists who require treatment at the Royal Free will not have an NHS number. Even those who do have NHS numbers may not know that number and it may be difficult to find out what that number should be; and
- having the patient's name is a very useful way to refer to the patient and confirm their identity, both when dealing directly with the patient and when discussion the patient with other clinicians. For example, if a clinician needed to speak to a patient and wanted to confirm they are speaking to the right person it would be strange to start that conversion "*Can I just check you are the patient with NHS number 6024515707?*". In other words, only having the NHS number available to identify the patient is likely to significantly increase the risk of misidentification for that patient.

10.8 Retention of records

The Royal Free has not specified a maximum retention period for patient information on Streams. In other words, there is no process to delete patient information once it reaches a certain date and the information is, at this time, stored indefinitely.

This also means that the size of the Streams database is increasing gradually over time. Around 17,000 new patient records are added to Streams each month.

We consider if this lack of a retention period is compatible with the Data Protection Act 1998 in paragraph 27.

10.9 Volume of records

Streams contains records for 1,632,142[12] patients of the Royal Free. As set out above, those records are created from a stream of HL7 messages and associated HES data.

Streams contains a total of 173,398,017 HL7 messages, meaning that the average record is created by slightly over 100 HL7 messages.

10.10 Data location

The Streams infrastructure is contained in a primary datacentre located in England. We were informed by DeepMind that the datacentre is owned by a third party and DeepMind uses it under a co-location arrangement. We were informed that the third party simply provides space in its datacentres and associated facilities (such as power and connectivity), but not the servers. We did not review the co-location contract. All of the computer servers used for Streams are owned and controlled by DeepMind.

DeepMind is in the process of bringing a secondary datacentre on line. That datacentre is also located in England, owned by a different third party and provided to DeepMind under a separate co-location arrangement. Once the secondary datacentre is online, in the event of failure of the primary datacentre, it would be possible to failover to the secondary datacentre within 24-36 hours of a failure of the primary datacentre.

We were informed by DeepMind that it currently uses mirror servers within the same primary datacentre. This would provide some protection if the primary servers failed. The secondary datacentre also contains a database that mirrors the data from the primary datacentre but does not contain the other infrastructure necessary to deliver Streams. This means that a catastrophic loss of the entire primary datacentre would disrupt the Streams service. This risk is tempered by the strong security controls around the primary datacentre (see paragraph 10.12). In addition, this would not compromise the personal data on Streams *per se* as all of that personal data is also stored at the secondary datacentre and on the Royal Free's own systems.

However, we recommend that the Royal Free encourage DeepMind to bring the secondary datacentre fully online as soon as reasonably practicable.

10.11 Sub-contractors

Three sub-contractors are or were used by DeepMind to deliver Streams. Two sub-contractors provide the datacentres (see above) and the third is a digital design studio that helped to create the Streams App. None of the sub-contractors process any confidential

[12] Record count at 8 February 2018.

patient information and so we have not reviewed the agreements with these third parties and do not comment further on these arrangements in this Report.

10.12 Information security

As set out in paragraph 8.4, this Report does not address technical security issues and so we have not reviewed the technical security of the Streams infrastructure.

However, we note that data on Streams is encrypted at rest and in motion. In addition, DeepMind's Independent Reviewers commissioned First Base to carry out a technical security review of the primary datacentre last year. This included:

- a technical security review on the primary datacentre and development process dated 12 May 2017.[13] Please note that this does not cover the secondary datacentre as it was not in place at that time. However, we were informed by DeepMind that the secondary datacentre is at least as well protected as the primary datacentre; and
- a datacentre server build review report dated 19 June 2017.[14] This also does not cover the secondary datacentre but we were informed by DeepMind that it will use the same datacentre server build.

Those reports described the datacentre as providing excellent security. In relation to the datacentre server build, it found one medium risk vulnerability.

DeepMind has made the following comment in relation to that vulnerability: "*There was a single medium level issue identified "World-Writeable Files", whereby it is claimed that some files on some of the servers could be modified by "all users on the network". However, this can only happen where a user is logged into the server, and these logins are very tightly controlled, so no material risk exists in this area at present. It is however best practice to minimise the number of world writeable files, so we will do this*".[15]

We discussed this with DeepMind's head of security, who also confirmed that DeepMind users did have access rights over the Streams servers. However, this is necessary for them to look after and maintain Streams, only a very limited number of users have this access (see paragraph 17.5) and their access is logged. We believe that DeepMind has addressed its mind to the issue. However, as this Report does not address technical security, we cannot comment on DeepMind's conclusions and do not comment further on this issue.

11 The Streams App

11.1 Overview of the Streams App

The Streams App is a mobile phone application that works on Apple iPhones only. The Streams user guide is publicly available[16] and contains a comprehensive overview of the operation of the App, including screenshots of the App. Accordingly, we only summarise some of the key features below.

[13] https://storage.googleapis.com/dmhir-documents/First Base Datacentre and Development review.pdf

[14] https://storage.googleapis.com/dmhir-documents/New First Base Datacente Server Build Review.pdf

[15] See Independent Reviewers: DeepMind Health Response, https://deepmind.com/documents/86/Independent%20Reviewers%20Annual%20Report%202017%20-%20DMH%20Response.pdf

[16] See https://support.deepmindhealth.com/#/how-to-use-streams?trust=RAL

11.2 AKI alerts

The Streams App serves two important functions. The first is to provide AKI alerts. When a new HL7 message is received:

- Streams processes the HL7 messages to convert it into a different format that can then be added to the Streams database;
- Streams analyses the HL7 message using the NHS AKI algorithm (see paragraph 12.1) to determine if an AKI alert is triggered; and
- if an AKI alert is necessary, a notification will be sent to the relevant clinician via their Streams-enabled iPhone. This is a real time alert and a significant improvement on the previous process which relied on clinicians logging into the Royal Free's system to obtain the patient's results. This is supported by a limited workflow process that allows the clinician to dismiss the alert, ask that someone sees the patient and/or see the patient themselves and record that fact on Streams.

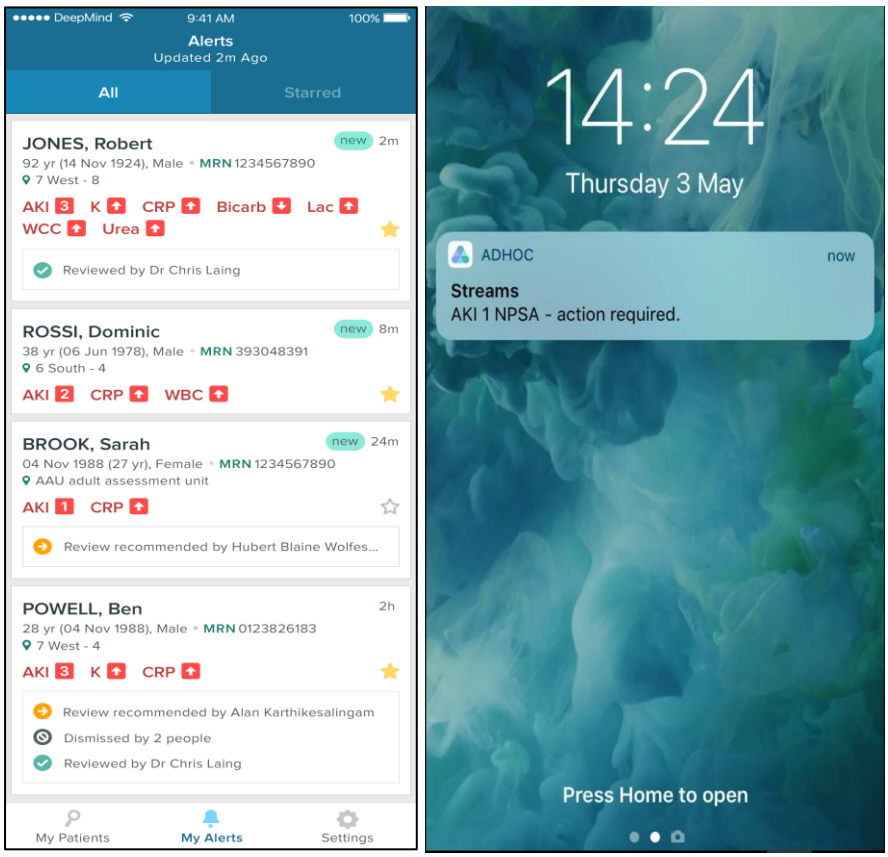
The alerts are available either as notifications on the iPhone or via the alerts screen. The notifications do not contain any personal data (see screenshot below).

We were informed that the Royal Free conducts around 2,000 blood tests every day. Those blood tests generate around 150 potential alerts. The potential alerts are then filtered to, for example, remove patients who have already caused an alert or who are on dialysis (see paragraph 10.5). This leaves approximately 25 alerts a day for the renal specialists to triage, which in turn is likely to require 5 to 10 interventions.

This means the Streams App allows the clinicians to detect, triage and if necessary intervene in acute kidney injury situations across the whole of the Royal Free hospital.

Screenshot showing AKI alerts (taken from the Streams user guide) and an AKI notification.

Please note the AKI alert page uses synthetic data.



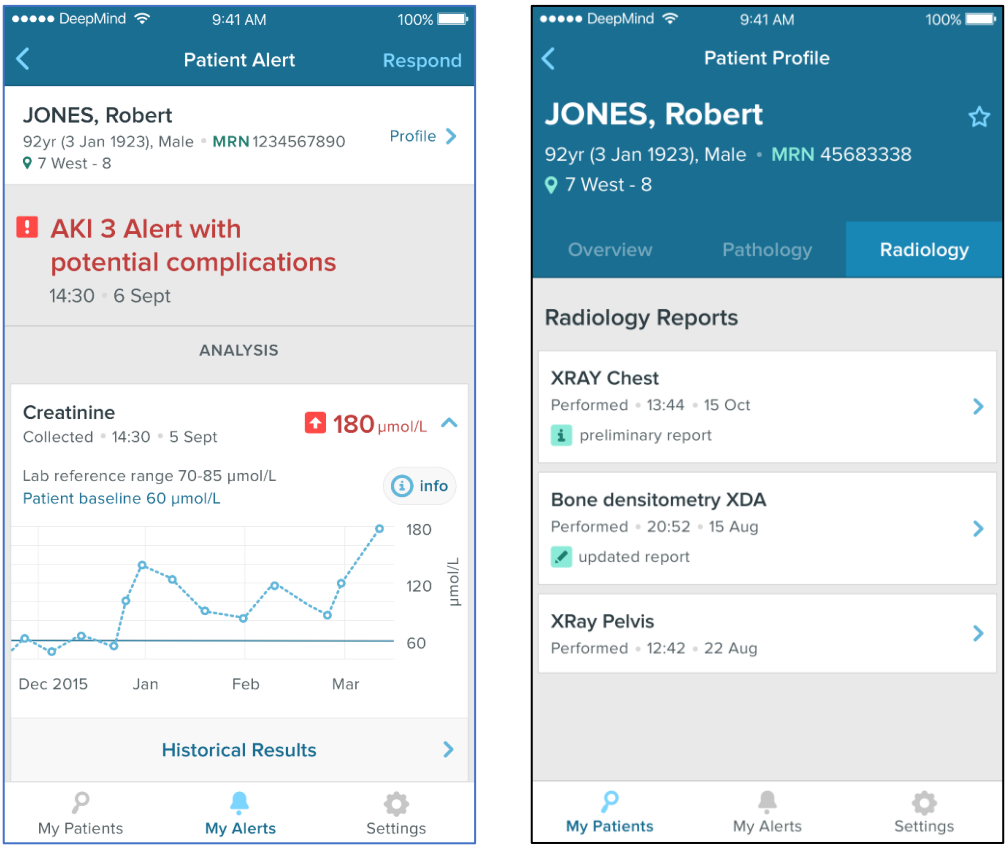
11.3 Contextual clinical information

The second important function is to provide contextual clinical information. Where the patient has an AKI alert, it is possible to see a screen summarising the AKI alert together with relevant test results, including historical test information (see screenshot below). This provides the clinician with the information needed to diagnose and treat the patient in an easily accessible manner.

This is supported by contextual clinical information for that patient. That information currently extends back for the last eight years (see paragraph 27 for a discussion about this retention period). This information is needed for a number of purposes:

- the medical history is needed for the prioritisation and effectiveness of care. For example, if the patient has had a nephrectomy (removal of a kidney) or diabetes, they are more likely to be a priority;
- while only blood tests for the last 12 months are used in the NHS AKI algorithm, older blood tests are relevant, for example to see if the patient has previously had AKI. Similarly, other conditions, such as kidney stones or hyperkalemia (elevated potassium levels) will help the management of the patient; and
- AKI can occur as a result of a procedure or operation, such as a fractured hip, so this information is also needed when treating the patient.

The Streams App also allows clinicians to search for patients based on a range of different criteria such as the patient's name, the ward the patient is on or the patient's consultant. Alternatively, the patient's details can be found by scanning the patient's barcode. It is possible to see a patient's profile and test reports, even if there is no AKI alert for that patient.



A detailed screenshot with creatinine levels and further contextual clinical information (taken from the Streams user guide). Further screenshots are available from the Streams user guide. Please note this uses synthetic data.

11.4 The Apple iPhones

The Royal Free uses eight Apple iPhone 6s. These are all owned by the Royal Free. The Streams App is not available on personal or BYOD[17] Apple iPhones.

The Apple iPhones are part of a pool and are shared between clinicians. For example, the acute care team uses two iPhones, one for the day shift and one for the night shift. This allows the iPhone that is not in use to be placed in a locked cupboard and recharged ready for the shift change. In contrast, the consultants will be issued with an iPhone while they are on duty and on call and will have the iPhone with them during the whole of that period (including whilst at home on call). There doesn't appear to be a formal process for this handover, for example a written log of who the iPhone is assigned to at any point in time. We do not think this is a material concern given there are only eight Streams-enabled iPhones. However, we recommend that if the pool of iPhones expands, a formal handover process is instituted to keep track of the individual to whom the iPhone is issued

The Apple iPhones all run iOS 9 or later. The iPhone we inspected was running iOS 11.[18] This means:

- the iPhones default to a 6-digit PIN code. However, because the iPhones are part of a pool, that PIN is shared between all of the clinicians using that iPhone. Whilst the sharing of PINs in this way would normally be bad practice, we are not concerned

[17] Bring Your Own Device – a personal phone used for work purposes.

[18] Please note we did not look at any confidential patient information on the Streams App. See paragraph 8.3.

about it because of the additional requirement to log into the Streams App (see paragraph 11.5); and

- the data on those phones is encrypted. After 10 failed attempts to access the iPhone, it will automatically erase itself. In other words, the information on the iPhone is inaccessible without the PIN code.

All of the Apple iPhones are also protected using the AirWatch mobile device management software. The AirWatch software allows the Royal Free to remotely wipe the Apple iPhones.

The Royal Free demonstrated the AirWatch software to us and confirmed that it had been used to remotely wipe iPhones in the past (though did not actually remotely wipe an iPhone for us as part of the demonstration).

11.5 Security controls in the Streams App

The Streams App is subject to the following security controls:

- when the clinician opens the App, they must enter their username and password. This is the same username and password used to access the Royal Free's systems. DeepMind does not hold this information, but instead verifies it with the Royal Free using the LDAP server. This means that once a clinician ceases to have access rights to the Royal Free's systems, they will also be prevented from accessing the App. We were informed by the Royal Free that removal from LDAP is part of their standard leaver process (but see paragraph 16.5);
- the App will automatically time out after a couple of minutes[19] and will time out if the user switches to a different App. If the user wants to reopen Streams, they will need to enter their username and password again. Both the nurse and consultant we spoke to felt the timeout period was too short and were constantly having to re-enter their username and password; and
- the Streams App obtains the clinician's location from the iPhone. This could be used to geofence the App and so permit access while the clinician is within the hospital. However, we understand this functionality is disabled. In particular, the consultant we spoke to uses the Streams App when she is on call. It means that if she is called by one of the junior doctors, she can immediately see relevant information about the patient which will help her to make the correct clinical decision.

The combination of the access controls to the iPhone itself (particularly the use of a PIN code, encryption and the use of AirWatch) together with the access controls to the Streams App (such as the need to log into Streams using their normal username and password and the timeout on the App) provides a significant degree of protection to the information accessible via the Streams App.

11.6 Logging of use of the Streams App

The use of the Streams App is logged. The Royal Free's data protection officer stated that these logs were not systematically reviewed. However, they would be looked at in relation to a specific complaint or concern, for example if there were an allegation a clinician had accessed confidential patient information inappropriately.

[19] Please note we did not establish the exact timeout period.

This is consistent with the approach to the logging of access to other systems at the Royal Free. We were informed by the data protection officer that over 4 million events are logged each day, making systematic manual review impossible.

However, we were informed that the Royal Free has purchased an intrusion detection system[20] called DarkTrace and the system should go live at the end of July 2018. It has also acquired ARCsight to automatically scan access logs and that this system should also go live in July 2018. We encourage the Royal Free to bring these systems online as soon as reasonably practicable. However, this issue does not specifically relate to Streams and so is outside the scope of our Report.

11.7 Medical device approval

The Streams App is registered as a Class 1 non-measuring, non-sterile medical device. A conformity assessment for the Streams App was most recently completed for version 1.4 on 9 October 2017. However, as set out in the Scope, this review does not consider medical device regulation and so we do not consider this issue further in this Report.

11.8 Information security

As set out in paragraph 8.4, this Report does not address technical security issues and so we have not reviewed the technical security of the Streams App.

However, we note that the Independent Reviewers commissioned First Base to carry out a technical security review. This included a technical security review of:

- the mobile iOS application dated 19 June 2017.[21] The report states the overall security of the Streams App is "excellent" with no critical, high or medium level vulnerabilities. There were two low level vulnerabilities identified; and
- the web API penetration dated 19 June 2017.[22] The report states that there were no critical, high or medium level vulnerabilities. There were 8 low level vulnerabilities.

We discussed the vulnerabilities with DeepMind's head of security. He stated that some of the vulnerabilities identified are not relevant[23], some had been fixed[24] and others are under review, but do not present a real security risk.[25] This risk assessment matches that of First Base. However, this Report does not address technical security issues, so we have not carried out a comprehensive review of DeepMind's response to each of the 10 low level vulnerabilities and do not comment on this issue further.

---

[20] The Royal Free has multiple other layers of security including the use of firewalls and virus detection systems. However, the Royal Free's general information technology security is outside the scope of this report.

[21] https://storage.googleapis.com/dmhir-documents/New First Base Mobile iOS App pen test report.pdf

[22] https://storage.googleapis.com/dmhir-documents/New First Base Web API Pen test report.pdf

[23] For example, some vulnerabilities identified relate to the manipulation of URLs, such as "*L3. API Key in URL*" in the Web API Penetration Report. However, Streams is accessed via an App, not a browser, so this vulnerability is not relevant.

[24] For example, steps had been introduced to prevent a brute force attack as identified in L5 in the Web API Penetration Report.

