# Privacy Impact Assessment Google DeepMind Streams at Royal Free London NHS Foundation Trust

| | |
|---|---|
| **Document Reference Information** | |
| **Version** | **0.1** |
| **Status** | **Draft** |
| **Author/Lead** | [redacted] |

| Version | Description of Change(s) | Reason for Change | Author | Date |
|---|---|---|---|---|
| 0.1 | Initial Draft | | [redacted] | 19 July 2017 |

**Other relevant documents to this Strategy:**
Integrated Risk Management Framework
Standing Orders & Standing Financial Instructions
Incident Reporting Policy
Serious Incident Policy

## Table of Contents

# Introduction

This document provides details of the PIA conducted into Streams. Full details are available in the Information Commissioner's handbook.

Privacy Law compliance checks and Data Protection Act compliance checks are part of the PIA process – the questions to assess this are included in this document.

All questions have been completed with as much detail as possible and this document is available on the Data Sharing Portal.

Further guidance on specific items can be found on the Information Commissioner's website.
http://www.ico.gov.uk
Reference information:
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html

## Section 1 – New/Change of System/Project General Details

| | | |
|---|---|---|
| **Name:** | Google DeepMind Streams | |
| **Objective:** | The objectives of Streams are | |
| **Background:**<br>**Why is the new system / change in system required?** | Streams is a secure instant alert app, addressing what clinicians call “failure to rescue”, when the right nurse or doctor doesn’t get to the right patient in time. Each year, many thousands of people in UK hospitals die from conditions like sepsis and acute kidney injury, which are preventable, because the warning signs aren't picked up and acted on in time. | |
| **Benefits:** | Streams quickly reviews test results for serious issues, such as acute kidney injury. If one is found, the system sends an urgent secure smartphone alert to the right clinician to request help, along with information about previous conditions so they can make an immediate diagnosis.<br><br>Streams puts the data securely into the clinician’s hands rather than keeping it on desktops in silos thereby allowing it to be viewed earlier so that clinical intervention can take place earlier thus minimising patient deterioration.<br><br>The Streams app allows clinicians to chat securely and collaborate in the treatment of patients via a chat facility, avoiding duplication of effort but allowing extra help when needed. | |
| **Constraints:** | Streams is dependent on the real time feed from the Royal Free London integration engine to provide timely alerts and patient results.<br><br>The Streams app is dependent on WiFi or mobile data signal.<br><br>The Streams app is currently only available on trust supplied iPhone 6s. | |
| **Relationships:**<br>**(For example, with other Trust’s, organisations)** | Streams has been developed in collaboration with Google DeepMind | |
| **Quality Expectations** | The Streams application is expected to be of very high quality and availability, and has been implemented in accordance with NHS Digital SCCI0129 and 160 Clinical Risk Management Standards.<br><br>The iPhone app used by clinicians is CE Kite Marked.<br><br>Google DeepMind is ISO27001 certified.<br><br>Extensive input from clinicians during the design assures the app is safe and usable with minimum training required. | |
| **Cross reference to other projects:** | Streams has been previously called ‘Waking Project’ | |
| **Project Manager:** | Name: | [redacted] |
| | Title: | Project Manager |
| | Department: | IM&T |
| | Telephone: | [redacted] |
| | Email: | [redacted] |

| | | |
|---|---|---|
| **Information Asset Owner:** | Name: | [redacted] |
| | Title: | Consultant Nephrologist |
| | Department: | Nephrology |
| | Telephone: | [redacted] |
| | Email: | [redacted] |
| **Information Asset Administrator:** | Name: | [redacted] |
| | Title: | Head of Systems Integration |
| | Department: | IM&T |
| | Telephone: | [redacted] |
| | Email: | [redacted] |
| **Customers and Stakeholders:** | Patients with tests carried out in diagnostic services used by Royal Free London NHS Foundation Trust (Pathology and Radiology)<br>Royal Free London NHS Foundation Trust NHS Foundation Trust Staff<br>Google DeepMind | |

