Key Q&A for media

What's different about this agreement compared to the previous? Is DeepMind being provided with more data?

- The types of patient data being shared are broadly the same as the previous agreement, with minor changes – for example, making it easier to see which patients are on dialysis (to prevent the app sending out false positive alerts)
- We estimate that around 2 million records will be processed
- In many cases these aren't complete patient histories, of course – it's often as simple as a single blood test

Isn't it unusual for a commercial company to have access to so much patient data?

- No, DeepMind is not able to process this information for any other purpose, other than streaming it to a nurse or doctor at the right time. They can't do anything else with it whatsoever.
- Data processing by third parties is an essential part of modern healthcare.
- Clinicians need fast access to patient medical information, and the NHS doesn't have the ability to process data in-house in this way.
- NHS trusts therefore routinely work with third party data processors like DeepMind, just as they work with external providers of a range of essential services that keep hospitals running smoothly.
- Other organisations currently processing large amounts of data for the NHS include TPP, which provides data processing services for GP surgeries and process the data of 26m patients (source) and Cerner, which has provided data processing for 22 NHS trusts (source).

When will Streams roll out to clinicians? How many clinicians will get it?

- We'll soon be conducting final clinical acceptance testing to demonstrate the app's functionality and identify any minor bugs that need fixing
- We're then aiming to roll out Streams AKI in early new year to the nephrology team at RFH encompassing dozens of staff.
- As other functions are developed, as per the roadmap, we hope to make these available to other clinical care teams

Will Streams replace any existing clinical systems?

- No. Streams is designed to supplement, not replace, existing hospital systems, so none will be turned off
- Clinicians will still be able to access information using the existing clinical systems if ever required

What permissions have you sought before you share additional data/use the data for purposes other than detecting AKI?

- The new agreement supersedes the old and a new information processing agreement has been signed to cover data processing under the new agreement
- We're confident that this adheres to data protection best practice
- We've also kept the ICO informed of our work throughout

How is patient data protected?

- Patients have the right to know that their health data is processed appropriately, and is handled with the utmost care and respect. We always have, and always will, hold ourselves to the highest legal and ethical standards. This includes working with trusts and regulatory bodies to obtain all approvals for any work we undertake. We rigorously train all of our staff to understand and abide by information governance for direct care and health research applications.
- The issue of data security is one we take seriously.
- For the clinical application we're developing, it has to present clinicians with all the necessary patient information required for them to make an accurate diagnosis and determine the right treatment. This information includes historical medical data such as previous illnesses and operations, allergies and previous blood tests results that can be compared to more recent blood tests.
- In order to process this data, we first copy it from the Royal Free's systems to DeepMind's NHS Digital approved data centre located in the UK. This is done over an end-to-end encrypted link, which itself is carried over a VPN. Either of these alone would be sufficient to

prevent eavesdroppers or man-in-the-middle attackers to intercept the data - both together give extra assurance.

- Once in DeepMind's data centres, the data is stored in an encrypted database and only decrypted when it is needed for processing. The decrypted data and data derived from it is never stored on disk without first being re-encrypted. Data transmitted between machines is also end-to-end encrypted, and all equipment is physically secured within a locked cage. All backups within the systems are also conducted over secure, encrypted links.
- Every access to patient data is logged. Those logs are regularly reviewed by the DeepMind Information Governance team to ensure that accesses are legitimate, as well as being open to review by our partners at the Royal Free and DeepMind's Independent Reviewers.
- Similarly, all software used to process the data is subject to both internal review by our software engineers and security teams, and external oversight by our Independent reviewers.
- Once data is no longer required, DeepMind permanently delete it from their systems. Where applicable, they also destroy any encryption keys associated with that data. Any storage device that is retired from service in DeepMind's data centre is physically destroyed to ensure there is no possibility of data leakage or recovery.

What about the danger of a cyberattack?

- The system has undergone rigorous third-party penetration testing, which means we've hired expert security consultants to use the latest technology to attempt to break into our systems, and no security flaws were found
- DeepMind uses the most advanced data protection and security technology in the world to secure patient data and monitor relevant security alerts and react appropriately
- We continually review and improve our security practices, both proactively and in response to new threats

Doesn't giving hundreds of clinicians access to sensitive data on their mobile phones constitute a huge data security risk?

- Not at all. Many large organisations operate this way these days. It's very common and standard best practises have been developed over many years.
- All devices have to be compliant with the trust's device management policy, which means the data can be deleted remotely
- You need to login to the app with a standard trust username and password in order to use it

- The data is streamed to the phone, rather than being permanently stored on the device, which means it is securely and remotely managed
- The user is automatically signed out of the application after a period of inactivity
- Our audit process will further ensure patient data is protected and only accessed by those people who need it

What happens at the end of the five year partnership?

We may continue to work together, if both parties agree, when this agreement ends. Our agreement lasts until 2021, before which date the data will be passed back to the Trust or destroyed unless the agreement is extended.