[25] For example, Streams caches usernames in the Streams App; see L1 of the Mobile iOS Application Penetration Report. We understand this is difficult to design around. However, exploiting this attack would: (i) require access to an unlocked iPhone, which is relatively unlikely given they are all subject to PIN controls and Airwatch management (see paragraph 11.4); and (ii) still require the attacker to guess the clinician's password.

12 Streams does not use artificial intelligence

12.1 NHS AKI algorithm

The core of Streams is the standardised national AKI algorithm, the use of which has been made mandatory by NHS England.

The NHS AKI algorithm was derived from a meeting organised by the Association for Clinical Biochemistry in June 2013 attended by clinical biochemists, nephrologists and providers of laboratory software systems[26] and is publicly available.[27] It was not developed by DeepMind.

The NHS AKI algorithm itself consists of a simple and deterministic decision tree based on a limited number of input variables relating to the patient's creatinine results, and age. It would be trivial for anyone with even basic programming skills to implement the NHS AKI algorithm.

Without intending any disrespect to DeepMind, we do not think the concepts underpinning Streams are particularly ground-breaking. It does not, by any measure, involve artificial intelligence or machine learning or other advanced technology. The benefits of the Streams App instead come from a very well-designed and user-friendly interface, backed up by solid infrastructure and data management that provides AKI alerts and contextual clinical information in a reliable, timely and secure manner.

12.2 Earlier ethics application

We understand that there are a number of limitations to the NHS AKI algorithm, for example, it has a tendency to generate false positives for patients with chronic (as opposed to acute) kidney disease and is also insensitive as to whether the patient has been admitted to hospital for two hours or two weeks.

Accordingly, DeepMind made an ethics application[28] in 2015 to the NHS Health Research Authority, for a potential research project at the Royal Free using depersonalised patient data to use AI to develop better algorithms. However, DeepMind and the Royal Free have not progressed this project. Streams just uses the NHS AKI algorithm. Accordingly, we do not consider this research project further in this Report.

13 Current development projects

The Scope of this Report includes any further development, functional testing or clinical testing that is either planned or in progress. Three Royal Free projects that are potentially relevant are addressed below.

We understand there is a fourth project that DeepMind considers is commercially sensitive because of the new features within that project still being designed and developed by DeepMind. We have therefore omitted details of that project from this Report and provided details to the Information Commissioner separately. In any event, that project is only at a very early design stage, and is on hold pending the outcome of this Report, so has limited relevance to patients' privacy or confidentiality at this time.

---

[26] See *Standardising the early indentification [sic] of Acute Kidney Injury 9 June 2014 (updated 30 January 2015)*, https://www.england.nhs.uk/wp-content/uploads/2014/06/psa-aki-alg-faqs.pdf

[27] https://www.england.nhs.uk/wp-content/uploads/2014/06/psa-aki-alg.pdf

[28] https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/research-summaries/using-machine-learning-to-improve-prediction-of-aki-deterioration/

These projects are unlikely to proceed until after the General Data Protection Regulation applies. This means they will need to be subject to a privacy impact assessment (with the exception of the extension to Barnet Hospital, for which a privacy impact assessment has already been carried out). Those privacy impact assessments should be completed well in advance of testing for clinical safety and effectiveness, the point at which the actual processing of personal data will take place.

13.1 Extension to Barnet Hospital

The Royal Free wants to roll out the Streams application to the Royal Free's Barnet Hospital. This would not involve any changes to the functionality of Streams. Instead, it just involves providing Streams-enabled iPhones to the clinicians at the Barnet Hospital.

However, it does require checks to confirm Wi-Fi availability at the Barnet Hospital and to confirm that the Streams App can access the Streams infrastructure via that Wi-Fi (e.g. to confirm access would not be blocked by any firewall).

A privacy impact assessment for this extension was completed on 1 September 2017. The extension was intended to go live on 1 November 2017. However, we were informed by the Royal Free that it has put this project on hold as a result of the Information Commissioner's investigation and that it will not proceed until the completion of this Report and the issues raised in the Undertakings are resolved.

13.2 Electronic observations

This project would allow clinicians to directly input observations about patients into Streams, which would then be fed back into the Royal Free's own systems. Currently, many observations are recorded on a paper file kept by the patient's bedside. We understand that the Royal Free and DeepMind ran a workshop allowing clinicians to try out a prototype App to record this information.

However, this project has not progressed beyond an early design stage. It is also on hold pending the outcome of this Report.

13.3 Alerts for other conditions

This project will involve adding additional alerting functionality to the Streams application to allow it to create alerts for conditions other than AKI; for example, sepsis or hypo- or hyperglycaemia. This project will require changes to the Streams application.

We were informed by the Royal Free that this project is at a very early design stage. It is on hold pending the outcome of this Report.

14 Development process

14.1 Timeline

This Report is limited to an assessment of the current live clinical use of Streams, and any further development, functional testing or clinical testing, that is either planned or in progress. It is not a historical review of the development of Streams. No such development or testing is imminent, so these issues are not strictly within the scope of this Report.

However, the development of Streams does provide context for this Report and hence an outline of the key events in the development of Streams is set out in Annex 2. We also include an overview of the various development stages to clarify the legal framework as and when development and testing resumes.

14.2 Product design

The design phase involves identifying features and functions and the design for the technical infrastructure. The clinicians at the Royal Free are likely to provide input into the design phase.

The design phase uses synthetic data (see paragraph 14.7). As this does not contain personal data, we do not consider the design phase further in this Report.

14.3 Product development

The development phase involves writing code, and procuring hardware, to implement the design.

The development phase uses synthetic data (see paragraph 14.7). As this does not contain personal data, we do not consider the development phase further in this Report.

14.4 Testing – Obligations to test

Testing involves checking that the components of Streams, including hardware components, work together.

Testing is an essential part of any systems deployment, particularly for a tool intended for clinical use where it is critical that the system is reliable and provides timely access to accurate information.

This is reflected in the clinical systems standards issued by NHS England under section 250 of the Health and Social Care Act 2012. The Royal Free is under a statutory obligation to "*have regard to those standards*" (section 250(6)).

The standard SCCI0160: *Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems*[29] requires the Royal Free to assess any third-party product used in a Health IT System as part of the clinical risk management process. The risk analysis of that project should also include appropriate testing as part of clinical risk control.[30] The standard SCCI0129: *Clinical Risk Management: its Application in the Manufacture of Health IT Systems* imposes similar testing requirements. Not only do these standards require testing, they specifically flag the hazards of inaccurate, incomplete or absent data and encourage testing specifically on these points.[31]

Our opinion is that it would be negligent for the Royal Free to deploy a bespoke system, such as Streams, in a clinical environment without having carried out appropriate testing. This could lead to significant liability and could also be a breach of the Data Protection Act 1998.[32]

---

[29] http://content.digital.nhs.uk/isce/publication/SCCI0160 This was published in May 2016. At the time the testing of Streams took place, the standard would instead have been ISB160.

[30] See *Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance*, http://content.digital.nhs.uk/media/20986/0160382012imp-guide/pdf/0160382012imp-guide.pdf

[31] By way of example, the *Clinical Risk Management: Middleware Implementation Guidance* created under SCCI0160 identifies incorrect, absent or invalid data as a potential hazard affecting middleware such as some of the components of Streams (A.2) and requires appropriate mitigations such as testing to "ensure that the messages and transport comply with requirements".

[32] For example, if the lack of testing resulted in Streams presenting inaccurate data (data protection principle 4).

14.5 Testing – Synthetic data

We were informed that the majority of the testing would use synthetic data (see paragraph 14.7). As this does not contain personal data, it falls outside the scope of this Report.

14.6 Testing – Confidential patient information

Final testing to assure clinical safety and effectiveness must be conducted using confidential patient information (reflecting the guidance set out above). This testing may involve the clinicians in the Royal Free using the Streams system side-by-side with its existing systems. This is not just to confirm that Streams works technically, but also that the information it provides is accurate and to confirm that the right clinical processes are in place for clinicians to operate in conjunction with Streams (for example, to confirm the Royal Free's processes to triage alerts are fit for purpose).

This is likely to require a full set of confidential patient information. This is partly to load test the system and ensure that it can handle real data volumes. However, more importantly, side-by-side testing will only work if Streams is loaded with a full data set so that if a patient is admitted to the Royal Free the clinician can view their information on Streams and compare it with the pre-existing system. This will only be possible if that patient's confidential patient information is already in Stream given the difficulties in implementing an alternative query-based system to fetch that information as and when required (see paragraph 26.1).

Both the Royal Free and DeepMind were adamant in discussions with us that testing with real data is necessary before deploying a clinical system to assure the correct functioning of the system. Deploying a system without that testing could endanger patient safety.

This is a particular issue, as DeepMind's synthetic data was created independently from the Royal Free. For example, Streams is dependent on the accurate ingestion and processing of HL7 messages. It is possible that the format used by the Royal Free for those HL7 messages does not exactly match that in the synthetic data or that the free text fields within the HL7 messages might not be accurately parsed by Streams (for example, if they contain delimiter characters that corrupt the structure of the message). Similarly, we understand there are examples in real data of name datafields (e.g. "John" or "Mary") extending to over 60 characters because of the way that information has been recorded. It is important that the Streams App is able to handle these peculiarities.

We were informed by the Royal Free and DeepMind that the original clinical testing using real data detected a number of defects in the end-to-end Streams solution which were not detected by testing using synthetic data. These include:

- incorrect data in the Royal Free's systems. For example, the HL7 message corresponding to a lab report did not always contain the right time for the test and instead were just coded with a default value, e.g. 00:00am. This might be due to systems failure or human error. However, Streams needs to be able to detect potentially anomalous data and alert clinicians to the risk; and
- missing patients. Apparently, some patients disappeared from the Royal Free's dataset. This had to be addressed as part of the testing process.

14.7 Synthetic data

We were told by DeepMind that its synthetic dataset was created prior to receiving any confidential patient information from the Royal Free. That synthetic data was created by

inserting randomised information into HL7 message formats. DeepMind informed us that the synthetic data does not contain real patient information.

We reviewed the synthetic data for one patient (see paragraph 10.2). Analysis of the HL7 messages show they relate to “Mr” Melanie Brown who is female, lives in “Hardy, Ingram” and is 110 years old. The HL7 messages appear to suggest a range of improbable events from heart surgery to stubbed toes. We were informed by DeepMind that the text of the observation results in the HL7 messages was in fact nonsense from a medical perspective and is just there to check the text shows correctly within the Streams App (and includes a range of different special characters to check they are displayed correctly and are not misinterpreted as delimiters).

15 The Royal Free’s wider information technology estate

15.1 Cerner

The Royal Free’s main information technology supplier is Cerner, an American supplier of health information technology solutions. Cerner is deployed in over 20 other NHS Trusts.

The Royal Free hospital currently uses Cerner for its Patient Administration System. That Cerner instance is remotely hosted in Cerner’s own datacentre. The Barnet Hospital uses a locally hosted instance of Cerner to host its electronic patient records.

The Royal Free is currently looking to move to a new Cerner instance to cover all three hospitals. That instance will be hosted by Cerner and is intended to allow the Royal Free to become “fully digital”. The Royal Free is in the process of testing this new Cerner instance and that testing will eventually include the use of live data.

15.2 Other suppliers

The Royal Free has a number of other third-party suppliers. For example, it uses CareStreams software to store radiology images on its own servers.

It also uses pathology services provided by HSL, a partnership between The Royal Free, The Doctors Laboratory and UCLH NHS Foundation Trust. HSL hosts this pathology information.

15.3 Information on Streams is also available on the Royal Free’s other systems

The information on Streams is a subset of the information available on the Royal Free’s other information technology systems. While Streams alerts clinicians to potential AKI and provides clinicians with a faster and more convenient means to access information about patients, the clinicians could obtain the same information by logging into those various other systems (albeit this would be time-consuming and inconvenient).

Part B: Governance & accountability

16 The Royal Free

16.1 Governance

The Royal Free has an Information Governance Group that meets quarterly.[33] The Group comprises a range of people including the data protection officer, SIRO, Caldicott Guardian and IG manager. The Group addresses a range of data protection and freedom of information issues.

16.2 Leadership and tone from the top

We talked to the senior leadership team at the Royal Free, including the group chief executive Sir David Sloman. They confirmed that respecting patient confidentiality was fundamental to the operation of the hospital. They confirmed they had completed their information governance training in accordance with the annual training cycle. They described a number of steps the Royal Free has taken recently to improve information governance including making a major investment in the hospital's cyber security defences and inviting two lay members to take part in the Information Governance Group.

We also talked to the Royal Free's Caldicott Guardian. He was appointed as Caldicott Guardian for the Chase Farm hospital in 2012 and recently became Caldicott Guardian for the whole of the Royal Free. He emphasised the need to allow innovation in the delivery of patient care whilst ensuring it is done in a lawful and appropriate way, and there is proper transparency with patients. The Caldicott Guardian has an MA in law and ethics and is supported by both the data protection officer and through the London Caldicott forum.

16.3 Data protection officer

The Royal Free's data protection officer has been at the Royal Free for six years and was previously the chief technology officer for the National Patient Safety Agency.

In addition to acting as data protection officer, the data protection officer is deputy chief information officer and is responsible for infrastructure and cyber security within the Trust.

We were informed that the data protection officer will act as statutory data protection office under the General Data Protection Regulation. We were concerned that his role as deputy chief information officer would conflict with his role as statutory data protection officer.[34] However, this Report does not address the Royal Free's wider data protection compliance, so we do not consider this point further in this Report.

16.4 Information governance manager

The Royal Free's IG manager reports to the Royal Free's data protection officer. The IG manager is responsible for a range of data protection, freedom of information and general information governance matters. This includes advising on these issues and responding to subject access requests. The IG manager handles opt-outs from Streams and subject access requests made specifically for information on Streams (see paragraph 28).

The IG manager has been at the Royal Free for 9 years, initially as an IG officer and for the last four years as IG manager. The IG manager is PDP-certified.

[33] We note that it met four times in 2016 but only three times in 2017 (the meeting in September 2017 was cancelled).

[34] See Article 38(6) and para 3.5 of the Article 29 Working Party's Guidelines on Data Protection Officers (WP 243).

16.5 Personnel with use of the Streams App

Access to the Streams App is controlled using the Royal Free's LDAP. There are 68 users whose LDAP profile provides them with access to the Streams App. We were informed they were made up of: (i) renal specialists; (ii) the acute care team; and (iii) a renal transplant surgeon.

We selected five of those 68 users at random and in relation to each of those users asked for details of the following:

- *Details of their role and title* – All five are specialists in renal medicine;
- *Confirmation that they are employed by the Royal Free* – Four of the five are employees. The fifth is a senior consultant working with the Royal Free as an honorary consultant;
- *Confirmation and details of their contractual duties of confidence* – We reviewed the template contracts that would be used for the five users (not the actual employment contracts). The template contracts all contain suitable confidentiality and data protection obligations and remind users that breach of these obligations will be regarded as misconduct resulting in disciplinary action; and
- *Details of their training record in relation to data protection and information governance issues* – The four employees had completed information governance training in 2017, 2016, 2014 and 2013 respectively. Some of the employees therefore last took this training some years ago. The Royal Free did not have any record of the senior consultant having taken any information governance training. However, he may have taken that training at one of the other NHS Trusts he works for and is a very senior member of staff. While these matters are of general application, rather than being limited to Streams, we recommend that the Royal Free requires employees to refresh their information governance training at least annually[35] and considers if there are any training needs for those working in an honorary consultant role.

We were subsequently informed during interviews that there were only around 35 users of Streams, which is clearly smaller than the 68 users with access on LDAP. We therefore started to check the whole list. Our initial investigation revealed that 2 individuals from the acute care team, and 10 registrars, are still on the LDAP list despite the fact they are no longer employed by the Royal Free. In the case of the registrars, this likely to be because they have rotated to different hospitals. The practical risk this poses is limited as it is only possible to access Streams from a Streams-enabled iPhone.[36] In addition, the Royal Free confirmed it has now reviewed the list and removed clinicians that no longer have a need to access Streams. However, we recommend that the Royal Free re-review its leaver and mover process to ensure the LDAP list is automatically updated when clinicians leave the Royal Free or move to another department where access to Streams is no longer required. The Royal Free should review the access list regularly to ensure this process is working.

The Royal Free confirmed to us that there had been no disciplinary issues arising out of the use of Streams.

[35] We were informed by the Royal Free that it recently conducted an exercise to encourage staff to complete this training. As a result, 95% of staff have now completed their information governance training within the annual cycle.

[36] Whether those individuals have access to any of the Royal Free's other systems is outside the scope of this Report.

16.6 Policies and training

The Royal Free has a patient and staff confidentiality policy. The policy provides a detailed overview of the data protection and confidentiality obligations placed on the Royal Free and the steps staff must take help satisfy those obligations.

In addition, all of the users of Streams are health professionals, either registered medical practitioners or registered nurses, so are all also subject to professional obligations of confidentiality.

All staff at the Royal Free are supposed to undergo mandatory annual information governance training, provided by eLearning. However, as noted in paragraph 16.5 above, it appears that clinicians have not always kept their training up to date. The Royal Free should ensure its staff complete mandatory annual information governance training and this should be tracked through the use of appropriate targets. The Royal Free should follow up on any instances of non-compliance.

The NHS Information Governance Toolkit is a system which allows organisations to assess their Information Governance policies and standards. The Royal Free has targeted level 2 or 3 (the highest level). KPMG assessed the Royal Free's compliance with the IG Toolkit at the start of March 2018 and found it provided "significant assurance with minor improvement opportunities". In particular, KPMG recommended that staff training levels are improved and that the Royal Free needed to provide better evidence of its governance of access controls.

16.7 Privacy impact assessment

The Royal Free conducted a privacy impact assessment for Streams in January 2016. This was after confidential patient information was transferred to DeepMind. The privacy impact assessment was also relatively thin given the scale of the project.

A further privacy impact assessment addressing the extension of Streams to the Barnet Hospital (see paragraph 13.1) was completed on 1 September 2017 in accordance with the Undertakings.

While there is no legal obligation under the Data Protection Act 1998 to conduct a privacy impact assessment,[37] we agree with the Information Commissioner that the initial privacy impact assessment should have been completed in a more timely manner. However, this Report does not include a historical review of Streams, so we do not comment further on that privacy impact assessment.

16.8 Operational use of Streams

We interviewed three users of the Streams application: two consultant nephrologists and a consultant nurse[38] in the acute care team. They thought the Streams App was extremely useful. They were impressed by the user-friendly interface and its reliability and accuracy. They did not have any concerns about the security of the App. Some of the benefits of Streams include:

- *Time saving* – The Streams App makes contextual clinical information available immediately. All of that information is already present on the Royal Free's systems,

[37] In contrast with the General Data Protection Regulation which would likely have required a privacy impact assessment for this processing.