## Section 2 – Privacy Impact Assessment Key Questions

| Question | Response |
|---|---|
| **1. Will the system /project/process (will now be referred to thereafter as 'asset' contain personal identifiable data or sensitive date** | ☐No<br>☑Patient<br>☑Staff<br>☐Other (specify) |
| **2. Purpose for the collection of the data. for example, patient treatment, health administration, research, audit, staff administration** | The data is not collected by Streams. DeepMind are processor acting on behalf of the Royal Free London. The data is collected by the RFL trust systems and processed by Streams.<br><br>The purpose of processing the data is to put the data into clinician's hands rather than keeping it on desktops in siloed systems. so allowing clinical decision making, alerting and patient location to be known at the point of care which is the prime objective of the Streams application in ensuring and improving patient safety.<br><br>Despite the introduction of a national algorithm for alerting the presence of Acute Kidney Injury in England and Wales the condition continues to afflict a large number of inpatients, in the worst cases causing death or chronic disease.<br><br>A reason for this is that often the alert, when generated, is not brought to the attention of a suitably qualified clinician in a timely manner. This is critical since the condition is highly time sensitive and can cause the patient condition to rapidly deteriorate without the correct clinical response. This has significant implications for the long term health of the patient and cost to the NHS.<br><br>This is well documented, and the vision of this service is to improve outcomes of patients with AKI by providing the AKI alert to the correct clinician at the right time.<br><br>Streams allows patient clinical records to be viewed quickly away from the desktop systems providing faster access, improving safety and increasing productivity. |
| **3. Does the asset involve new privacy-invasive technologies.<br>e.g. visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic** | ☐Yes<br>☑No<br>If yes, please give details: |
| **4. Please tick the data items that are held in the system** | |
| **Personal** | ☑Name Address<br>☑Post Code<br>☑Date of Birth |

| | |
|---|---|
| | ☑GP<br>☑Consultant<br>☑Next of Kin<br>☑Hospital No.<br>☑Sex<br>☑NHS Number<br>☐National Insurance Number |
| **Sensitive** | ☑Treatment Dates<br>☑Sex<br>☑Diagnosis<br>☑Religion<br>☐Occupation<br>☑Ethnic Origin<br>☑Medical History<br>☐Other (please state here): |
| **5. Will the asset collect new data items which have not been collected before?** | ☐Yes<br>☑No |
| **6. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and / or sensitive data for this asset?** | The information is being shared according to clinical requirements from the project clinical board which is led by a Royal Free London NHS Trust Senior Consultant to ensure patient safety and provide doctors with the tools to respond to alerts and request for their clinical guidance. |
| **7. Does the asset involve new or changed data collection policies that may be unclear or intrusive?** | ☐Yes<br>☑No |
| **8. Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number?** | ☑Yes<br>☐No<br>Data Protection Act Notification Number: ZA216865. Note this is only in relation to the user data held by DeepMind, not the patient data it processes of which the trust is the controller. |
| **9. Is the third party contract / supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?** | ☑Yes<br>☐No |
| **10.Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003** | ☑Yes<br>☐No |

| | |
|---|---|
| **11. Who provides the information for the asset? Others – please specify e.g. Interface from another asset** | ☑Patient<br>☑Staff<br>☐Others – please specify |
| **12. Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?** | ☐Yes<br>☑No |
| **13. If yes, how will that consent be obtained? Please state:** | Not Applicable |
| **14. Have individuals been informed of and have given their consent to all the processing and disclosures?** | ☐Yes (Explicit)<br>☑No<br><br>The sharing of data is to provide direct care and therefore consent is implied. |
| **15. How will the information be kept up to date and checked for accuracy and completeness?** | The information is updated in real time from the Royal Free London NHS Trust Integration Engine. |
| **16. Who will have access to the information?** | The information will be accessible to Royal Free Clinicians and Nurses who have been given access on the Royal Free London NHS Trust's instance of Microsoft Active Directory access control.<br><br>The Trust is in complete control of the accounts that are permitted to access the Streams application. Whenever a user tries to sign in to the app, they are authenticated against the Trust's LDAP servers and only allowed to proceed if an account with the appropriate privileges exists for them.<br><br>The application will log user access and certain usage details. Note that this is a 'read-only' application, with no data entry and no ability to update or change the underlying data.<br><br>DeepMind system administrators will have access purely for rectifying issues escalated to them by the RFL service desk.<br><br>**DeepMind staff training & related contractual obligations**<br>Measures are in place to educate and train staff on information governance. These are linked to disciplinary procedures for failure to adhere. In addition, DeepMind has placed contractual obligations on employees to ensure the protection of any personal data that they come into contact with.<br>• All members of the DeepMind Health team undergo HSCIC IG training and are subject to ongoing monitoring and auditing. Only a small subset of these employees have any access to the Trust's data for testing and administrative purposes.<br>• All DeepMind employees sign an extensive confidentiality agreement, and have confidentiality obligations in their |

