Streams Project Privacy Impact Assessment

Description: Streams Project

To develop a service which notifies suitably qualified clinicians of patients experiencing Acute Kidney Injury. The Streams project has previously been referred to as the 'Waking' project.

Questions to identify Privacy Issues	Answer
Technology	
(1) Does the proposal include the use of new or additional technologies with the potential for privacy intrusion?	**Infrastructure** The service will provide and deploy: • An app to run on smartphones. The app will provide two functions, both facilitating the direct care of patients: o for receiving alerts to specific trust employed clinicians to assist in the treatment of inpatients.. o for enabling specific trust employed clinicians to display pathology results to assist in the treatment of inpatients. • The app will communicate with the webserver via a secure API. • A secure web based dashboard only accessible to suitably authorised clinicians. • A data repository provisioned by an existing ADT and Pathology HL7 data feed from the hospital integration engine. The platform uses industry standard technologies with good security reputations. **Medical Device Classification** The Streams device when CE marked will be classed as a **Class I, non-measuring, non-sterile active device** based on the advice given in the European Commission Guidance on Medical Devices (MEDDEV 2.1/6 - '3. Classification of stand alone software'). Streams is an active device as it falls within the definitions of Article 1(2)(a) in the Medical Device Directive 93/42/EEC. The device is Class I, non-measuring as it falls under Rule 12 of Annex IX in MDD 93/42/EEC. DeepMind are in the process of putting together their technical file prior to CE marking their device in preparation for putting the device into production. **Future implications of the technology** The device will be used initially by a small number of clinicians. We expect the number of users within the Trust to rise if the device delivers clinical benefit.

(2) **Justification** Is the justification for the new data-handling unclear or unpublished?	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. 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. 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.
(3**)** **Identity**: Does the project involve an additional use of an existing identifier?	The key demographic data items: NHS Number, MRN, Patient name and DOB will be used to positively identify the patient. This will be used to allow comparison between pathology results obtained within the hospital. There will be no combination with other demographic data or linkage of data obtained from disparate sources.
(4) **Identity**: Does the project involve use of a new identifier for multiple purposes?	The service does not involve use of a new identifier for multiple purposes.
5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?	The service does not involve new or substantially changed authentication requirements with the exception that the clinician will have the option to authenticate by fingerprint to unlock the smartphone.
Data	
(6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?	The service will use data from the following existing source systems: **EPR**: Contains Demographics to allow matching of results with the correct patient. Historic Episode data including previous diagnoses and procedures. **VitalData:** List of patients receiving dialysis who are excluded from the service. **Winpath & HNAM**: Pathology. Provides biochemistry results required by the AKI algorithm.

	POC: Pathology. Provides biochemistry results required by the AKI algorithm from Point of Care analysers. **RIS:** Radiology reports e.g. CTKUB and ultrasound renal tract. **Opt-out list:** Patients who have dissented from their data being shared with DeepMind.
(7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?	The service focuses on inpatients and Emergency Department patients within the hospital trust and also includes non-inpatient historic blood test data e.g. outpatient/GP to provide baseline reference data should these patients be admitted in the future.
(8) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?	Yes, Streams now provides the ability for clinicians to view pathology from both RFH and BCF side-by-side which was not previously possible.
Data Handling	
(9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?	All data used is already being collected for the treatment of the patients.
(10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?	The service will re-use existing data from a number of source systems, including Laboratory Information Systems, EPR, POC systems, VitalData. The algorithm will use this data to determine the AKI level of inpatients. The service will not change any of the underlying data, or attempt to over-write any of the source systems. There are no proposed changes to existing standards on data quality.
(11) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?	Every effort has been made to ensure that the measures to secure the data maintains or exceeds those in place to protect the data within the source systems. **Security of Data Located on System Servers** 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. Measures to secure the data include: • The data is encrypted at rest using AES256 and in transit using TLS. • No connection exists between DeepMind Health network and the Google corporate network. • Access to the data centre is strictly controlled. **Staff training & related contractual obligations** 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. • 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. • 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. **Security of Data in Transit** Pathology data is streamed from the Trust over an encrypted N3 connection between fixed IP end-points. **Security of Data Displayed on Mobile Devices.** 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: • Remote wiping • Geolocation of device

	• Blocking device use • Installation of critical security updates. **Authentication of Users** 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. 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. **Safeguards in Place to Mitigate a Data Breach** Should a breach occur the system is designed to mitigate the potential damage to data security including: • Encrypted drives within the data centre. If the data was stolen it would be inaccessible away from the data centre. • The Mobile devices are managed by AirWatch and can be locked and wiped as soon as a loss or theft is reported. • Only LDAP authenticated users have access. If a user is suspected of abusing their access rights the Trust can disable their access. • Logging of activity would allow an individual's activity to be investigated and provide evidence in the case that the individual is prosecuted.
(12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?	The service does not involve new or changed data access or disclosure arrangements.
(13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?	The service does not involve new or changed data retention processes that are out with existing NHS data retention practices.
(14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible	The service does not involve a new or changed medium or method of disclosure which would make information already within the public domain more accessible.

than before?	
Exemptions and Exceptions	
(15) Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?	The service will not give rise to new or changed data handling that is exempt from the Data Protection Act 1998.
(16) Does the proposal intend to disclose personal data to, or access by, third parties that are not subject to EU or comparable privacy regulation?	The data will not be transferred out with the UK, nor made available to third parties.