[38] Note that the consultant nurse had been involved in the initial design of the Streams App and had appeared publicly to support the use of the App.

but is spread across multiple different systems. Streams saves the clinicians from having to extract the data from all those systems. The consultant nurse suggested it can save over an hour a day;

- *Workflow* – The Streams App allows a form of simple workflow. When an alert is triggered, the clinician is presented with different options, such as to dismiss the alert or ask that another clinician see the patient. The clinicians can also add notes to that patient's record within Streams so that all the clinicians within the team can update each other on that patient's condition;
- *Patient engagement* – Because the information on the Streams App is presented graphically, see paragraph 11.1, it allows a much better engagement with the patient who can see their own results vary over time. This is important for AKI, which, in some cases, can be quickly resolved by patients increasing their fluid intake;
- *On call* – The consultants use the Streams App when on call, including when at home. This allows them to deal much more efficiently with issues that arise when they are not in the hospital as they have the relevant information available to them; and
- *Treatment of other conditions* – The Streams App is also useful when dealing with other conditions such as a sepsis. While the App is not currently set up to create sepsis alerts, the contextual clinical information on Streams and the AKI alerts are a useful way to also identify these conditions.

The clinicians had carried out information governance training and considered the Royal Free to have a culture that respected patient confidentiality. They had been trained to use the Streams App; however, as the user interface is so intuitive, it is very easy to pick up its use. As health professionals, they were also well aware of their own professional responsibility to maintain patient confidentiality.

17 DeepMind

17.1 Governance

The information governance arrangements at DeepMind are set out in its Information Governance Management Framework, which was most recently updated on 1 January 2018.

DeepMind has Information Governance Board which meets once a month. The board includes DeepMind's IG Lead, Caldicott Guardian, Senior Information Risk Officer and Information Security Officer. The Information Governance Board has a broad remit consistent with its obligations.

17.2 Leadership and tone from the top

We talked to the senior leadership team at DeepMind, including Mustafa Suleyman, co-founder and Head of Applied AI. They demonstrated a strong commitment to proper information governance at DeepMind. They confirmed they had completed their information governance training in accordance with the annual training cycle.

Their commitment to good information governance manifests itself in a number of different ways including supporting and empowering DeepMind's IG Lead, appointing the Independent Reviewers (see below) and personally taking action if they detect any failure to comply with DeepMind's strict information governance standards.

17.3 Independent Reviewers

DeepMind has appointed a number of public figures to act as Independent Reviewers. The Chair is Dr Julian Huppert and a list of the other Independent Reviewers is available from DeepMind's website.[39] The Independent Reviewers meet four times a year to scrutinise DeepMind's work with the NHS.

The Independent Reviewers appointed First Base to carry out a security review of Streams (see paragraphs 10.12 and 11.8). They also reviewed Streams for their first annual report.[40] It contains a detailed and considered assessment of a number of issues affecting Streams. The report did not include an assessment of the legal grounds for the use of confidential patient information under data protection law or the laws of confidence. However, this is because these are matters for the Royal Free as data controller.

We had originally planned to share a draft of the Report with the Independent Reviewers as part of the audit process and discuss our findings with them. However, it was felt this would be inappropriate given the Independent Reviewers' role. DeepMind will instead provide the Independent Reviewers with a final copy of the report.

17.4 IG Lead

The current IG Lead has been at DeepMind for six months. She spent the previous 17 years in various information governance roles in the NHS. In the 9 years before joining DeepMind, she was Head of Information Governance at two different hospitals.

During her interview she informed us that she considered DeepMind to have a strong information governance culture and staff at DeepMind had a clear understanding of the confidential nature of the information they handled. This was supported by a clear emphasis from the management of DeepMind on the need for strong information security.

She felt that DeepMind already had a very good level of compliance when she arrived, with strong processes and systems in place to provide good information governance. Her work since arriving had been to ensure those high standards were maintained. She felt the processes and procedures at DeepMind were better than a number of those within the NHS and she had no material concerns about the information governance measures at DeepMind.

We understand that DeepMind has not made a final decision on who will act as its statutory data protection officer under the General Data Protection Regulation but is confident that a suitable candidate is available.

17.5 Employees with access to Streams

We reviewed the list of persons with access rights to the Streams servers ("**personnel with access to Streams**"). In summary:

- there are only eight personnel with such access to Streams with such access (as at January 2018). They are all employees of DeepMind;
- the personnel with access to Streams are split across development, testing, database administration and system administration roles;

[39] https://deepmind.com/applied/deepmind-health/transparency-independent-reviewers/independent-reviewers/

[40] https://deepmind.com/documents/85/DeepMind%20Health%20Independent%20Review%20Annual%20Report%202017.pdf

- the access rights are for varying periods of up to 6 months, depending on that person's role. We were informed by DeepMind that renewal of access must be approved by DeepMind's IG Board; and
- all access to the Streams servers is logged. Those logs are reviewed by DeepMind's IG Lead and security officer to confirm that the access is appropriate. This involves using a programme to review and randomly select parts of the access log of a member of personnel, and also scanning the personnel's laptop. The member of personnel would then be asked to explain why they had accessed that data.

There have been no disciplinary issues related to DeepMind employees' access to Streams.

17.6 Policies and training

DeepMind has a range of policies relevant to data protection and confidentiality, including a specific policy addressing Privacy & Information Security Policy (Clinical Applications). The policies we reviewed have been revised and updated on a regular basis. They covered all of the issues we consider relevant.

We reviewed the template confidentiality provisions imposed on DeepMind's personnel. We consider them to be appropriate.

DeepMind's personnel are required to undergo a range of training, including taking a quiz to confirm their understanding of data protection and confidentiality issues. We consider that training to be appropriate.

All of the DeepMind personnel we interviewed, including the senior leadership team, confirmed that they had taken the information governance training annually.

The NHS Information Governance Toolkit is a system which allows organisations to assess their Information Governance policies and standards. DeepMind has achieved level 3 (the highest level) for the whole of the NHS Information Governance Toolkit.

17.7 Remote working

The personnel with access to Streams can also ask for permission to work remotely. That request requires authorisation from the IG Board, and we understand that it is necessary to deal with situations in which employees might be working in another part of the country. However:

- it does not allow access from outside the UK;
- access is via a VPN into DeepMind's corporate network and then via a VPN to the Streams servers (i.e. it does not allow direct access to the Streams servers);
- access is only permitted on DeepMind's own laptops which are secured and encrypted; and
- all access is logged (see above).

We were concerned that remote working could increase the risk of misuse of patient information. However, the team needs to have remote access to, for example, deal with failures or breakdowns in the system outside normal working hours. On that basis, given the very small number of people with access to the Streams servers and the controls set out above, we do not think this is a material concern, but should be kept under review.

17.8 Assessment of employees

We selected two of the eight personnel with access to Streams at random for interview.

The first was a software engineer supporting the Streams infrastructure. She had worked at DeepMind for around a year and had worked at Google for the previous four years. The majority of her work is for development purposes and hence she only rarely needs access to confidential patient information. Where she does need access, she would need to raise a ticket with the IG Lead to justify her access.

The second was from the 'devops' team. He had worked for DeepMind for two years. His job was to ensure that the various parts of the Streams systems are operating. To fulfil this role, he needs to access confidential patient information; for example, if parts of the system fail, he would need access to the underlying data to understand the reason for that failure. He is pre-approved to access confidential patient information where necessary.

Both personnel:

- had undergone IG training on an annual basis and had a clear understanding of the confidential nature of the information they handle; and
- felt that the culture at DeepMind was one that respected the confidential nature of this information and did not have any material concerns about DeepMind's security and information governance practices.

18 Joint governance arrangements

18.1 Technology Project Board

The Information Processing Agreement requires the parties to participate in an "Information Governance Board" and meet on a monthly basis.

The Royal Free and DeepMind instead meet as a "Technology Project Board". The meetings are approximately monthly (there appear to be some months in which no meeting takes place). The meeting addresses a range of issues, including developments to the Streams App, information governance and other matters.

18.2 Monthly audits

The Information Governance Board is responsible for a range of matters. This includes implementing "*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*".

It appears that these monthly audits have not, in fact, taken place. It is possible that, given the Independent Reviewers' investigation, First Base review and our audit, there has been little space to schedule these additional audits. However, the Royal Free should reinstitute this audit process once this Report is complete.

Part C: The relationship between the Royal Free and DeepMind

This part considers the status of DeepMind when handling patient data.

19 Contracts with DeepMind

The relationship between the Royal Free and DeepMind is set out in three agreements.

19.1 The Services Agreement

DeepMind provides Streams to the Royal Free under the Services Agreement dated 10 November 2016. The agreement will run for five years.

The Services Agreement provides DeepMind with an intellectual property licence to use patient information. In relation to that licence:

- DeepMind is permitted to use patient information solely for the purpose of providing Streams to the Royal Free; and
- the licence allows use world-wide and permits sub-licensing. However, the broad nature of this licence is because the relevant clause provides a general licence of a range of intellectual property rights to DeepMind. However, it is subject to the additional restrictions on the use of confidential patient information set out in the Information Processing Agreement (see paragraph 19.2).

The Services Agreement also contains project governance arrangements, which are discussed in paragraph 18.

The agreement also contains a number of other provisions addressing issues such as fees, compliance with medical device regulation, insurance, warranties and limits of liability. These issues fall outside the scope of this Report.

19.2 The Information Processing Agreement

Any processing of patient information under the Services Agreement is subject to a separate Information Processing Agreement.

The Information Processing Agreement was entered into on 10 November 2016 and replaces the earlier Information Sharing Agreement, which was entered into on 29 September 2015.

The Information Processing Agreement imposes a broad range of obligations on DeepMind's use of confidential patient information. A copy of the agreement is available on DeepMind's website. It includes the following key obligations on DeepMind:

- to only use confidential patient information on the Royal Free's instructions and not to combine or link it to any other data unless instructed to do so by the Royal Free;
- not to transfer the personal data outside England without written consent from the Royal Free;
- to delete confidential patient information if instructed by the Royal Free;
- to only disclose confidential patient information to personnel and subcontractors who have a need to know, have undergone suitable training and are subject to suitable confidentiality obligations;

- not to engage any subprocessors, nor to disclose patient information to a third party without the Royal Free's consent; and
- to take a wide range of security measures including encrypting data in motion and at rest, to back up data and to notify data breaches to the Royal Free.

We consider these obligations at appropriate points in this Report. The Information Processing Agreement also contains project governance arrangements, which are discussed in paragraph 18.

The Information Processing Agreement contains a curiously formatted version of Schedule 1 describing the data transferred by the Royal Free to DeepMind. It appears to be scanned separately to the rest of the document (the scan of the rest of the document being lower quality, suggesting it was a fax copy) and is marked "*DRAFT: 27.10.16 Confidential Subject to Contract*".[41] However, we were informed this is in fact the final version of Schedule 1 and the DRAFT marking was left in by accident.

Finally, Schedule 1 also refers to the Royal Free transferring: "*(f) radiology images…; and (g) FHIR messages*...". We understand that this information is not actually transferred from the Royal Free to Streams. We suggest that the Information Processing Agreement is updated to better reflect the data actually transferred as a result.

19.3 Memorandum of Understanding

The Royal Free and DeepMind entered into a Memorandum of Understanding on 28 January 2016. The Memorandum of Understanding primarily relates to "*a proposed acute kidney injury project involving research for project development on anonymised and psueudonymised data under the National Research Ethics framework*".

However, DeepMind has informed us that they have abandoned their potential research project into the use of AI to develop better algorithms, and their processing is limited to execution of the NHS AKI algorithm (see paragraph 12). In addition, the majority of the provisions in the Memorandum of Understanding are non-binding. The limited provisions that are binding are superseded by the Services Agreement and the Information Processing Agreement discussed above, hence we think the Memorandum of Understanding has very limited relevance to Streams.

We recommend that the Royal Free considers if the Memorandum of Understanding continues to be relevant to its relationship with DeepMind and, if it is not relevant, terminates that agreement.

20 DeepMind's status under data protection law

As set out in paragraph 22, the primary source of data protection law in the UK is the Data Protection Act 1998. Those processing personal data under the Act do so as either data controller or data processor. The distinction is crucial to the data protection analysis.[42]

[41] A "subject to contract" marking is normally used to indicate a document is not intended to create a legally binding contract. The "subject to contract" wording also appears in the header of Schedules 2 and 3. However, this wording only appears in the Schedules and the main body of the Information Processing Agreement has been signed by both parties. We have no doubt that it forms a binding contract.

[42] The position is the same under the General Data Protection Regulation.

20.1 Data controller

A data controller is a person who alone, or jointly with others, determines the purposes and means of the processing of personal data. In layman's terms, they determine what personal data is used for.

Data controllers are responsible for compliance with the Data Protection Act 1998, including ensuring that personal data is processed fairly and lawfully (see paragraph 22).

A person can either be an independent data controller or can act as a joint data controller or data controller in common with other data controllers.

20.2 Data processor

In contrast, a data processor just processes personal data on behalf of a data controller.

Data processors do not have any direct obligations under the Data Protection Act 1998. Instead, the data controller is responsible for any processing by the data processor. The data controller must only choose data processors that have proper security measures in place. In addition, the data controller must have a contract with the data processor, under which the data processor:

- only acts on the instructions from the controller; and
- is obliged to take appropriate technical and organisational measures to ensure that the personal data is secure.

20.3 Data controller or data processor?

The binary distinction between data controller and data processor can be problematic. It is often difficult to come to a firm conclusion about whether a party receives personal data as data processor or data controller. Our analysis of this issue therefore draws heavily on:

- the Information Commissioner's guidance *Data controllers and data processors: what the difference is and what the governance implications are*, dated 6 May 2014 ("**ICO Controller-Processor Guidance**"); and
- the Article 29 Working Party's *Opinion 1/2010 on the concepts of "controller" and "processor"* adopted on 16 February 2010 ("**A29WP Controller-Processor Guidance**").

This guidance suggests the need to consider a range of factors.

20.4 The contract with DeepMind

The starting point is the Information Processing Agreement. This agreement clearly states that DeepMind processes personal data as processor for the Royal Free.[43]

This is not determinative of DeepMind's status as a data processor (see example 3 in the A29WP Controller-Processor Guidance). However, this is a strong indicator that DeepMind is a data processor.

[43] We note that the old Information Sharing Agreement also clearly identified DeepMind as a data processor.

20.5 Substantive control over processing

Of equal importance is the extent to which the Royal Free retains substantive control over the processing of patient information. The ICO Controller-Processor Guidance suggests that you must consider who decides:

- *to collect the personal data in the first place?* The Royal Free collects patient data from patients. DeepMind has no involvement in this process and the patient has no relationship or contact with DeepMind;
- *the legal basis for collecting personal data?* The Royal Free is responsible for determining the legal basis for collecting personal data (see paragraphs 23 and 24). DeepMind has no part in this. The DeepMind Independent Reviewers' report expressly declined to consider which legal basis the Royal Free might rely on to process patient data;
- *which items of personal data to collect, i.e. the content of the data?* The clinicians at the Royal Free are responsible for collecting personal data from patients and for the decision to then convert that information into an appropriate HL7 message or HES data (albeit the HL7 message and HES data format is standardised);
- *the purpose or purposes the data are to be used for?* The Royal Free is responsible for using the output of the Streams App to provide healthcare services to patients. DeepMind is not responsible, and expressly disclaims responsibility, for any subsequent use of the output of Streams;
- *which individuals to collect data about?* Information will be collected about patients who visit the Royal Free's hospitals. To the extent that either party has control over this factor, it is the Royal Free;
- *whether to disclose the data, and if so, who to?* The Royal Free retains control over disclosure. DeepMind can only disclose patient information to third parties with the Royal Free's express written consent;
- *whether subject access and other individuals' rights apply i.e. the application of exemptions?* Subject access requests (and similar rights under the General Data Protection Regulation) are handled by the Royal Free who will be responsible for application of exemptions if relevant. DeepMind is under an express obligation to forward any such requests to the Royal Free; and
- *how long to retain the data or whether to make non-routine amendments to the data?* The Royal Free is responsible for determining the retention period and can ask DeepMind to delete the confidential patient information at any time (see paragraph 19.2).

20.6 Streams does not use AI and technical means are constrained

DeepMind also has comparatively little control over the substantive processing. The Streams application does not use complex artificial intelligence or machine learning to determine when a patient is at risk of AKI (which could suggest sufficient discretion over the means of processing to be a data controller). Instead, it uses a simple algorithm mandated by the NHS (see paragraph 12).

In addition, patient information is not used for development work (areas in which DeepMind would conceivably have greater discretion). Development work is conducted using synthetic data (see paragraph 14.7).

Finally, even at a technical level, the processing by DeepMind is constrained by the Information Processing Agreement which:

- sets out the security measures that must be used by DeepMind in Schedule 1 (including obligations to encrypt data at rest and in transit);
- sets out the technical architecture used to support the Streams in Schedule 3; and
- requires that confidential patient data be hosted within a specific datacentre in England.

The ICO Controller-Processor Guidance and A29WP Controller-Processor Guidance both state that a service provider can have a degree of freedom over the technical means by which the processing takes place and still be a data processor. The ICO's Controller-Processor Guidance states:

> "*Within the terms of the agreement with the data controller, and its contract, a data processor may decide: [1] what IT systems or other methods to use to collect personal data; [2] how to store the personal data; [3] the detail of the security surrounding the personal data; [4] the means used to transfer the personal data from one organisation to another; [5] the means used to retrieve personal data about certain individuals; [6] the method for ensuring a retention schedule is adhered to; and [7] the means used to delete or dispose of the data.*"

It is clear that DeepMind operates well within this envelope.

20.7 Conclusion

We consider the relationship between the Royal Free and DeepMind to be a controller-processor relationship. While the dichotomy between data controllers and data processors can be complex, we see no basis to conclude that DeepMind is anything other than a data processor.[44]

21 Should the involvement of Google make a difference?

In conducting our review, we considered if we ought to treat DeepMind differently from the Royal Free's other information technology partners, such as Cerner.

In particular, should the Royal Free be subject to more demanding requirements because of DeepMind's other high-profile work in the field of artificial intelligence? Or because DeepMind is owned by Google, a very high-profile US company involved in a number of areas of advanced technology?

We decided that this is would not be appropriate. DeepMind acts only as the Royal Free's data processor, so is permitted only to process confidential patient information on the Royal Free's behalf and in accordance with the Royal Free's instructions. Given this limited mandate, we do not see why the Royal Free's engagement with DeepMind should be any different from its use of other technology partners.

[44] For completeness, our conclusion would be the same under the General Data Protection Regulation.

Part D: Compliance with data protection law

22 Outline of data protection law

22.1 The Data Protection Act 1998

The primary source[45] of data protection law in the UK is currently the Data Protection Act 1998. The Data Protection Act 1998 implements the EU Data Protection Directive (95/46/EC).

The Information Commissioner has been appointed to act as supervisory authority in relation to the Data Protection Act 1998.

The Article 29 Working Party acts as a representative body for the European data protection authorities and issues guidance on the interpretation of the Data Protection Directive.

22.2 The General Data Protection Regulation

The Data Protection Act 1998 should be repealed on 25 May 2018 and replaced with the General Data Protection Regulation. As an EU Regulation, it will be directly effective in the UK, but the UK Government is currently passing a Data Protection Bill to complete the implementation of the General Data Protection Regulation and regulate law enforcement and national security processing.