| | |
|---|---|
| | employment agreements. The activity monitoring measures in place would allow sufficient evidence to be gathered to take a non-compliant employee to court. |
| **17. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?** | ☐Yes<br>☑No |
| **18. If applicable are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?** | Not applicable |
| **19. Is automated decision making used? If yes, how do you notify the individual?** | ☐Yes<br>☑No |
| **20. Is there a useable audit trail in place for the asset. For example, to identify who has accessed a record?** | ☑Yes<br>☐No<br><br>The Streams application maintains logs of all accesses to the system data. |
| **21. Have you assessed that the processing of personal/sensitive data will not case unwarranted damage or distress to the individuals concerned? What assessments has been carried out?** | ☑Yes<br>☐No<br>The processing of the personal/sensitive data is purely for the purpose of providing direct care. |
| **22. What procedures are in place for the rectifying/blocking of data by individual request or court order?** | Patients are able to write to the trust Information Governance Manager. On receipt of the request to block the processing of data the request is recorded in a log and passed to the system administrator in a secure directory.<br><br>The system manager confirms deletion of the patient's information and that future transfers of data are blocked.<br><br>This confirmation is fed back to the patient. |
| **23. Does the asset involve new or changed data access or disclosure arrangements that may be unclear?** | ☐Yes<br>☑No |

| | |
|---|---|
| **24. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data becomes more readily accessible that before? (for example, from paper to electronic via the web?)** | ☐Yes<br>☑No |
| **25. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management: NHS Codes of Practice)** | The information is retained according to the NHS guidlelines. |
| **26. How will the data be destroyed when it is no longer required?** | The data will be deleted from the system database and backups will be deleted once the retention period is passed. |
| **27. Will the information be shared with any other businesses?** | ☐Yes<br>☑No |
| **28. Does the asset involve multiple businesses whether public or private sector?** | ☐Yes<br>☑No |
| **29. Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?** | ☑Yes<br>☐No<br>Streams provides the ability for clinicians to view pathology from both RFH and BCF side-by-side which was not previously possible. |
| **30. Where will the information be kept/stored/accessed?** | ☐On paper<br>☐On a database saved on a network folder/drive<br>☐Website<br>☑On a dedicated system saved to the Network<br>☐Other – please state below: |
| **31.Will any information be sent offsite<br>If yes where is this information being sent.** | ☑Yes<br>☐No<br>The service is hosted within a secure England-based data centre which complies with HSCIC data security standards and is independently certified to ISO20000 (IT Service Management), ISO27001 (Information Security Management), and ISO9001 (Quality Management) standards.<br><br>Measures to secure the data include:<br>• The data is encrypted at rest using AES256 and in transit using TLS.<br>• No connection exists between DeepMind Health network and the Google corporate network.<br>• Access to the data centre is strictly controlled. |

| | |
|---|---|
| **32.Please state by which method the information will be transported** | ☐Fax<br>☐Email<br>☐Via NHS Mail<br>☐Website<br>☐Via Courier<br>☐By Hand<br>☐Via Post – internal<br>☐Via Telephone<br>☐Via Post – external<br>☑Other – please state below:<br>HL7 messages over dedicated N3 VPN between trust integration engine and Streams message handler. |
| **33. Are you transferring any personal or sensitive data to a country outside the UK?**<br>**If yes, where?** | ☐Yes<br>☑No |
| **34. What is the data to be transferred outside the UK?** | Not applicable |
| **35. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?** | ☐Yes<br>☐No<br>☑Not Applicable |
| **36. Have you checked the country has a adequate level of protection for data security?** | ☐Yes<br>☐No<br>☑Not Applicable |
| **37. Is there a system level security policy in place for the asset?** | ☑Yes<br>☐No |
| **38. Has an information risk assessment been carried out and reported to the Information Governance Lead? Where there any risks highlighted? Please provide details and how these will be mitigated?** | ☑Yes<br>☐No<br>**Data Breach Risk**<br>Should a breach occur the system is designed to mitigate the potential damage to data security including:<br>• Encrypted drives within the data centre. If the data was stolen it would be inaccessible away from the data centre.<br>• The Mobile devices are managed by AirWatch and can be locked and wiped as soon as a loss or theft is reported.<br>• Only LDAP authenticated users have access. If a user is suspected of abusing their access rights the Trust can disable their access.<br>Logging of activity would allow an individual's activity to be investigated and provide evidence in the case that the individual is prosecuted.<br><br>**Unauthorised Access**<br>The Trust is in complete control of the accounts that are permitted |