The Scope of our Report is limited to compliance with the Data Protection Act 1998 and hence we do not consider the General Data Protection Regulation or Data Protection Bill in detail. However, we still refer to it at points in this Report. We doubt that our conclusions would have been materially different if the Royal Free were subject to the General Data Protection Regulation.

22.3 Personal data and sensitive personal data

The Data Protection Act 1998 applies to the processing of personal data. This is any information relating to an identified or identifiable natural person. The patient information processed in Streams is clearly personal data.

The Data Protection Act 1998 applies additional restrictions to the processing of sensitive personal data, which includes personal data about an individual's physical or mental health or condition. The confidential patient information is clearly sensitive personal data.

22.4 Data controller and data processors

As set out in paragraph 20, we have concluded that the Royal Free is data controller in respect of patient information and so subject to the Data Protection Act 1998.

In contrast, DeepMind is simply a data processor and so has no direct regulatory obligations under the Data Protection Act 1998.[46]

[45] The Privacy and Electronic Communications (EC Directive) Regulations 2003 impose *sui generis* privacy obligations in relation to electronic communications. However, these obligations are not relevant here.

[46] DeepMind will have direct regulatory obligations under the General Data Protection Regulation relating to matters such as security and record keeping.

22.5 The eight data protection principles

As a data controller, the Royal Free must comply with the eight data protection principles. These state that:[47]

1. Personal data shall be processed fairly and lawfully and, in particular, must satisfy a processing condition and (if necessary) a sensitive personal data processing condition. We address the operation of Streams in paragraph 23 and the testing of Streams in paragraph 24. This principle also requires individuals to be informed of the processing. We consider this requirement in paragraph 25.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. Confidential patient information is just used to deliver Streams and for no other purpose, so this principle is satisfied.[48]

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. We address this principle in paragraph 26.

4. Personal data shall be accurate and, where necessary, kept up to date. We do not believe this to be a concern. Firstly, the use of HL7 messaging to feed Streams is synchronised with the data on the Royal Free's systems. One of the aims of Streams is to accurately represent to the clinicians data held elsewhere in the Royal Free and not to improve that data – to this extent our understanding is that Streams achieves its ends. Secondly, the assessment of whether the data is accurate in Streams is primarily a technical issue and so outside the scope of this Report. Thirdly, we do not understand the accuracy of the data in Streams to have been raised as a concern. Indeed, the clinicians we interviewed stated they had no concerns about the accuracy of the information in Streams.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. We address this principle in paragraph 27.

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998. We address this principle in paragraph 28.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Technical security measures are outside the scope of this Report but we address operational security in paragraph 29.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The confidential patient information is stored in a datacentre in England and so this principle is not relevant (see paragraph 10.10).

[47] The General Data Protection Regulation contains broadly the same obligations.

[48] Please note that we consider this principle is satisfied despite the fact that clinicians do not just use Streams to diagnose AKI and also use the contextual clinical information when treating other conditions, see paragraph 16.8.

22.6 Fair and lawful processing

The Data Protection Act 1998 requires that any processing of personal data must satisfy a processing condition. There are six processing conditions set out in the Data Protection Act 1998. Those conditions are set out in Schedule 2 and include:

- The processing is necessary in order to protect the vital interests of the data subject (paragraph 4). [49]
- The processing is necessary for the exercise of any function conferred on any person by or under an enactment (paragraph 5(b)). [50]

22.7 The processing of sensitive personal data

The processing of sensitive personal data must satisfy a sensitive personal data processing condition. There are a large number of these conditions set out in both Schedule 3 and the associated statutory instruments, though each is narrow in scope. For the purpose of this Report we consider the following conditions:

- The processing is necessary for the exercise of any function conferred on any person by or under an enactment (paragraph 7(1)(b)).[51]
- 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. "Medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services (paragraph 8). [52]

22.8 When is processing "necessary"?

The processing conditions described above apply where the processing is "necessary".

The meaning of this term was considered by the Supreme Court in *South Lanarkshire v Scottish Information Commissioner* [2013] UKSC 55. The Court concluded that "necessary" means "reasonably" necessary (rather than absolutely or strictly necessary). It imports a requirement of proportionality and a requirement for the minimum level of interference to achieve the legitimate aim.

23 Use of personal data for the operation of Streams

23.1 Fair and lawful

Data protection principle 1 requires the processing of personal data to operate Streams to be fair and lawful.

---

[49] The General Data Protection Regulation contains an equivalent condition in article 6(1)(d).

[50] The General Data Protection Regulation should contain an equivalent condition in article 6(1)(e), read in light of section 8 of the Data Protection Bill.

[51] The General Data Protection Regulation should contain an equivalent condition in article 9(2)(h), read in light of sections 10 and 11 and Schedule 1, para 2 of the Data Protection Bill.

[52] The General Data Protection Regulation should contain an equivalent condition in article 9(2)(g), read in light of sections 10 and Schedule 1, para 6 of the Data Protection Bill. Paragraph 6 contains an additional requirement that the processing be in the substantial public interest, which we consider would be satisfied here.

We consider that the operation of Streams is not a breach of confidence (see paragraph 33) and therefore conclude the processing is lawful.[53]

We also consider that it is fair to process patient information to operate Streams. The Royal Free has been transparent about the operation of Streams (see paragraph 25). More generally, we think it is fair for the Royal Free to use a third party processor, such as DeepMind or Cerner, to provide information technology services under strictly controlled conditions (as is the case here).

23.2 Processing condition

We consider that the operation of Streams satisfies a processing condition as the processing is necessary in order to protect the vital interests of the data subjects (condition 4 of Schedule 2).

Those vital interests include the detection and treatment of acute kidney injury given that it can lead to serious complications or death (see paragraph 9). This conclusion is supported by the Data Protection Directive, which states "*the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life*".[54]

We consider this processing to be "necessary" even though Streams contains details of all the patients at the Royal Free, and not just those who have had a blood test or triggered an AKI alert. The patient's personal data is still stored on Streams to protect them against AKI, albeit the AKI event might only occur in the future or not occur at all.

Put differently, the Royal Free cannot predict which of its patients will present with AKI in the future. That patient's information needs to be kept in Streams to ensure that an AKI alert will be triggered (if appropriate) and the clinician can be provided with contextual clinical information to treat the patient.[55] Retaining information about a patient on Streams for the purposes of future treatment is not significantly different from retaining information about the patient on the Royal Free's other systems.

Alternatively, we also consider that the operation of Streams is necessary for the Royal Free's exercise of functions conferred on it by section 43 of the National Health Service Act 2006 (condition 5(b) of Schedule 2).[56] Section 43 sets out that the principal purpose of the Royal Free is the provision of goods or services for the purpose of the health service of England. It may provide services for any purpose related to the prevention, diagnosis or treatment of illness. The Royal Free may do anything which appears to it to be necessary or expedient for the purpose of or in connection with its functions (see section 47).

---

[53] We are not aware of any other basis on which the lawfulness of this processing can be challenged.

[54] Recital 31.

[55] And for the reasons set out in paragraph 26.1, we understand it would be very difficult to just pull this information off the Royal Free's systems when needed.

[56] This conclusion raises interesting questions about whether it is possible to rely on multiple conditions. We note, and understand, the strong aversion to relying on consent and an additional processing condition, as this negates the choice given to the individual. However, we think the position is different where consent is not one of the processing conditions relied upon. In this regard, we differ from the conclusions of the Article 29 Working Party in their draft guidance on consent (see page 22 of WP259).

23.3 Sensitive personal data processing condition

We consider that the operation of Streams would satisfy a sensitive personal data processing condition as it is necessary for medical purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (condition 8 of Schedule 3).

Medical purposes are defined widely to include "*preventative medicine, medical diagnosis … and the provision of care and treatment*", which is clearly the purpose of Streams.[57]

The processing is also undertaken by a health professional or person under a similar duty of confidence. In particular:

- the clinicians at the Royal Free using Streams are all registered medical practitioners or registered nurses and so qualify as "health professionals";[58] and
- the limited number of DeepMind personnel with access to the Streams database are not "health professionals", but are subject to duties of confidentiality which are equivalent to that which would arise if that person were a health professional. In particular, we consider that DeepMind personnel will be subject to the same equitable duty of confidence as would be imposed on a health professional (see paragraph 31.4)[59] and the existence of this duty is reinforced by the contractual obligations and policies with which those personnel must comply. The DeepMind personnel would not be directly subject to professional oversight, but given that this provision expressly permits processing by people who are not "health professionals", we do not think professional regulation is necessary to satisfy this condition.[60] There are also alternative arguments that this condition is satisfied,[61] which we do not explore here.

Alternatively, for the reasons set out above, we also consider that the operation of Streams is necessary for the Royal Free's exercise of functions conferred on it by section 43 of the National Health Service Act 2006 (condition 7(1)(b) of Schedule 3).

Importantly, our conclusion is a point of general application. It would be surprising if it were unlawful for the Royal Free to use information technology suppliers. This would be entirely at odds with the way modern healthcare is delivered across the NHS. For example, if the Royal Free's use of DeepMind to provide Streams were unlawful, then, presumably, so would the use of Cerner to provide the Royal Free's core information technology systems.

---

[57] We note that the Article 29 Working Party's *Working Document on the processing of personal data relating to health in electronic health records*, February 2007 suggests a slightly narrower approach. This could be interpreted as limiting this processing condition to the narrow bilateral relationship between a patient and their doctor that would not permit access by other medical professionals treating that patient. Access by other medical professionals to treat the patient should instead have a specific basis in national law. However, we do not think the opinion should be read in this narrow fashion, which would not reflect the way modern healthcare is delivered.

[58] See the definition of health professional in section 69 of the Data Protection Act 1998.

[59] In particular, the information is clearly imparted to the DeepMind personnel in a situation that imposes a duty of confidence on the DeepMind personnel.

[60] We are fortified in our conclusion by section 11 of the Data Protection Bill, which states that this condition also applies to a person "who in the circumstances owes a duty of confidentiality under an enactment or rule of law".

[61] For example, it is arguable that disclosure to a processor does not need to satisfy a processing condition as the personal data remains under the control of the controller at all times (though it is less clear how this principle applies here, given the condition appears to focus on the actual individuals carrying out the processing and not the controller). Similarly, it is arguable that the reference to "undertaken" should be interpreted as meaning that the person responsible for the relevant processing must be a health professional, but can direct others to assist them with that aim.

23.4 Conclusion

We consider the Royal Free's processing of personal data to operate Streams to be fair and lawful.

24 Use of personal data for testing

24.1 Fair and lawful

Data protection principle 1 requires any processing of personal data to test Streams to be fair and lawful.

We consider that the use of confidential patient information to test if Streams is working correctly would not be a breach of confidence (see paragraph 33) and therefore would be lawful.[62]

We also consider that it would be fair to use confidential patient information to confirm that Streams is working correctly. We think it would be negligent for the Royal Free to deploy a product like Streams in a live clinical environment without properly testing first, and that inevitably means using confidential patient information (see paragraph 14.4). Given that confidential patient information is held under tightly controlled conditions, we see no meaningful detriment to the individual.

24.2 Processing condition

We consider that testing Streams using confidential patient information would satisfy a processing condition as it is necessary in order to protect the vital interests of the data subjects (condition 4 of Schedule 2).

It is necessary for a product like Streams to be properly tested before deploying it in a live clinical environment, and there is sufficient nexus between testing and live clinical use for this processing condition to cover both testing and live use (see the interpretation of "necessary" in paragraph 22.8). In addition, where testing takes place in a clinical environment, the clinicians are using Streams in parallel with their existing systems to actually treat patients.

Alternatively, we also consider that the operation of Streams is necessary for the Royal Free's exercise of functions. Those functions are conferred on it by section 43 of the National Health Service Act 2006,[63] read in light of the obligation of the Royal Free to "have regard to" the various information technology standards pursuant to section 250(6) of the Health and Social Care Act 2012 (condition 5(b) of Schedule 2). Those information technology standards require testing and are described in paragraph 14.4.

24.3 Sensitive personal data processing condition

We consider that testing of Streams using confidential patient information would satisfy a sensitive personal data processing condition as it is necessary for medical purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (condition 8 of Schedule 3).

[62] We are not aware of any other basis on which the lawfulness of this processing can be challenged.

[63] Described in further detail in paragraph 23.2.

Medical purposes are defined widely to include "*the purpose of preventative medicine, medical diagnosis … and the provision of care and treatment and the management of healthcare services*". We think that testing a clinical system to confirm that it operates safely and effectively is sufficiently closely connected to the final operation of Streams to still be "*necessary*" for "*the purpose of …medical diagnosis*" (see paragraph 22.8).[64] In addition, where testing takes place in a clinical environment, the clinicians are using Streams in parallel with their existing systems, so the processing is to actually treat patients (albeit that use is limited and secondary).

As set out in paragraph 23.3 above, we consider that the processing is conducted by a health professional or by persons subject to an equivalent duty of confidence.

Alternatively, for the reasons set out above, we also consider that the operation of Streams is necessary for the Royal Free's exercise of functions conferred on it by section 43 of the National Health Service Act 2006, read in light of section 250(6) of the Health and Social Care Act 2012 (condition 7(1)(b) of Schedule 3). [65]

24.4 Conclusions

The development (and any consequent testing) of Streams has been suspended pending the finalisation of this Report. This means that these issues are, technically, outside the scope of the Report.

However, as and when that development resumes, we believe that the use of confidential patient information to test clinical safety and effectiveness is fair and lawful. This is conditional on the use of confidential patient information being necessary for testing, minimised as far as possible (with synthetic data used wherever possible instead) and tight controls over the use of that information being in place.

We recommend that the Royal Free confirms that the use of confidential patient information is necessary in advance of any future testing as part of the relevant privacy impact assessment. The Royal Free should clearly document: (a) the justification for using confidential patient information, rather than synthetic data; (b) the justification for the volume of confidential patient information being used in testing including a consideration of whether a smaller amount would suffice; and (c) the controls used to protect that confidential patient information.

25 Transparency of the Streams application

25.1 Transparency obligations

Under the Data Protection Act 1998, the Royal Free must identify itself as data controller and tell patients:

- the purposes for which it processes their personal data; and

[64] We note that the equivalent provision under the General Data Protection Regulation, expressly applies to the "management of health care systems" (see Schedule 1, para 2 of the Data Protection Bill).

[65] We note that it would be extremely problematic for neither condition to apply. We do not think it possible to rely on explicit consent (condition 1 of Schedule 3). It would be very difficult, if not impossible, to obtain that consent from a sufficiently large proportion of the population to allow a full suite of functional and non-functional tests (e.g. load testing). Just testing on patients who provide consent might not provide a representative sample. As previously discussed, we understand that proper testing is a necessary pre-condition to clinical use (see paragraph 14.4) so a narrow interpretation of Schedule 3, paragraph 8 would, in effect, largely prevent the use of new information technology systems in healthcare in the UK under the current law.

- "*any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair*".[66]

The Information Commissioner's Code of Practice, *Privacy notices, transparency and control*,[67] states that this means disclosing with whom a data subject's information will be shared with (page 8). However, the Code suggests that this obligation is just directed at sharing with third party data controllers (page 10) and not use of processors.

The General Data Protection Regulation will require much greater disclosure. While this Report does not extend to the General Data Protection Regulation, we note that it will require the disclosure of recipients or categories of recipients of personal data, and that "recipient" is defined to include data processors. The draft guidance from the Article 29 Working Party states that recipients should be named unless it is fair not to do so, in which case information should be given about the industry, sector and sub-sector and the location of the recipient.

25.2 Privacy notices

The Royal Free has a general privacy statement on its website and a Q&A on data sharing.[68] This includes highlighting the patient's right to withdraw consent to data sharing. We consider this to be sufficient under the Data Protection Act 1998. It will not meet the much broader disclosure obligations in the General Data Protection Regulation when it applies in May 2018, but we do not consider those additional obligations in this Report.

The Royal Free has a separate web page that sets out how it uses patient information. This includes a video explaining how patients' information is processed and shared with third parties. There is also a specific webpage that describes the Streams application in detail, including two further videos on the Streams application. Finally, there is a separate webpage with details of the Information Commissioner's current investigation.[69]

While we were impressed with the amount of information on the Royal Free's website and the accessibility of that information, we were concerned that it might not be brought to patients' attention. We carried out a tour of the Royal Free hospital[70] and the only reference to the privacy policy was a banner stand at the entrance to the hospital. We did not see other references to the privacy policies in the hospital clinics. We were told there were electronic screens in the clinics that displayed this information, but it appears that those screens had been removed as part of a recent refurbishment of those clinics.

We discussed this with the IG manager, who agreed that the Royal Free could do more to highlight the privacy policy to visitors to the hospital. For example, the Royal Free has electronic registration terminals that could be used to highlight this information to patients.

---

66 Schedule 1, Part II, para 2(3), Data Protection Act 1998.

67 See https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

68 See https://www.royalfree.nhs.uk/patients-visitors/privacy-statement/
https://www.royalfree.nhs.uk/patients-visitors/privacy-statement/data-sharing-qa/

69 See https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/
https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/our-work-with-deepmind/
https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/information-commissioners-office-ico-investigation-into-our-work-with-deepmind/

70 Please note we did not conduct a similar review at the Royal Free's Barnet or Chase Farm hospitals.

Finally, the Royal Free should amend its privacy notices to make it clear that they apply to all three hospitals, i.e. not just the Royal Free hospital but also the hospitals in Barnet and Chase Farm.

25.3 Conclusions

We consider that the Royal Free has largely satisfied its transparency obligations in relation to Streams, but needs to do more to explain to visitors to the hospital (as opposed to its website) how their information is used. It should also make it clear that the privacy notices cover all three hospitals. Finally, it should also update its privacy notices in light of the General Data Protection Regulation.

26 Proportionality – Adequate, relevant and not excessive

26.1 HL7 feed vs query-based model

The Royal Free currently provides an HL7 feed to Streams. The feed contains all ADT, ORR, ORU and ORM HL7 messages, together with HES data and renal reporting information.

In other words, this information is provided for all patients at the Royal Free regardless of whether or not they have blood tests, and regardless of whether an AKI alert is triggered. That information is added to Streams and currently retained indefinitely (see paragraph 27).

We asked the Royal Free if Streams could have been designed so that it doesn't store patient information and instead queries the Royal Free's systems as and when that information is required. In other words, when a blood test result is provided, the Streams system would be alerted and would then pull in contextual clinical information for that patient alone. That information could then be purged from the system after an appropriate period.

The Royal Free informed us that they had considered this approach and it is not technically possible. The key reasons for this are:

- that a query-based system would need to use the Royal Free's ODBC (Open Database Connectivity) connection to their central database. This simply does not have the capacity to deal with the volume of queries likely to be generated by Streams. We were informed that an ODBC query-based model was used when rolling out a dictation system at the Royal Free. This caused significant systems delays that had a serious effect on the dictation system;
- that a query-based system would also need to interrogate over 120 other systems to obtain relevant clinical information. This would be problematic if any of those other systems were unavailable, as relevant clinical information could not be provided. Added to that, not all of those systems support query requests. For example, the Royal Free uses blood gas analysers that transmit just HL7 messages onto the Royal Free's network, but do not have the functionality to respond to queries;[71] and
- an HL7 message feed would still be needed to trigger the Streams system in the first place (i.e. the Streams system would still need to be alerted to a new blood test).

Accordingly, we consider that the current HL7 feed is proportionate for three reasons:

- while we are not in position to determine if the technical barriers to move to a query-based model are insurmountable, it is clear that it would require very significant

[71] This would fail to make relevant information available to clinicians, contrary to the seventh Caldicott principle.

changes both to Streams and to the Royal Free's other information technology systems. It is also very likely to lead to a system that is slower and does not always provide complete information;

- DeepMind holds the information received as data processor under tightly controlled conditions. We do not think their holding this information presents any significant risks to patients' information and is not different in nature from other third parties hosting this information on the Royal Free's behalf (e.g. Cerner); and
- the Royal Free, as data controller, will always holds this information separately in its other systems (see paragraph 15). In other words, the assessment is not whether it is proportionate for the Royal Free to hold this information at all, but rather is it proportionate to hold an additional copy in the Streams system where there is a very clear technical and clinical need to do so to provide the Streams App.

26.2 Inclusion of Barnet and Chase Farm

The HL7 messages from Streams include patients from not only the Royal Free hospital, but also the Chase Farm and Barnet hospitals. This is despite the fact that the Streams App is only used by clinicians in the Royal Free hospital.

We challenged the Royal Free about this practice on the basis that it is disproportionate to feed information about Barnet and Chase Farm patients into the Streams system given they may never visit the Royal Free hospital and so never benefit from the Streams application.

The clinicians we interviewed (see paragraph 16.8) and the Trust's data protection officer informed us that the three hospitals operate as a single unit and patients move freely between the hospitals. For example, a patient might be treated initially in Barnet, be tested and subsequently be transferred to the Royal Free hospital. If the HL7 feed into Streams did not include data from all three hospitals, then important information relevant to clinical care provided at the Royal Free hospital would be missing from the Streams App (i.e. it would just show details of treatment in the Royal Free hospital). We were informed that this would be clinically dangerous.

Again, this information would be available from the Royal Free's other information technology systems in any event (see paragraph 15).

26.3 Conclusions

We consider the current model of feeding the Streams system with information about patients from the Royal Free, Barnet and Chase Farm hospitals to be processing of personal data in a manner that is adequate, relevant and not excessive.

27 Retention period for Streams and accountability

27.1 Lack of retention period

The Royal Free does not apply a retention period to the information on Streams. While only five years of results were initially transferred to Streams, there is no process to delete old information. Instead, the volume of information grows over time. This means the information in Streams is now up to eight years old.

The older information is not used to generate AKI alerts, which only requires data from the previous 12 months, but does provide contextual clinical information that is relevant when treating the patient (see paragraph 11).

We discussed this issue with the clinicians we interviewed (see paragraph 16.8). They were of the opinion that information over eight years old is relevant and important when treating patients. The consultant we spoke to said some of the information would continue to be relevant even when it was over ten years' old. For example, the fact that a patient had a kidney taken out 20 years ago would be highly relevant when dealing with AKI. Obviously, not all the contextual clinical information will always be relevant but it would be extremely difficult, if not impossible, to accurately predict which information would be needed in the future. The clinicians we interviewed said that they would prefer to have that information available and then decide what was relevant at the time.

The current approach to retention can be benchmarked against that set out in the *Records Management Code of Practice for Health and Social Care 2016* published by the Information Governance Alliance for the Department of Health. This suggests that adult health records should be kept for eight years from the date of discharge or last treatment. However, certain types of records should be kept for a longer period, such as records of long term or recurrent illnesses which should be kept for 30 years or 8 years after the patient's death. Similarly, pathology reports should be kept for as long as there is a clinical need with a review of the retention of that record after 20 years.

It is also important to note that the information in Streams is a subset of the information in the Royal Free's other information technology systems (see paragraph 15.3). We understand that those systems retain this information for a longer period. This means that clinicians can access much older information directly from those systems regardless of any retention period applicable to Streams. This Report is limited to issues related to Streams, and so we do not comment on the Royal Free's wider approach to record retention.

Finally, we do not think it is relevant that the information in Streams is hosted by DeepMind. DeepMind holds the information received as data processor under tightly controlled conditions. This should not affect the retention period for that information.

27.2 Accountability

The Royal Free should ensure that it maintains appropriate records regarding its processing of personal data. This will become particularly important once the record keeping obligations in the General Data Protection Regulation come into force. The Royal Free should ensure those records include details of Streams.

27.3 Conclusions

We are not health professionals and so defer to the clinicians' judgement that there is a clinical need to access at least eight years' worth of contextual clinical information.[72] On that basis, we do not think that confidential patient information is *currently* kept longer than is necessary for medical purposes.

However, we do not think it is good practice for the Royal Free not to have set a retention period of this information and that is potentially a breach of their accountability obligations once the General Data Protection Regulation applies in May 2018. We recommend that the Royal Free considers this issue in further detail and sets an upper limit on the age of the information contained in Streams.

[72] While there might be arguments for an alternative period, eight years falls within the bracket of legitimate periods of retention. See *C, R (on the application of) v Northumberland County Council* [2015] EWHC 2134.

28 Complying with individual rights

28.1 Subject access requests

The Data Protection Act 1998 gives individuals a right to ask a controller if it is processing their personal data and, if so, to have a copy of that personal data together with details of the purposes and recipients of that data. This is known as a subject access request.

All of the information stored on Streams is also stored on the Royal Free's core system. This means that the vast majority of subject access requests are satisfied by simply extracting the patient's information from those core systems without any need to interrogate Streams. These general subject access requests fall outside the Scope of this Report.

However, the Royal Free received three subject access requests over the last two years that specifically asked for information on the Streams system. We inspected anonymised copies of those three requests on site at the Royal Free. In relation to those three redacted subject access requests:

- the Royal Free contacted DeepMind to obtain copies of the patients' information from Streams;
- DeepMind provided copies of the relevant HL7 messages. We did not inspect the actual HL7 messages due to the difficulties in properly redacting that information; and
- the Royal Free responded to the patient with a copy of those HL7 messages. In relation to those responses:
  - a response was provided in 44, 40 and 4 days. The first was very slightly outside the statutory 40-day period. The response to the last two was provided on time, or, in the case of the last request, significantly within the 40-day period;
  - the response states that the data was provided from "*the trust's Pathology system called WinPath*". However, we were informed during the interview with the IG manager that the information was instead obtained from Streams (see above). We recommend that this point is clarified in future responses; and
  - the response states "*your data is not visible to Google DeepMind staff*". As set out in paragraph 17.5, DeepMind's personnel do have access to the data albeit under tightly controlled conditions. We recommend that this point is clarified in future responses.

28.2 Rights to object to processing

The Data Protection Act 1998 gives individuals the right to object to unwarranted processing that would cause substantial damage or distress. It is not clear how this right would apply to Streams.[73]

However, the Royal Free provides patients with the option to object to the sharing of their health records. We understand that this is done on confidentiality and ethical grounds. This is not standard practice and we were informed that other NHS Trusts do not allow patients

[73] Similarly, we think it unlikely that the rights in the General Data Protection Regulation to object to processing and to erasure would apply. However, as the Royal Free gives patients a right to opt out of Streams, this issue is largely irrelevant.

to opt out of inclusion in core patient treatment systems. The Royal Free has received approximately 190 objections from patients objecting to their data being shared with DeepMind.

We chose 5 of those 190 objections at random and reviewed anonymised copies of the correspondence relating to them. In relation to the process to deal with those objections:

- the Royal Free confirms the patient's identity (as this is not always clear from the initial contact);
- when the patient's identity is confirmed, their details are added to a spreadsheet, which is then added to a secure server to which DeepMind has access;
- DeepMind will then automatically filter out HL7 messages for that patient using the Mirth engine, so that they are deleted rather than be added to the HL7 database (see paragraph 10.3).[74] DeepMind informed us that they will also delete any existing records for that patient within 30 days and HES data is not loaded for such patients;[75] and
- the Royal Free responds to the patient to confirm that their details have been removed from Streams. Of the five redacted opt-outs we reviewed, the Royal Free responded to patients within 1, 4, 5 and 22[76] days in relation to four of them. The 22-day period was a case in which the initial opt-out request was made to the Royal Free's Patient Administration Liaison unit and there was a delay of two weeks before it was forwarded to the Royal Free's IG manager. The Royal Free did not have a record of a written response to the fifth request. However, the IG Manager indicated that this was an unusual case as it came from a clinician at the Royal Free and so confirmation of the opt out was provided to that clinician orally.

We consider this to be an appropriate way to deal with these requests. We also understand that there was an increase in opt-outs at the time the Streams arrangement was reported in the press and another increase at the time the Information Commissioner issued her Undertakings. There have been very few opt-outs since then. We recommend that the Royal Free's Patient Advice and Liaison Service is reminded of the need to identify opt-outs and forward them to the IG Manager in a timely manner.[77]

Finally, we asked the Royal Free if opting out would compromise that patient's care.[78] The Royal Free felt it likely that acute kidney injury would still be picked up by the medical team treating that patient through the pre-existing processes to review the results of blood tests. However, this could take longer. In addition, the medical team might wrongly assume that AKI would automatically be picked up by the Streams-enabled renal specialists or acute care

[74] This means that the information is still technically sent to the Streams system. However, as it is immediately deleted, we do not think the transitory presence of that information on Streams is of any significance.

[75] We were informed by DeepMind that this is how Streams operates. As technical issues are outside the scope of this Report we have not independently verified this to be the case.

[76] Please note that we only measured the time to provide a final response to the patient. The time to update the relevant spreadsheet and then send that to DeepMind could be different and was not measured. However, we consider that the response time is likely to be indicative of the overall timescale.

[77] The Royal Free's Patient Advice and Liaison Service should, of course, be able to identify and deal with patient's requests more generally, including the exercise of new rights under the General Data Protection Regulation. However, these issues fall outside the scope of this report.

[78] We note that the privacy impact assessment issued by Yeovil District Hospital NHS Foundation Trust indicates that it does not provide patients with an opt out because of the potential impact on their healthcare.

team. We recommend that the Royal Free considers warning patients opting-out of Streams that this could directly affect their care.

28.3 Conclusion

Subject to the minor recommendations set out above, we consider that the Royal Free has appropriate procedures in place to deal with subject access requests and opt-out requests.

29 Operational security measures

29.1 The Royal Free's security

The seventh principle of the Data Protection Act 1998 requires the Royal Free to take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing or accidental loss, destruction or damage.

We describe the security measures used on the Streams App at paragraph 11 and the Royal Free's governance at paragraph 16. We consider that they are appropriate to protect patient information in the Streams App.

29.2 DeepMind's security

The Royal Free is required under the seventh principle to choose data processors that apply suitable data security measures and to take reasonable steps to ensure compliance with those security measures.

We describe the various technical and organisational measures used by DeepMind in paragraphs 10, 11 and 17. We consider that the operational measures are appropriate to protect patient information in the Streams App.

29.3 Contract with DeepMind

The Royal Free is obliged to have a written agreement with DeepMind that obliges it to only act on its instructions and comply with equivalent data security obligations as are imposed on the Royal Free under the Data Protection Act 1998. The Information Processing Agreement satisfies this obligation.

The Information Processing Agreement also contains a number of additional obligations that will largely satisfy the additional requirements on processor contracts under the General Data Protection Regulation. However, it does not contain an express obligation on DeepMind to inform the Royal Free if, in its opinion, the Royal Free's instructions infringe data protection laws.[79] We note that there is some doubt if it is mandatory for a processor contract to contain this obligation, but recommend that the Information Processing Agreement is amended to include this provision prior to the General Data Protection Regulation applying to the UK.

29.4 Conclusion

Subject to the proposed minor amendment to the Information Processing Agreement set out in paragraph 29.3, we consider that the Royal Free has satisfied its obligation under the seventh data protection principle. However, as set out in the Scope, we have not conducted a technical security review.

[79] See Article 28(3) of the General Data Protection Regulation.

Part E: Confidentiality

30 Duties of confidence

The law of confidence is very different from data protection laws. Data protection laws originate from an EU Directive,[80] are detailed and codified and enforced by a regulator specifically created for that purpose.

In contrast, the laws of confidence largely originate[81] from case law, i.e. the law is developed through judgments of the courts. They are not enforced by a single regulator and are instead subject to private enforcement through the courts.

This has complicated our review. The courts have avoided providing a comprehensive overview of the qualifications to a health professional's duty of confidence, preferring instead to concentrate on the specific issue before them.

In addition, the application of the law of confidence to modern health care is not straightforward. Many patients no longer have a simple bilateral relationship with a single doctor. Instead, they are treated in a complex multi-agency environment with support from different specialists using a range of information technology systems.

31 Legal duty

31.1 Undisputed aspects of the duty of confidence

Case law does not provide a consolidated overview of the qualifications to a health professional's duty of confidence. However, we think that the following aspects of the duty are clearly established and are not controversial:

- information about a person's health, and treatment for ill-health, is both private and confidential. It is crucial to respect not only the privacy of a patient, but also to preserve confidence in the health profession and health services in general. Without this protection, those needing medical assistance might be deterred from doing so or from revealing private and intimate information. This would endanger the patient's own health and, in the case of transmissible diseases, that of the community;[82]
- the duty of confidence stems from both the relationship between the patient and the health professional, and also from the nature of the information itself;[83] and
- a health professional is permitted to disclose information in the following situations:
  - with the patient's express consent;
  - where necessary for the treatment of the patient, including disclosing information to other health professionals; this is commonly regarded as being justified on the basis of implied consent to direct care. We consider this issue further in paragraph 31.4 and 31.5;

[80] Soon to be replaced by the EU General Data Protection Regulation.

[81] The Trade Secrets Directive 2016/943 is likely to result in some statutory intervention but the current proposal is to limit this to procedural issues. In any event, the Directive is not relevant for current purposes as confidential patient information would not constitute a trade secret under the Directive.

[82] *Z v Finland* (1997) 25 EHRR 371.

[83] *Campbell v MGN* [2004] UKHL 22.

- where it is justified in the public interest.[84] We do not think that any such public interest arises here;
- where the disclosure is authorised for the purposes of research, audit or other activities under section 251 of the Health and Social Care Act 2012. We do not think this exemption is relevant here (see paragraph 31.7); and
- where the health professional is permitted, or obliged, to disclose information by law or by an order from the Court.[85] We do not think any such legal obligation arises here.

This is sufficient to decide the vast majority of cases before the Courts.

31.2 Contentious aspects of the duty of confidence

However, to address the issues raised in this Report, particularly the question of whether the use of confidential patient data for testing of information technology systems is a breach of confidence, it is necessary to go beyond these agreed principles. We therefore consider the following questions, the answers to which appear to be less clearly defined and less clearly considered:

- whether a health professional is subject to a "common law" or "equitable" duty of confidence? We conclude that this is an equitable duty of confidence (see paragraph 31.3);
- what is the correct test to determine if a health professional has breached their duty of confidence? We conclude that the key test is whether a reasonable health professional's conscience would be troubled by the disclosure (see paragraph 31.4); and
- whether a health professional can disclose information to a "confidential agent" without breaching the duty of confidence? We conclude that such disclosures are likely to be permitted in most cases (see paragraph 31.6).

While we accept that these aspects are not universally recognised, we believe they correctly reflect the law and our subsequent analysis is based upon them.

None of these conclusions undermine the crucial importance of maintaining the privacy and confidentiality of patient information.

31.3 Common law or equitable duty of confidence

Duties of confidence owed by health professionals might have a range of jurisdictional basis, including equity, contract or the tort of misuse of private information.[86] This might seem like an obscure and technical question of interest only to lawyers, but it is fundamental to understanding the nature of a health professional's duty and its exceptions.

We consider that a health professional's duty of confidence arises in equity. There are a number of reasons for this conclusion:

[84] *W v Egdell* [1990] 2 WLR 471.

[85] *Hunter v Mann* [1974] QB 767.

[86] *Toulson & Phipps* para 2-004 and *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311.

- the existence of equity as a jurisdictional basis for an action for breach of confidence is firmly established[87] and has been reiterated on numerous occasions.[88] Moreover, where there is no contract with the injured party, equity is the proper jurisdictional basis for a claim.[89] This conclusion is supported by *Gurry*[90] and *Toulson & Phipps*,[91] the leading texts on confidentiality, and the *Principles of Medical Law* which states that "*the common law has long recognized a legal obligation of confidence rooted in equity*";[92]

- we have found very limited support for the proposition that the duty of confidence imposed on a health professional is one that, exceptionally, arises under common law rather than in equity. On the occasions on which the courts have referred to a "common law duty of confidence" it is either simply to quote from relevant guidance (or similar guidance)[93] or used as a generic reference to case law without any serious analysis of the distinction between the common law and equity.[94] The courts have also referred to a common law duty in situations in which the relationship is contractual,[95] which is not relevant to dealings between the Royal Free and its patients.[96] This tendency to elide the common law and equity, and the fact that in most cases the difference is not decisive, was addressed recently by Sir James Munby when addressing the doctor's duty of confidentiality, stating: "*I start with long-established common law principles (I need not for present purposes distinguish between the common law, properly so-called, and equity)*";[97]

- the Court of Appeal's decision in *W, X, Y and Z v The Secretary of State for Health* [2015] EWCA Civ 1034 considered if Government guidance requiring disclosure of information about non-UK residents who failed to pay for NHS services was

---

87 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203.

88 *Attorney General v Guardian Newspapers Ltd and Others (No 2)* [1990] LRC (Const) 938 (Spycatcher), *Campbell v MGN* [2004] 2 AC 457 and *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31.

89 *OBG v Allan* [2007] UKHL 21.

90 "*where the parties to a confidential disclosure are not in a contractual relationship, equity provides the only basis for the court's intervention*", para 4.43.

91 *Toulson & Phipps* posits that an action for breach of confidence is either: (a) founded on an equitable obligation; or (b) the multi-faceted jurisdiction under which the court may award a full range of equitable and common law remedies. It concludes "*the first [i.e. equitable obligation] is the preferable analysis, both historically and conceptually. The action for breach of confidence has come to occupy its own area within the law, and it may in that sense be described as sui generis, but is desirable for its coherent development that its underlying foundation is clear*", para 2-101.

92 Para 12.06. This compares to *Unlocking Medical Law and Ethics* (Second Edition, Claudia Carr) which refers to an "equitable common law duty of confidence".

93 See *Ashworth Hospital Authority v MGN Ltd* [2001] 1 All ER 991 quoting from the Department of Health's Guidance on the Protection and Use of Patient Information.

94 See *A v General Medical Council and another* [2004] All ER (D) 246 in which the parties had agreed there was a "common law" duty of confidence without consideration of its jurisdictional basis. See also *W, X, Y and Z v The Secretary of State for Health* [2015] EWCA Civ 1034 "*The importance of the confidentiality attaching to information about a person's health and treatment for ill-health has been repeatedly asserted in both common law and Strasbourg jurisprudence*".