| | |
|---|---|
| | to access the Streams application. Whenever a user tries to sign in to the app, they are authenticated against the Trust's LDAP servers and only allowed to proceed if an account with the appropriate privileges exists for them.<br><br>The application will log user access and certain usage details. Note that this is a 'read-only' application, with no data entry and no ability to update or change the underlying data.<br><br>**Data Security Breach on Mobile Device.**<br>Data is sent over a TLS connection from the data centre to the mobile devices held by clinicians. The Mobile Devices are Trust owned and provisioned with AirWatch mobile device management system which the Trust has implemented. The AirWatch configuration for mobile devices for this service enables:<br>• Remote wiping<br>• Geolocation of device<br>• Blocking device use<br>• Installation of critical security updates.<br><br>**Data Insecure in Transit**<br>Data from Royal Free Hospital is streamed from the Trust over an encrypted N3 connection between fixed IP end-points. |
| **39. Is there a contingency plan/backup policy in place to manage the effect of an unforeseen event?**<br>**Please provide a copy.** | ☑Yes<br>☐No<br>All data shared with Streams is backed up by the Royal Free London NHS Foundation Trust IT Department in accordance with its IGSoC submission. All data shared with Streams is accessible through the trust's own IT systems in the event of Streams not being available.<br><br>Contingency planning at DeepMind is detailed in the attached documentation. |
| **40. Are there procedures in place to recover data (both electronic/paper) which may be damaged through:**<br>**Human Error**<br>**Computer virus**<br>**Network failure**<br>**Theft**<br>**Fire**<br>**Flood**<br>**Other disaster**<br><br>**Please provide policy titles** | ☑Yes<br>☐No<br>**Safeguards in Place to Mitigate a Data Breach**<br>Should a breach occur the system is designed to mitigate the potential damage to data security including:<br>• Encrypted drives within the data centre. If the data was stolen it would be inaccessible away from the data centre.<br>• The Mobile devices are managed by AirWatch and can be locked and wiped as soon as a loss or theft is reported.<br>• Only LDAP authenticated users have access. If a user is suspected of abusing their access rights the Trust can disable their access.<br>Logging of activity would allow an individual's activity to be investigated and provide evidence in the case that the individual is prosecuted.<br><br>Recovery planning at DeepMind is detailed in the attached documentation. |

| | |
|---|---|
| **Form Completed by:** | Name [redacted]<br>Title Project Manager<br>Signature<br>Date |
| | |

## Section 3: Evaluation

| | |
|---|---|
| **41. Is the PIA approved?** | □Yes<br>□No |
| **42. If not, please state the reasons why and action plan put in place to ensure the PIA can be approved including any timeframes.** | |
| **43. Information Governance Committee Approval.** | **Name**<br>**Title**<br>**Signature**<br>**Date** |

**Appendix – Glossary of Terms**

| Item | Definition |
|---|---|
| **Personal Data** | This means data which relates to a living individual which can be identified:<br>A) from those data, or<br>B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.<br><br>It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual |
| **Sensitive Data** | This means personal data consisting of information as to the:<br>A) racial or ethnic group of the individual<br>B) the political opinions of the individual<br>C) the religious beliefs or other beliefs of a similar nature of the individual<br>D) whether the individual is a member of a trade union<br>E) physical or mental health of the individual<br>F) sexual life of the individual<br>G) the commission or alleged commission by the individual of any offence<br>H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings |
| **Direct Marketing** | This is "junk mail" which is directed to particular individuals. The mail which are addressed to "the occupier" is not directed to an individual and is therefore not direct marketing.<br>Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you.<br>Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity. |
| **Automated Decision Making** | Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned. |
| **Information Assets** | Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware. |
| **SIRO (Senior Information Risk Owner)** | This person is an executive who takes ownership of the organisation"s information risk policy and acts as advocate for information risk on the Board |
| **IAO (Information Asset Owner)** | These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they „own" and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the |

| | |
|---|---|
| | assets under their control/area. |
| **IAA (Information Asset Administrator)** | There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers |
| **Implied consent** | Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure. |
| **Explicit consent** | Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information. |
| **Anonymity** | Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients. |
| **Pseudonymity** | This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. |
| **Information Risk** | An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information. |
| **Privacy Invasive Technologies** | Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk |
| **Authentication Requirements** | An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks. |
| **Retention Periods** | Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives. |

| | |
|---|---|
| **Records Management: NHS Code of Practice** | Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule. |
| **Data Protection Act 1998** | This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must:<br><br>with those purposes.<br>loss, destruction or damage.<br>unless that country or territory protects the rights and freedoms of the data subjects. |
| **Privacy and Electronic Communications Regulations 2003** | These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information. |