95 These cases do not involve health professionals. See *Liffe Administration and Management v Pinkava and another* [2007] EWCA Civ 217 in relation to an employee's duty of confidence or *Parry-Jones v Law S*ociety [1969] 1 Ch 1 in relation to a solicitor's duty of confidence.

96 The *Principles of Medical Laws* states: "*Within the NHS today it is generally accepted that there is no contractual relationship between a doctor (whether a general practitioner or hospital doctor) and the patient. Equally, there is no contractual relationship between the patient and the hospital, such as the NHS Trust, where the patient is cared for*", para 3.08. For completeness, we note *Gurry* states that a health professional's obligation "*in most cases is a contractual one*", para 9.63. However, the authority for this statement is *Sidaway v Board of Governors of Bethlem Royal Hospital* [1985] AC 871 in which the House of Lords stated the relationship was not contractual. Accordingly, we think *Gurry* is wrong on this point. Note the position might be different if the patients were treated privately.

97 *In the Matter of C (A Child)* [2015] EWFC 79.

compatible with human rights law. As such, the focus of that judgment was necessarily on Article 8 of the European Convention on Human Rights, which might arguably be described as a common law duty.[98] However, for the reasons set out in paragraph 31.8, we think that where there is a pre-existing relationship between a health professional and their patient, the duty of confidence will arise in equity; and

- in contrast, the Court of Appeal's judgment in *R v Department of Health ex parte Source Informatics* 52 BMLR 65 not only expressly states that a pharmacist's duty of confidence arises in equity, but decides the case on that basis.[99] We see no reason to distinguish between the duty owed by pharmacists and other health professionals.[100]

Accordingly, we think that a health professional's duty of confidence arises in equity. We think that references to a "common law" duty of confidence are intended to refer to case law. They ought instead to refer to an "equitable duty of confidence" to more precisely describe this duty.

31.4 Equity as a jurisdictional basis and the conscience test

Our conclusion that a health professional's duties arise in equity is important not only in form but also in substance.

This Report is not the right place for an exhaustive analysis of the origins, and differences between, the common law and equity. However, in brief, the English common law was principally developed and administered in the central royal courts. The common law was characterised by relatively rigid rules and strict application of precedent. As a result, the laws of equity developed. Equity was not bound by the rigours of the common law and so was able to exercise much greater discretion and, through a flexible and adaptable application of the law, achieve greater fairness and justice.

This inevitably led to a conflict that was finally resolved by Judicature Acts in 1873-75 which reformed the court system and fused the *courts* of common law and equity. However, this did not fuse the common law and equity, which continue to operate as two distinct areas of law.

The flexible approach of equity is reflected in equitable duties of confidence. These arise in the following circumstances:[101]

- First, the information must be of a confidential nature. There is little doubt that information about a person's health, and treatment for ill-health, is very likely to be of a confidential nature. We consider that patient information is confidential.
- The second requirement is that the information must have been communicated in circumstances importing an obligation of confidence. Again, there is little doubt that this will be the case both because of the relationship between the patient and the health professional, and also from the nature of the information itself. We consider

[98] In the same way that the tort of misuse of private information arises out of the common law, *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311.

[99] There was no breach of confidence because "*the pharmacists' consciences ought not reasonably to be too troubled by*" the relevant disclosure.

[100] We also note *X v Y* [1988] 2 All ER 648 and *W v Egdell* [1989] EWCA Civ 13 involve doctors and appear to have been implicitly decided on the basis of an equitable duty of confidence.

[101] *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41.

that the Royal Free has an equitable duty of confidence towards its patients in relation to patient information.

- Thirdly, there must be an unauthorised use of the information to the detriment of the person communicating it. There are two key elements to this third requirement:
  - the use is unauthorised. What constitutes misuse is necessarily dependent on the scope of the duty owed in a particular relationship.[102] In the context of the duty of confidence owed by a health professional, we believe the correct test is that identified in *Source Informatics*. Simon Brown LJ concluded that he would "*stand back from the many detailed arguments addressed to us and hold simply that the pharmacists' consciences ought not reasonably be troubled*" by the proposed disclosure (the "**conscience test**").[103] We also consider that the conscience test should be approached on an objective basis and consider the position of a reasonable health professional standing in the shoes of the person using the information.[104] We adopt this conscience-based test in the remainder of this Report; and
  - that the use causes detriment. There is some doubt over the need for detriment but as a general rule, it ought to be present if equity is to intervene. Cleary an uncontrolled disclosure or publication of details of a person's health, and treatment for ill-health, would be likely to cause distress and detriment.

Finally, it is a defence to an action for breach of an equitable duty of confidence to show that there was a public interest in disclosing the information.[105]

We consider that this equitable duty, focused on the conscience test, provides a principled framework for the assessment of a health professional's duty of confidentiality, and is properly rooted in precedent.

The conscience test will be driven by all the relevant circumstances.[106] In our view this is an objective ethically-driven assessment. It starts with a recognition of the private nature of medical information and the need to maintain the patient's confidence in the handling of their information. It would then involve a consideration of all relevant factors, including:

- the exact nature of the information being disclosed, the purpose for which it is disclosed, the person to whom it is disclosed, the benefit of disclosing that information and any subsequent controls on the use of that information;
- an assessment of the patient's likely expectations about the use of their information, what they have been told about the disclosure, whether the patient should be consulted on the disclosure and any view expressed by the patient on the disclosure;
- the content of any advice from the relevant Caldicott Guardian or any legal advice; and

[102] *Smith Kline & French v Community Services* (1991) 28 FCR 291.

[103] This is also supported in *Campbell v MGN* [2004] 2 AC 457: "*Breach of confidence was an equitable remedy and equity traditionally fastens on the conscience of one party to enforce equitable duties which arise out of his relationship with the other*."

[104] *W v Egdell* [1989] EWCA Civ 13 and *Primary Group (UK) Ltd v Royal Bank of Scotland plc* [2014] EWHC 1082.

[105] *W v Egdell* [1989] EWCA Civ 13 and *London Regional Transport v The Mayor of London* [2001] EWCA Civ 1491.

[106] *Smith Kline & French v Community Services* (1991) 28 FCR 291.

- the best interests of the patient and any relevant professional guidance or practice.

31.5 Implied consent

We note that our conclusions do not align with the original finding that use of confidential patient information for the testing of Streams was a breach of confidence because the Royal Free could not rely on implied consent from patients for direct care.[107] We have two comments about this original finding.

First, it pre-supposes that the use of confidential patient information for testing is a breach of confidence that must be justified on the basis of implied consent. We think the starting point should, instead, be to be assess whether the use of that information for testing would trouble a health professional's conscience and so be a breach of its equitable duty of confidence. Only if there is a potential breach is it then necessary to consider[108] if it can be justified on the basis of implied consent or some other qualification.[109]

Secondly, it is not clear if implied consent must be restricted to direct care. This concept is said to arise because there "*is in effect an unwritten agreement between the individual and the professionals who provide [direct] care that allows this sharing to take place*", but this "*implied consent is only applicable in instances of direct care*".[110] For an implied consent to arise, there "*are three tests … all of which must be met affirmatively:*

- *Is the person sharing the information a registered and regulated professional or one of their direct care team?*
- *Is the activity a type of direct care within the scope specified by the professional's regulatory body?*
- *Does the professional have a legitimate relationship with the person or persons concerned*?"[111]

Implied consent can qualify a duty of confidence.[112] However, it is not clear from case law that the implied consent can only relate to "direct care". In *A v General Medical Council and another* [2004] All ER (D) 246 the court added a number of points "*doctors are likely to be assisted by*". They include that a health professional's duty of confidence "*prevents [the] use or disclosure of confidential information for purposes that have not been expressly or impliedly authorised by the person to whom the duty is owed*". That authorisation is not

[107] Letter from the National Data Guardian to the Royal Free dated 20 February 2017.

[108] Though we do recognise that these two issues are interwoven and, in part, involve similar consideration.

[109] This is the approach in *Source Informatics*, where the case is decided on equitable principles and the Court rejects an analysis based on implied consent.

[110] Para 3.2 of the National Data Guardian's *Information Governance Review* (March 2013).

[111] Para 5.3 of the National Data Guardian's *Information Governance Review* (March 2013).

[112] For example, it is clear that implied consent will justify the disclosure of banking information (*Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461). *Toulson* also suggests that disclosure is permitted with express or implied consent, para 3-169.

limited to direct care.[113] There is also limited support for this narrow interpretation in *Toulson,*[114] *Gurry*[115] or the *Principles of Medical Law.*[116]

This may be a welcome conclusion. We understand the concept of implied consent to direct care is increasingly problematic. The National Data Guardian and Sheffield Solutions hosted two seminars to address the fact that the concept of implied consent is "coming under strain". This reflects the fact that many patients no longer have a simple bi-lateral relationship with their doctor and instead receive health care in a complex multi-agency environment from a range of specialists. The three particular concerns are:

- in a number of cases, the patient may have not taken any step or action that might constitute an implied consent;
- patient information is currently shared for legitimate reasons that cannot be regarded as direct care; and
- patient information is used for direct care purposes in ways that patients would not reasonably expect.[117]

The seminar explores the possibility that the disclosures might instead be permitted where they are within the "reasonable expectations" of the patient. We agree that this is a useful alternative test to consider (see paragraph 31.8).[118]

As an aside, while a test based on an individual patient's reasonable expectations would reflect the patient's autonomy in medical matters,[119] it could be very hard to apply to disclosures affecting large groups of patients. Should a health professional consider the views of *every* patient in the group (some of whom may be opposed to any sharing) or the hypothetical patient squeezed on to the Clapham omnibus?[120] In contrast, the conscience test would clear these legal fictions aside, be simpler to apply and would directly focus on the ethical concerns raised by the disclosure of that information.

31.6 Disclosure of information to "confidential agents"

An associated question is whether it is a breach of confidence to disclose patient information to a third party that will only use the information on the health professionals' behalf and will keep the patient information confidential. For the purposes of brevity, we refer to such a third

[113] We have also considered *de Taranto v Cornelius* [2001] EWCA Civ 1511. However, on the particular facts of that case the Court of Appeal considered that Dr de Taranto could only pass on a medico-legal report with express consent from Mrs Cornelius.

[114] See paragraph 11-105.

[115] See para 9.75, which refers to implied consent as a basis for a health professional consulting with colleagues about a patient's medical condition, but does not treat this as the only circumstance in which implied consent might arise.

[116] See para 12.52, which suggests that while implied consent might be limited to direct care, this a question of fact and there is no rule of law to limit implied consent to direct care.

[117] See *Sharing patient data: exploring consensus on reasonable expectations*, July 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663089/Exploring_consensus_on_reasonable_expectations_-_July_2017_seminar_FINAL.pdf

[118] This approach is also discussed in *Using and disclosing confidential patient information and the English common law: What are the information requirements for valid consent?* Victoria Chico and Mark J Taylor, Medical Law Review Fol. 26, 17 August 2017.

[119] *Montgomery v Lanarkshire Health Board* [2015] UKSC 11.

[120] "*The Clapham omnibus has many passengers. The most venerable is the reasonable man, who was born during the reign of Victoria but remains in vigorous health. Amongst the other passengers are the right-thinking member of society, familiar from the law of defamation, the officious bystander, the reasonable parent, the reasonable landlord, and the fair-minded and informed observer, all of whom have had season tickets for many years*" *Healthcare at Home Limited v The Common Services Agency* [2014] UKSC 49.

party as a "**confidential agent**" (this is not a recognised legal concept in the laws of confidence but would be broadly similar to a data processor under data protection laws).

The laws of confidence do not contain a concept of a confidential agent. This is perhaps not surprising. These laws developed through precedent and it seems unlikely that anyone would want to bring a claim purely as a result of a disclosure to a confidential agent. However, we are satisfied that such disclosure would not breach a health professional's duty of confidence. There are a number of routes to this conclusion:

- the Courts have recognised that disclosure for record keeping and similar functions is not a breach of confidence: "*The duty of confidence originates as a professional duty of the treating doctors, nurses and ancillary staff. Plainly they are entitled without being in breach of that duty, to pass [information] to hospital administrators for the purpose of record keeping and of recovery of the charges*";[121]
- the ability to disclose to third parties acting on a health professional's behalf is recognised by *Toulson* on the basis that keeping records about the patient's treatment is for the protection of the hospital's proper interests and so not a breach of confidence[122]. *Gurry* comes to a similar conclusion[123]; and
- in our view, the disclosure to a confidential agent would be permitted as it would not trouble the health professional's conscience to disclose to a third party who will use it solely for the health professional's purposes and under tightly controlled conditions.

31.7 Section 251

For completeness, we also assess if the disclosure of patient information to DeepMind could be justified under section 251 of the National Health Act 2006 and the associated Health Service (Control of Patient Information) Regulations 2002.

Our view is that this would not be a proper basis for the disclosure. The Regulations permit disclosure for the diagnosis or treatment of neoplasia, managing communicable diseases, medical research or audit. None of these conditions are relevant to the arrangements with DeepMind.

31.8 Alternative approach based on Article 8 of the European Convention on Human Rights

The Human Rights Act 1998 has played an important role in the development of privacy in English law. This includes providing the basis for the tort of misuse of private information, a separate and distinct action to that of breach of confidence.[124] The scope of the tort of misuse of private information is uncertain, but in broad terms it is said to apply where:

- the individual has a reasonable expectation of privacy in respect of the information in issue. This would clearly be the case in respect of confidential patient information;
- the information has been used in a way which interferes with the individual's right to privacy. This would greatly depend on the particular use; and

[121] *W, X, Y And Z, R (on the application of) v The Secretary of State for Health & Ors* [2015] EWCA Civ 1034.

[122] Or that it is based on implied consent from the patient. Para 11-033.

[123] Para 9.80.

[124] *Google Inc v Vidal-Hall* [2015] EWCA Civ 311.

- there is no justification for the interference. A justification must be in accordance with the law and necessary in a democratic society, proportionate and for a legitimate aim.[125]

The emergence of the tort of misuse of private information has not circumscribed the law of confidentiality,[126] but the interrelationship between this tort and conventional confidence cases is not entirely resolved.[127]

The Human Rights Act 1998 already plays a pivotal role where publication is threatened and the courts must inevitably balance Article 8 and Article 10 of the European Convention on Human Rights.[128] Moreover, the courts place significant emphasis on Article 8 rights when asked to order disclosure of health information.[129] Article 8 was also essential to the question of whether Government guidance requiring disclosure of non-UK residents who failed to pay for NHS services was compatible with human rights law, as per *W, X, Y and Z v The Secretary of State for Health* [2015] EWCA Civ 1034.

It is possible[130] that Article 8 of the European Convention on Human Rights will also play an increasingly important role in assessing the more conventional duty of confidence between health professionals and their patients as a means to better clarify this duty: "*by what instrument this balance is to be struck. Is it to be… the golden and straight metwand of the law or the incertain and crooked cord of discretion?*"[131]

However, based on our assessment of current case law we do not think that position has been reached yet. Where there is a pre-existing relationship the duty of confidence will arise in equity.[132]

If we are wrong about this, we think this alternative human rights based approach will lead to much the same conclusion.[133]

An interference with privacy will be justified if it is in accordance with the law, proportionate and for a legitimate aim.

---

[125] *CATT and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9.

[126] *Imerman v Tchenguiz* [2010] EWCA Civ 908.

[127] In theory, a health professional might have to consider ***both*** their equitable duty of confidence and the tort of misuse of private information. However, we think this is unlikely in practice given the additional complexity and the that fact both are likely to lead to the same result, see footnote 133.

[128] *A v B plc [2003] QB 195.*

[129] See for example, *R (on the application of B) v Stafford Combined Court* [2006] All ER (D) 22 or *A Health Authority v X* [2001] Lexis 1479 (upheld on appeal).

[130] We note that the National Data Guardian and Sheffield Solutions recently hosted two seminars to explore this, see paragraph 31.5.

[131] "*It seems to me, with great respect, that this now well established approach [of making an assessment under the European Convention on Human Rights] furnishes a more certain guide for people and their lawyers than the test of the reasonable recipient's conscience. While the latter has the imprimatur of high authority, I can understand how difficult it is to give useful advice on the basis of it. One recipient may lose sleep a lot more readily than another over whether to make a disclosure, without either of them having to be considered unreasonable. If the test is whether the recipient ought to be losing sleep, the imaginary individual will be for practical purposes a judicial stalking-horse and the judgment more nearly an exercise of discretion and correspondingly less predictable. So for my part I find it more helpful today to postulate a recipient who, being reasonable, runs through the proportionality checklist in order to anticipate what a court is likely to decide, and who adjusts his or her conscience and conduct accordingly*." *London Regional Transport v The Mayor of London* [2001] EWCA Civ 1491.

[132] See *Toulson*, para 2-003 and *Ash v McKennitt* [2006] EWCA Civ 1714 and paragraph 31.3.

[133] "*In the present case, as one would hope in most cases, the human rights highway leads to exactly the same outcome as the older road of equity and common law. But it may be that it is in some respects better signposted, and it is therefore helpful that it has played a central role in the argument*." *London Regional Transport v The Mayor of London* [2001] EWCA Civ 1491.

It is very far from clear that the use of confidential patient information for the operation and testing of Streams would be an infringement of the patient's privacy. It seems very likely that the use of information technology by hospitals to deliver health care is within a patient's reasonable expectations, and that the patient would reasonably expect the hospital to properly test the system before deploying it.[134]

Even if there has been an interference with a patient's privacy, we consider that the use of confidential patient information for the operation and testing of Streams would be justified as being in accordance with the law (the Data Protection Act 1998[135]), proportionate (given the strict controls over its use) and for a legitimate aim (the provision of health care[136]).

32 Professional guidance

32.1 Effect of guidance

While the Scope of our Report is limited to assessing the Royal Free's compliance with the privacy and duties of confidence, we consider that this entails a review of professional guidance on duties of confidence for the following reasons:

- the processing of personal data in breach of that professional guidance is likely to be unfair; and
- in relation to the duty of confidentiality, it may be difficult to satisfy the conscience test if the processing is in breach of professional guidance.

32.2 Relevant guidance

For the purposes of this Report, we comment on the Caldicott principles, the Care Record Guarantee and the NHS Code of Practice. However, in order to prepare this Report, we have reviewed:

- the National Data Guardian's *Review of Data Security, Consents and Opt-Outs* (June 2016), *Information Governance Review* (March 2013) and *Report on the Review of Patient-Identifiable Information* (December 1997);
- the *NHS' Confidentiality: NHS Code of Practice* (November 2003), *Confidentiality Policy* (June 2016), *Records Management Code of Practice for Health and Social Care 2016* (July 2016), *Care Record Guarantee* (January 2011), the *HSCIC Code of practice on confidential information* (December 2014) and the NHS Constitution; and
- the GMC's *Confidentiality: Good practice handling patient information* (25 April 2017).

In some cases, it was not clear to us if the guidance was intended to reflect the law or to extend it. The content of an obligation imposed upon a professional by his profession is not,

[134] For example, if one were to ask the reasonable patient on the Clapham omnibus if they would expect a hospital to properly test its information technology systems before putting them into use, the patient might well testily suppress the question with an 'Oh, of course!' However, none of the studies on patient expectations we reviewed seem to have directly asked about attitudes to the testing of information technology systems. See *Wellcome Trust, Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data* (2013), *Royal Statistical Society Response to the Department of Health on Protecting Health and Care Information in England: A Consultation on Proposals to Introduce New Regulations* (August 2014) and *Wellcome Trust, The One-Way Mirror: Public Attitudes to Commercial Access to Health Data* (March 2016).

[135] *CATT and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9.

[136] Article 8 expressly recognises that protection of health is a legitimate aim.

of course, necessarily co-terminus with the obligations imposed by law[137] and indeed "*an enduring feature of professional codes of conduct is that they set higher standards for their members than the general norms of society*".[138] However, if the intent of this guidance is to extend the scope of the law, it would be useful to make it clear and preferably justify why that extension is necessary.

32.3 Caldicott Principles

The seven Caldicott Principles are set out below. We have considered how they apply to the Royal Free's use of Streams below:

Principle 1: Justify the purpose. Confidential patient information is transferred for the testing and operation of Streams, and for no other purpose. The disclosure is clearly documented and is subject to review.

Principle 2: Don't use personal confidential data unless it is absolutely necessary. It is absolutely necessary to use confidential patient information to test and operate Streams. We note that most of the testing is conducted using synthetic data. We have concluded that it was absolutely necessary to use confidential patient information to test Streams (see paragraph 14.4).

Principle 3: Use the minimum necessary personal confidential data. We consider the amount of confidential patient information used in Streams in paragraphs 26 and 27. We have concluded that it is proportionate to use that patient data.

Principle 4: Access to personal confidential data should be on a strict need-to-know basis. We have reviewed the access controls relevant to Streams at various points in this Report, in particular paragraphs 16.5 and 17.5. We consider those controls to be adequate.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities. We have considered the training and awareness of those with access to confidential patient information in paragraphs 16.6 and 17.6. We are generally satisfied with those arrangements, but have recommended that the Royal Free ensure that its personnel conduct information governance training on a more regular basis.

Principle 6: Comply with the law. This Report contains an extensive review of whether the use of Streams is lawful. We have concluded that it is.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality. We agree.

In summary, we are satisfied that the operation and testing of Streams satisfies these principles.

32.4 Care Record Guarantee

The Care Record Guarantee sets out details about how NHS care records will be used. It states that NHS providers "*will not share health information that identifies you…for any reason other than providing your care, unless: (a) you ask us to do so; (b) we ask and you give us specific permission; (c) we have to do this by law; (d) we have special permission for health or research purposes; (e) we have special permission because the public good is thought to be of greater importance than your confidentiality*".

[137] *Lewis v Secretary of State for Health* [2008] EWHC 2196.

[138] *Wingate v The Solicitors Regulation Authority* [2018] EWCA Civ 366.

We do not think this prevents the use of confidential patient information for the operation or testing of Streams. First, as DeepMind only act as data processor/confidential agent we do not think the Royal Free is "sharing" this information. The Royal Free remains in full control of this information at all times.

Secondly, we consider this use is "*providing…care*" to patients. The testing and operation is carried out for the sole purpose of eventually using Streams to provide care to those patients.

Thirdly, the commitments in the Care Record Guarantee should be read in light of the other information provided to patients at the Royal Free, which expressly refers to DeepMind's provision of Streams (see paragraph 25).

Accordingly, we do not think that the Care Record Guarantee materially affects the application of the conscience test to the operation or testing of Streams.

32.5 NHS Confidentiality Code of Practice

The NHS Confidentiality Code of Practice contains a range of obligations that are relevant to Streams. The policy is long and some of its content is not directly relevant to Streams. However, the key principles can be summarised as follows:

- *Protect Patient Information*: We have reviewed the security and access controls relevant to Streams at various points in this Report, in particular paragraphs 16.5 and 17.5. We consider those controls to be adequate.
- *Inform Patients Effective – No Surprises*: We have considered the steps that the Royal Free has taken to bring Streams to patients' attention in paragraph 25. Subject to the recommendations in that paragraph, we are satisfied that the Royal Free complies with this requirement. We recognise the challenges of providing patients with complete and accessible information about the use of their data in a complex multi-agency environment. However, this is part of a bigger conversation affecting the whole of the healthcare system and we doubt it begins with a requirement to give patients a detailed explanation about one particular piece of information technology infrastructure used within a hospital.
- *Provide Choice to Patients*: Information in Streams is used for the purposes of that patient's care. Patients are given the right to object to their data being included in Streams.
- *Improve Wherever Possible*: We have reviewed the policies and training applicable to the Royal Free and DeepMind, including the obligation to notify data breaches, in paragraphs 16.6 and 17.6.

The Code also states: "*information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so*". We think the operation and testing of Streams is compatible with this requirement. Firstly, we think it is "*for [the] purposes [of] healthcare*". Secondly, we think this statement is intended to reflect the legal position, rather than add any additional requirements, and we consider the operation and testing of Streams to be lawful (see paragraph 33) hence satisfying this requirement.

33 Confidentiality: Testing and operation of Streams

33.1 Operation

We consider that the Royal Free has not breached its duty of confidence to patients through the operation of Streams. Applying the test described in paragraph 31.4, we do not think the conscience of a reasonable health professional should be troubled by the use of confidential patient information within Streams to provide care to patients.

We also consider that the Royal Free has not breached its duty of confidence to patients though the use of a third party, DeepMind, to operate the Streams platform. DeepMind can only use confidential patient information on behalf of the Royal Free and only for the operation of Streams. There are a number of the controls and security measures in place to protect that confidential patient information. This arrangement should not trouble the conscience of a reasonable health professional.

33.2 Testing

We consider that the Royal Free would not breach its duty of confidence to patients as a result of using confidential patient information to test Streams. The conscience of a reasonable health professional should not be troubled by the use of confidential patient information for the testing of Streams. In particular, as set out in paragraph 14.4:

- testing is conducted with synthetic data wherever possible. Confidential patient information is only used where strictly necessary;
- testing of confidential patient information takes place under strictly controlled conditions to ensure that the confidentiality and security of that patient data is maintained. Clinical safety and effectiveness testing is conducted by clinicians in the clinical environment using both existing and new systems;
- testing is a necessary part of the clinical deployment of any system and is mandated by standards issued under section 250 of the Health and Social Care Act 2012. Deploying a system without properly testing would be negligent; and
- in our view, patients would reasonably expect the Royal Free to properly test its information technology systems before rolling them out, and it is unlikely that any properly informed patient could reasonably object to the use of their information in this manner. We cannot see how this testing could cause any detriment to the patient.

33.3 Conclusions

We believe that the Royal Free has not breached its duty of confidence to patients through the operation of Streams.

The Royal Free would not breach its duty of confidence through the use of confidential patient information to test Streams in the future, so long as the use of confidential patient is necessary for this purpose, the amount of information used is minimised, and tight controls over the use of that information are in place. We recommend that the Royal Free confirms this is the case in advance of any future testing as part of the relevant privacy impact assessment. The Royal Free should clearly document: (a) the justification for using confidential patient information, rather than synthetic data; (b) the justification for the volume of confidential patient information being used in testing including a consideration of whether

a smaller amount would suffice; and (c) the controls used to protect that confidential patient information.

Part F: Summary of recommendations

34 Recommendations

34.1 The Royal Free

- *Handover of iPhones* – The iPhones loaded with the Streams App are shared between clinicians. There is no formal process for this handover. We do not think this is a material concern, given the small number of iPhones. However, we recommend that if the pool of iPhones expands, a formal handover process is instituted to keep track of the individual to whom the iPhone is issued (see paragraph 11.4).
- *Conduct privacy impact assessments* – If the current projects to extend Streams advance beyond the early design phase, they should be subject to a privacy impact assessment (with the exception of the extension to Barnet Hospital, which has already been subject to a privacy impact assessment). That impact assessment should take place long before conducting testing using confidential patient information (see paragraph 13). This should include the following information on testing: (a) the justification for using confidential patient information, rather than synthetic data; (b) the justification for the volume of confidential patient information being used in testing, including a consideration of whether a smaller amount would suffice; and (c) the controls used to protect that confidential patient information.
- *Statutory data protection officer* – The Royal Free should consider if appointing their current data protection officer to be the statutory data protection officer under the EU General Data Protection Regulation would create a conflict of interest given his responsibilities for the Royal Free's information technology estate (see paragraph 16.3).
- *Leaver and mover process* – We recommend that the Royal Free review its leaver and mover process to ensure that access rights to Streams are withdrawn from clinicians once they leave the Royal Free or move to another department where access is not required. The access list should be reviewed regularly to confirm this process is working (see paragraph 16.5).
- *Training* – The Royal Free should ensure its staff complete mandatory annual information governance training and this should be tracked through the use of appropriate targets.[139] The Royal Free should follow up on any instances of non-compliance (see paragraph 16.6).
- *Audit process* – The Information Processing Agreement provides for a monthly audit programme. This should be restarted once this Report is complete (see paragraph 18.2).
- *Memorandum of Understanding* - We recommend that the Royal Free considers whether its Memorandum of Understanding with DeepMind continues to be relevant to its relationship with DeepMind and, if it is not relevant, terminates that agreement (see paragraph 19.3).
- *Telling patients about Streams* – The Royal Free has provided a lot of useful information about Streams on its website. However, it should do more to bring this

[139] We were informed by the Royal Free that it recently conducted an exercise to encourage staff to complete this training. As a result, 95% of staff have now completed their information governance training within the annual cycle

to the attention of visitors to its hospitals, e.g. notifying patients using the electronic registration screens. The privacy notice will also need to be updated to reflect the additional disclosures required by the General Data Protection Regulation in May 2018 (see paragraph 25.3).

- *Retention period* – The Royal Free is not currently storing confidential patient information in Streams for longer than necessary. However, it has not set a formal retention period for that information. The Royal Free should review this matter and set a retention period for the information in Streams (see paragraph 27).
- *Subject access requests* – The Royal Free should amend its response letter to subject access requests specifically directed at Streams to make it clear that they obtain the relevant information from DeepMind (not WinPath), and to delete the statement that DeepMind does not have access to the data (see paragraph 28.1).
- *Rights to object to processing* – The Royal Free should consider amending its response letter to patients who opt out of Streams, to inform them that it could adversely affect their care (see paragraph 28.2).
- *Information Processing Agreement* – The Royal Free should amend the Information Processing Agreement to require DeepMind to inform the Royal Free, if the Royal Free's instructions breach data protection law. This is a requirement under the EU General Data Protection Regulation (see paragraph 29.3). We suggest that the Information Processing Agreement is also updated to better reflect the data actually transferred by the Royal Free (see paragraph 19.2).

34.2 DeepMind

- *Remote working* - The limited number of DeepMind employees with access to Streams can ask to work remotely. While we understand the need for remote access, we recommend that DeepMind keeps these arrangements under review and continues to carefully review the access logs relevant to employees working remotely (see paragraph 17.7).

Annex 1 – Glossary

acute care team means the nurse-led patients at risk and resuscitation team.

AKI means acute kidney injury. See paragraph 9.

Caldicott Principles means the seven information handling principles developed by the National Data Guardian. See paragraph 32.3.

confidential agent means a third party engaged to use confidential information only on the instructions of the person providing that confidential information. This is not a recognised concept in law and we only use it in this Report for convenience. See paragraph 31.6.

confidential patient information means any information about a patient at the Royal Free. Please note we use the adjective "confidential" to emphasise the private nature of all of this information and not to try and create a distinction between confidential and non-confidential information.

conscience test means the test described in paragraph 31.4.

data controller is a data protection concept and means a person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

data processor is a data protection concept and means a person who processes personal data on behalf of the data controller.

Data Protection Bill means the Data Protection Bill. For the purpose of this report we refer to the version of the Bill published on 18 January 2018.

DeepMind means DeepMind Technologies Limited, a subsidiary of Alphabet Inc and part of the Google group of companies.

First Base means First Base Technologies LLP.

General Data Protection Regulation means the EU General Data Protection Regulation 2016/679.

Gurry means *Gurry on Breach of Confidence: The Protection of Confidential Information*, Second Edition, Tanya Aplin, Lionel Bently, Phillip Johnson and Simon Malynicz.

HES data means the limited HES/SUS data containing diagnosis and procedure codes. See paragraph 10.4.

HL7 messages means the messages in standardised format containing health information. See paragraph 10.2.

Independent Reviewers means the independent review panel appointed by DeepMind, see paragraph 17.3.

Information Processing Agreement means the information processing agreement between DeepMind and the Royal Free dated 10 November 2016. See paragraph 19.2.

LDAP means Lightweight Directory Access Protocol. It is used by the Royal Free to authenticate users on its network and authenticate users of the Streams App. See paragraph 11.5.

MRN means the patient's identification number.

National Data Guardian means Dame Fiona Caldicott who was appointed as the National Data Guardian for Health and Care in November 2014.

NHS AKI algorithm means the NHS algorithm that must be used to detect AKI. See paragraph 12.1.

NHS Confidentiality Policy means the Confidentiality NHS Code of Practice November 2003.

personal data means any information relating to an identified or identifiable natural person.

Principles of Medical Law means *Principals of Medical Law,* Fourth Edition, Judith Laing, Jean McHale, Sir Ian Kennedy and Andrew Grubb.

Scope means the scope of this Report, as set out in paragraph 8 and Annex 3.

Services Agreement means the information processing agreement between DeepMind and the Royal Free dated 10 November 2016. See paragraph 19.1.

Streams App means the App used by clinicians to access Streams. See paragraph 11.

Streams means the AKI detection system audited in this Report.

Streams timeline means the timeline for the development of Streams set out in Annex 2.

synthetic data means the data used by DeepMind to design, develop and partially test applications. It does not contain information about real patients. See paragraph 14.7.

The Royal Free means the Royal Free London NHS Foundation Trust.

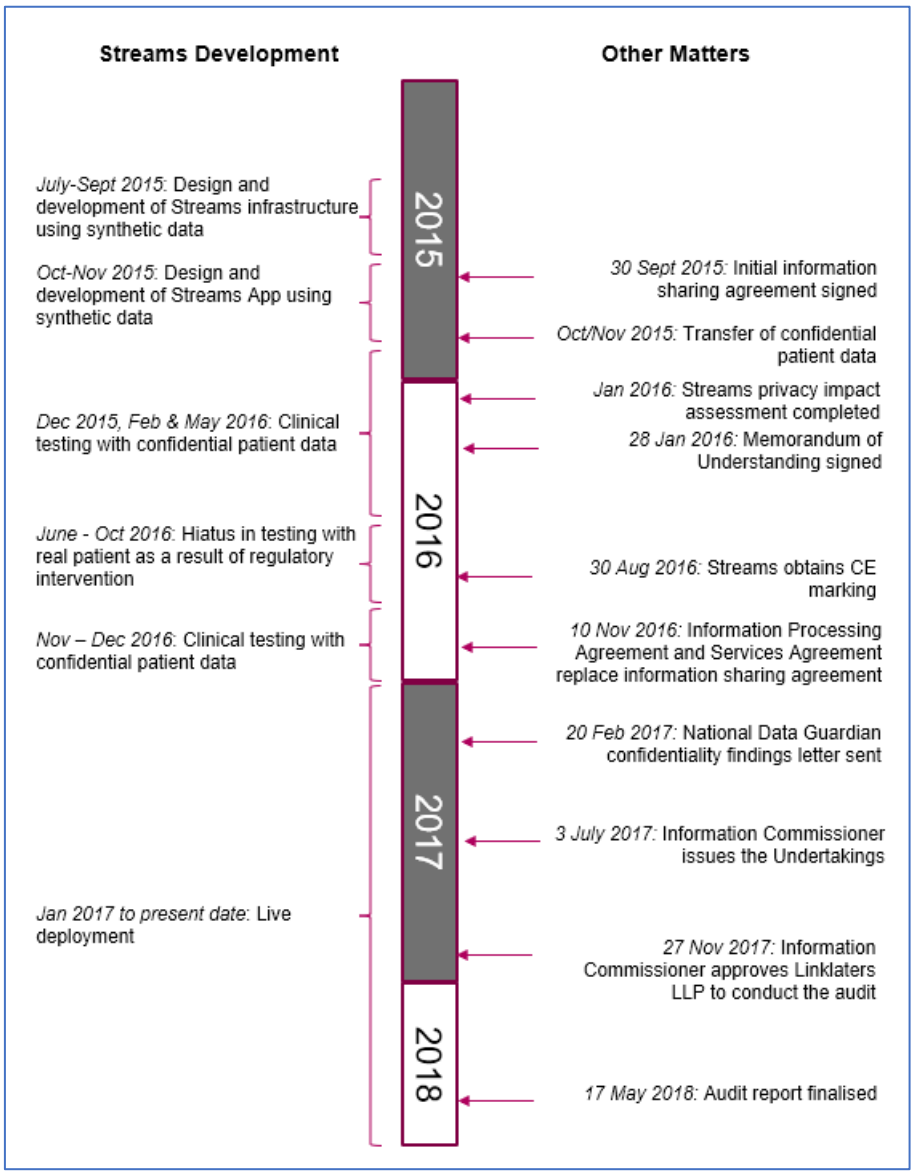
The Royal Free hospital means the Royal Free hospital at Pond Street, London, NW3 2QG.

Toulson & Phipps means *Confidentiality*, Third Edition, The Hon Mr Justice Toulson and, Charles Phipps.

Undertakings means the undertakings given by the Royal Free to the Information Commissioner on 3 July 2017. See Annex 3.

Annex 2 – Timeline

The diagram below provides a broad outline of the key events in the development of Streams and the subsequent investigation by the Information Commissioner.



Annex 3 – Review process

1 Scope of review

On 3 July 2017, the Information Commissioner issued the Undertakings against the Royal Free. Those Undertakings contain the following obligation:

> "*The [Royal Free] 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 [Royal Free] and DeepMind is operating, in practice in order to ensure compliance with [the] Act, and disclose the findings to the [Information] 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 [Information] Commissioner will first approve the [Royal Free]'s choice of auditor and agree the terms of reference. The [Information Commissioner] 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*."

2 Our appointment and conflicts

We were engaged by the Royal Free in June 2017 to advise on the terms of the Undertaking and associated issues. This is the first time we have acted for the Royal Free. We did not advise on the development of Streams or the arrangements with DeepMind before this time or on any other previous matter for the Royal Free.

We do not act for Google or DeepMind.

The Information Commissioner approved our appointment on 27 November 2017.

We were paid a fixed fee of £40,000 (plus VAT) to complete this Report.

3 No reliance by third parties

This Report is addressed solely to the Royal Free. We accept no responsibility or liability to any third party for the contents of this Report.

4 Documentary collection and phased interviews

This Report was prepared in three phases:

- *Documentary Collection*: We asked to review a wide range of documents to supplement those we had already been provided with when advising on the Undertakings.
- *Operational Interviews and Review*: We reviewed the operation of Streams and interviewed a number of individuals from the Royal Free and DeepMind. The operational review included using a version of the Streams App loaded with synthetic data, various data sampling exercises and discussions with clinicians about use of the Streams App in practice.

- *Governance Interviews*: We interviewed a number of senior individuals from the Royal Free and DeepMind. These included Sir David Sloman, the chief executive of the Royal Free, and Mustafa Suleyman, co-founder and Head of Applied AI at DeepMind. We did not interview Dr Demis Hassabis CBE, Co-Founder & CEO, DeepMind as he is not directly involved in the management of DeepMind Health.

5 Review of the Report by the Royal Free and DeepMind

We provided a draft copy of this Report to the Royal Free and DeepMind on Thursday, 8 March 2018. We did so to allow the Royal Free and DeepMind to identify any factual or technical corrections, identify information that might be commercially sensitive, and to comment on the findings.

We had largely completed the Report at that point but had not completed the interviews with Mustafa Suleyman of DeepMind nor DeepMind's Clinical Lead. We had also not interviewed Sir David Sloman of the Royal Free nor the Royal Free's CIO or Caldicott Guardian.

We made the following changes to the Report based on feedback from the Royal Free and DeepMind:

- DeepMind and the Royal Free suggested a small number of typographical corrections.
- The Royal Free asked us to amend the summary to point out the steps they had taken to address the concerns raised by the Information Commissioner.
- The Royal Free asked us to replace references to the "London hospital" in our initial draft of the Report with refences to the "Royal Free hospital". We have made this amendment.
- DeepMind suggested we better clarify the areas of law that fell within the Scope of our Report. We revised the fourth bullet of paragraph 8.4 in light of those comments.
- DeepMind stated that Streams was originally populated by way of transfer of historic HL7 messages and HES data, not Commissioning Data Sets as originally stated. We have updated paragraph 10.6 to reflect this comment.
- Our initial draft of the Report stated that when a user switches to another App and back to Streams, they must reauthenticate themselves. This is correct. However, the initial report stated that the user could use Apple's TouchID to re-enter the App in this situation. DeepMind informed us TouchID cannot be used for this purpose. In any event, this issue is not relevant as the clinicians we spoke to at the Royal Free said TouchID was not enabled on their iPhones (see paragraph 11.5).
- Our initial draft could be read as suggesting we had conducted a historic review of testing conducted on Streams. This is not correct. Our Report does not include a historic audit of this issue. We have clarified this point at DeepMind's suggestion (see paragraph 14 and elsewhere in the report).
- Our initial draft of the Report stated that the NHS AKI algorithm had been "endorsed" by NHS England. DeepMind asked us to clarify that the use of this algorithm is mandatory (see paragraph 12.1).
- Our initial draft described four potential projects relating to Streams. DeepMind considers one of those projects to be commercially sensitive. We have therefore

omitted details of that project from this Report and supplied that information to the Information Commissioner separately. In any event, that project is only at a very early design stage, and is on hold pending the outcome of this Report so has limited relevance to our Report (see paragraph 13).

- Our initial draft stated that the Royal Free Information Governance Committee meets "two times"/"three times" a year (the reference to meeting twice a year was an error on our part). The Royal Free asked us to amend the Report to state this Committee should meet quarterly. We have made this amendment, subject to a caveat that it only met three times in 2017 (see paragraph 16.1).
- DeepMind asked us to amend our description of their Information Governance Board to state it meets once a month. We have done so. This is consistent with our audit of the Board's operation (see paragraph 17.1).
- DeepMind asked us to clarify that personnel with access to Streams had access rights that lasted between *one week* and six months. Our initial draft stated that access rights were between *one month* and six months. When we originally audited those access rights, the shortest period for which access was provided was one month. We have therefore amended the Report to simply state that access rights are for variable periods of up to six months (see paragraph 17.5).
- Our initial draft addressed some broader confidentiality issues that were not directly relevant to the use of Streams. We have removed those comments at the Royal Free's request (see paragraph 31).

We made other amendments independently to the initial draft of the Report. These amendments mainly relate to the legal analysis and to reflect the Governance interviews. We provided a further draft to the Royal Free (copied to DeepMind) on 16 March 2018 for submission to the Royal Free's board and a further revised draft on 23 March 2018.

6 Review of the Report by the Information Commissioner

We provided a copy of this Report to the Information Commissioner on 27 March 2018 in order to allow her to comment on the findings. We received comments from the Information Commissioner on 2 May 2018 and provided a further draft to the Information Commissioner on 10 May 2018.

Addendum to address the General Data Protection Regulation and the Data Protection Act 2018

On 17 May 2018, we issued our Report into the acute kidney injury detection system known as Streams. In accordance with the Undertakings, our Report considered whether Streams complied with the Data Protection Act 1998.

The Report made reference to the General Data Protection Regulation and the Data Protection Bill, but did not, and could not, come to any final conclusions about the lawfulness of Streams under this new regime. This is because the Data Protection Bill had not been agreed at the time we issued our Report.

The Data Protection Act 2018 subsequently received Royal Assent on 23 May 2018.[1] The purpose of this addendum is to update our findings in light of the General Data Protection Regulation and that Act.

This addendum only contains a legal analysis of the General Data Protection Regulation and the Data Protection Act 2018. We have not conducted a further audit into the Royal Free or taken steps to confirm if the recommendations in our Report have been implemented.

Like the Report, this addendum is limited to issues associated with Streams. It does not address the Royal Free's broader compliance with the General Data Protection Regulation and the Data Protection Act 2018.

Lawfulness of processing – Use of Streams

We consider that the processing of confidential patient information by the Royal Free for the operation of Streams is fair and lawful. It satisfies:

- a processing condition on the basis that it is either:
  - necessary to protect the vital interests of patients (see Article 6(1)(d) of the General Data Protection Regulation); or[2]
  - necessary for the exercise of the Royal Free's statutory functions (see Article 6(1)(e) of the General Data Protection Regulation, read in light of section 8(c) of the Data Protection Act 2018, which permits processing where it is for "*the exercise of a function conferred on a person by an enactment*"). The relevant statutory function is set out in section 43 of the National Health Service Act 2006;[3] and
- a special category personal data processing condition on the basis that it is necessary for health purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (Article 9(2)(h) and 9(3) of the General Data Protection Regulation, read in light of sections 10 and 11 and Schedule 1, para 2 of the Data Protection Act 2018, which specifically refers to this condition encompassing "*medical diagnosis*" and "*the provision of healthcare and treatment*"). Section 11 requires that the processing of health information is carried out: (a) by or under the responsibility of a health professional. This

[1] The majority of the Data Protection Act 2018 provisions came into force on 25 May 2018 by virtue of The Data Protection Act 2018 (Commencement No. 1 and Transitional and Saving Provisions) Regulations 2018.

[2] Footnote 56 of our Report addresses the question of whether it is possible to rely on more than one processing condition.

[3] Section 43 of the National Health Service Act 2006 expressly refers to the provision of "*goods and services for any purposes related to - (a) the provision of services provided to individuals for or in connection with the prevention, diagnosis or treatment of illness*".

would apply to the use of Streams by clinicians at the Royal Free;[4] or (b) by another person who, in the circumstances, owes a duty of confidentiality under an enactment or rule of law. This would apply to the DeepMind personnel as they are subject to an equitable duty of confidence imposed by rule of law.[5] There are also alternative arguments that this requirement is satisfied, which we do not explore further here.[6] [7]

The detailed analysis supporting these conclusions is set out in paragraph 23 of our Report. While that analysis addressed the Data Protection Act 1998, we consider the position under the General Data Protection Regulation and Data Protection Act 2018 is very similar and thus our detailed analysis is equally applicable (save for the specific points addressed above).

In particular, we consider that the processing of confidential patient information for the operation of Streams is "necessary"[8] for these purposes as Streams could not perform its functions without using confidential patient information, nor is it possible to achieve those purposes by less intrusive means (see paragraphs 23, 26 and 27 of our Report).

Lawfulness of processing – Testing of Streams

We consider the Royal Free's future use of confidential patient information for the testing of Streams will be fair and lawful so long as it is genuinely necessary for that purpose, minimised as far as possible and appropriate controls are in place. It would satisfy:

- a processing condition on the basis that it is:
  - necessary to protect the vital interests of patients (see Article 6(1)(d) of the General Data Protection Regulation). The testing is "necessary" to protect vital interests given the nexus between the testing and deployment of Streams, and the fact that clinical testing is likely to involve the actual use of Streams to detect AKI in patients alongside existing systems; or
  - necessary for the exercise of the Royal Free's statutory functions (see Article 6(1)(e) of the General Data Protection Regulation, read in light of section 8(c) of the Data Protection Act 2018, which permits processing where it is for "*the exercise of a function conferred on a person by an enactment*"). The relevant statutory function is set out in section 43 of the National Health Service Act 2006, read in light of section 250(6) of the Health and Social Care Act 2012 and the relevant standards issued under section 250(6); and

[4] The clinicians using Streams are all registered medical practitioners or registered nurses, so qualify as health professionals under section 204 of the Data Protection Act 2018.

[5] We consider that an equitable duty of confidence is imposed by "rule of law". For example, see *Crane v Sky In-Home Service Ltd* [2007] EWHC 66 in which a contractual right to terminate was found not to be a result of a rule of law. In contrast, a common law right to terminate for repudiatory breach was a result of a rule of law. In other words, the courts recognised that a "rule of law" need not be limited to a statutory obligation.

[6] See footnote 61 to our Report which addressed the question of whether processing by DeepMind is "by or under the responsibility of a health professional".

[7] Alternatively, this processing could be justified as being necessary for the exercise of the Royal Free's statutory functions (Article 9(2)(g) of the General Data Protection Regulation, read in light of section 10 and Schedule 1, para 6 of the Data Protection Act 2018 which permits processing where it is for "*the exercise of a function conferred on a person by an enactment*"). The relevant statutory function is set out in section 43 of the National Health Service Act 2006. Para 6(1)(b) of Schedule 1 contains an additional requirement that the processing be necessary for the substantial public interest, which we consider would be satisfied here given the very clear benefit of detecting AKI in a timely manner (see paragraph 9 of our Report for a discussion of the serious nature of AKI). However, this would require the Royal Free to have an appropriate policy (see Schedule 1, para 39 of the Data Protection Act 2018).

[8] See paragraph 22.8 of our Report for a discussion of the meaning of "necessary" under data protection law.

- a special category personal data processing condition on the basis that it is necessary for health purposes and is undertaken by a health professional or person subject to an equivalent duty of confidence (Article 9(2)(h) and 9(3) of the General Data Protection Regulation, read in light of sections 10 and 11 and Schedule 1, para 2 of the Data Protection Act 2018, which specifically refers to this condition encompassing "*management of health care systems*" as well as "*medical diagnosis*" and the "*provision of health care and treatment*"). The testing of Streams not only constitutes the management of health care systems but will also be "necessary for" medical diagnosis and the provision of healthcare given the nexus between the testing and deployment of Streams, and the fact that clinical testing is likely to involve the actual use of Streams to detect AKI in patients alongside existing systems. Finally, under section 11 the processing must be carried out by persons subject to an appropriate duty of confidentiality (see discussion above).[9]

The detailed analysis supporting these conclusions is set out in paragraph 24 of our Report. While that analysis addressed the Data Protection Act 1998, we think the position under the General Data Protection Regulation and Data Protection Act 2018 is very similar and thus our analysis is equally applicable (save for the specific points addressed above).

In particular, we consider that the processing of confidential patient information for the testing of Streams may well be "necessary"[10] for these purposes as: (i) it may not be possible to assure the correct functioning of Streams without using confidential patient information; (ii) there are measures are in place to minimise the use of confidential patient information for testing (see paragraphs 14.2, 14.3 and 14.5); and (iii) it may not be possible to achieve those purposes by other less intrusive means (see paragraphs 14.6 and 24 of our Report).

However, we recommend that the Royal Free documents its approach to the use of confidential patient information in testing as part of the data protection impact assessment for any future modifications to confirm the use of confidential patient information is indeed necessary (see paragraph 24.4 of our Report).

Data protection principles

Article 5 of the General Data Protection Regulation imposes an obligation on the Royal Free to comply with six data protection principles, namely:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation; and

[9] Alternatively, this processing could be justified as being necessary for the exercise of the Royal Free's statutory functions (Article 9(2)(g) of the General Data Protection Regulation, read in light of section 10 and Schedule 1, para 6 of the Data Protection Act 2018 which permits processing where it is for "*the exercise of a function conferred on a person by an enactment*"). The relevant statutory function is set out in section 43 of the National Health Service Act 2006, read in light of section 250(6) of the Health and Social Care Act 2012 and the relevant standards issued under section 250. Para 6(1)(b) of Schedule 1 contains an additional requirement that the processing be in the substantial public interest, which we consider would be satisfied here given the clear need to ensure Streams works properly before deploying it in a clinical environment. However, this would require the Royal Free to have an appropriate policy (see Schedule 1, para 39 of the Data Protection Act 2018).

[10] See paragraph 22.8 of our Report for a discussion of the meaning of "necessary" under data protection law.

- security, integrity and confidentiality (see also Articles 32 and 33[11] of the General Data Protection Regulation).

We have concluded that the Royal Free complies with those principles, subject to the recommendations set out below. The substantive analysis supporting this conclusion is set out in paragraphs 23 to 29 of our Report. While that analysis addressed the Data Protection Act 1998, we consider it is equally applicable under the General Data Protection Regulation and Data Protection Act 2018.

In relation to these data protection principles, our Report recommended that the Royal Free: (i) consider the handover procedure for iPhones; (ii) review its leaver and mover process; (iii) ensure staff complete mandatory training; and (iv) set a retention period (see paragraph 34.1 of our Report). These recommendations are equally applicable under the General Data Protection Regulation and the Data Protection Act 2018.

We understand the Royal Free has accepted these recommendations, but we have not conducted a further audit to confirm if they have all been implemented.

Individual rights

Individuals are granted a variety of rights under the General Data Protection Regulation.

Those rights include the right to make a subject access request, to object to the processing of their personal data and to ask that their personal data be erased (see Articles 15, 17 and 21 of the General Data Protection Regulation). We consider that the processes used by the Royal Free - set out in paragraph 28 of our Report - are capable satisfy those requests subject to: (i) the minor recommendations set out in paragraph 28; and (ii) other generic modifications to the process of responding to subject access requests arising out of the General Data Protection Regulation.[12]

We do not think the right to data portability applies as the processing is not carried out on the basis of the consent of, or contract with, the individual. We do not think the rights in relation to automated decision making would apply as the NHS AKI algorithm does not make decisions about individuals, but rather simply detects potential AKI and sends alerts to clinicians (Article 20 and 22 of the General Data Protection Regulation).

Our Report did not consider how the Royal Free would comply with individuals exercising their right to rectification and to restriction of processing, but we consider these rights to be of limited relevance to Streams[13] (Articles 16 and 18 of the General Data Protection Regulation).

Other obligations of the Royal Free

The Royal Free has other obligations under the General Data Protection Regulation to:

- provide additional information to individuals about the processing of their personal data (Articles 13 and 14 of the General Data Protection Regulation). Our Report recommended that the Royal Free update its privacy notice and do more to highlight that notice to patients visiting its hospital (see paragraph 25.3);

[11] A personal data breach affecting Streams would need to be recorded, and possibly reported to the Information Commissioner and data subjects, in the same way as any other personal data breach. However, this largely relates to the Royal Free's broader compliance and is not specific to Streams.

[12] For example: (i) subject access requests will be free; (ii) the time limit to respond to requests will be one month (extendable by two months in some cases); and (iii) the response should include the additional information set out in Article 15(1) of the General Data Protection Regulation. However, this largely relates to the Royal Free's broader compliance and is not specific to Streams.

[13] See, for example, paragraph 22.5 point 4 of our Report in relation to accuracy of personal data.

- appoint a data protection officer (Article 37 of the General Data Protection Regulation). This mainly relates to the Royal Free's broader compliance and so is outside the scope of our Report but is addressed briefly in paragraph 16.3 of our Report;
- conduct a data protection impact assessment on high-risk processing (Article 35 of the General Data Protection Regulation). Our Report recommends that data protection impact assessments are carried out prior to future developments of Streams (see paragraph 13 of our Report). That data protection impact assessment should address the Royal Free's obligations in relation to data protection by design and default (Article 25 of the General Data Protection Regulation);
- keep records about its processing (Article 30 of the General Data Protection Regulation). This mainly relates to the Royal Free's broader compliance and so is outside the scope of our Report but is addressed briefly in paragraph 27.2 of our Report; and
- ensure that personal data is not transferred outside the Union unless certain conditions are met (Articles 44 to 49 of the General Data Protection Regulation). This is not relevant as Streams does not result in the transfer of personal data outside the Union (see paragraph 10.10 of our Report).

DeepMind is a processor

We have concluded that DeepMind is a processor under the General Data Protection Regulation. The substantive analysis supporting these conclusions is set out in paragraph 20 of our Report. While that analysis addressed the Data Protection Act 1998, we consider it is equally applicable under the General Data Protection Regulation and Data Protection Act 2018.

We consider that the Royal Free's contract with DeepMind meets the requirements of Article 28 of the General Data Protection Regulation, subject to the contract being amended to contain an express obligation on DeepMind to inform the Royal Free if, in DeepMind's opinion, the Royal Free's instructions infringe data protection laws. Further detail is set out in paragraphs 19.2 and 29.3 of our Report. The Royal Free has accepted our recommendation to make this amendment.

Other obligations on DeepMind

DeepMind, as a processor, has more limited obligations under the General Data Protection Regulation. Those more limited obligations include:

- an obligation to keep personal data secure (see Article 32 of the General Data Protection Regulation). We have concluded that DeepMind complies with this security obligation, subject to a minor recommendation regarding remote access (see paragraph 17.7 of our Report). The substantive analysis supporting this conclusion is set out in paragraph 29 of our Report. While that analysis addressed the Data Protection Act 1998, we consider it is equally applicable under the General Data Protection Regulation and Data Protection Act 2018;
- the appointment of a data protection officer (see Article 37 of the General Data Protection Regulation). We noted that DeepMind had identified a suitable candidate, but we have not confirmed that the appointment has taken place (see paragraph 17.4 of our Report);
- the maintenance of certain records (see Article 30 of the General Data Protection Regulation). We did not confirm if DeepMind had prepared such records as part of our audit as there was no obligation on DeepMind to hold them at that time. In any event, the record keeping obligations are limited so we do not consider this to be a material issue; and

- ensuring that personal data is not transferred outside the Union unless certain conditions are met (Articles 44 to 49 of the General Data Protection Regulation). This is not relevant as Streams does not result in the transfer of personal data outside the Union (see paragraph 10.10 of our Report).

Other issues

This addendum uses the same defined terms as our Report (see Annex 1).

The provisions of paragraph 8 and Annex 3 to our Report apply to this Addendum.

Linklaters LLP

7 June 2018