PRIVACY IMPACT ASSESSMENT (PIA)
DeepMind Technologies

1. Introduction

Taunton and Somerset NHS Foundation Trust are working with patients to bring digital technology to the bedside to improve care. In May 2017, the Trust signed a 5-year service agreement with DeepMind Technologies Limited (DeepMind) forming an anchor partnership to implement and develop, over a number of phases, a mobile application called Streams. This work will contribute to the Trust's digitisation obligations as a Global Digital Exemplar (GDE) site.

The introduction of mobile technology into the live clinical environment has the potential to deliver significant improvements to the quality and safety of patient care. The "Streams Project" will provide viewing of pathology and radiology results on mobile devices, to inform clinical decision making at the bedside or on the move. The software will also have the ability to flag up patients at risk of Acute Kidney Injury (AKI) and it will also be the platform on which the patient's clinical observations will be captured and displayed electronically.

The Streams application will display information contained within the existing Electronic Patient Record (EPR) held in Maxims, pathology and radiology results feeds. This information is already available to clinicians but requires them to access a desktop computer, or check a paper record. Computers are in short supply and located away from the patient bedside. These barriers can prevent timely access to this information and often result in clinicians transcribing results into multiple parts of the medical record (Principle c and d of the GDPR, Data Protection Act 2018(DPA)).

The Streams application will be used for patients who meet the following criteria:

- Attendance to A&E or pending ambulance attendance.
- Any inpatient admission at Taunton and Somerset NHS Foundation Trust.

For Streams to function, personally sensitive data of patients being treated in the Trust will need to be uploaded to, and held within, the DeepMind data centre, with DeepMind acting as a Data Processor on behalf of the Data Controller: Taunton and Somerset NHS Foundation Trust. The scope of the data upload is restricted to inpatients and A & E attendances under the care of the Trust and any change in data transfer scope will be further defined within future Privacy Impact Assessments (PIA) issued by the Trust. It is important to stress that the re-surfacing and representation of this information via Streams, and identification of potential kidney injury is the limit of the data processing that is permitted under our agreement with DeepMind Technologies Ltd. Any further processing, other than as expressly instructed by the Trust, would be in breach of the service agreement and therefore the Data Protection Act (Principle b, c, d of the GDPR, DPA).

Clinicians are already able to view all results via an existing OrderComms system from both primary and secondary care, regardless of where those results originated. This is enabled by an existing agreement between the Data Controllers, Yeovil District Hospital NHS Foundation Trust, Taunton and Somerset NHS Foundation Trust, Somerset Partnership NHS Foundation Trust and individual

Somerset GP practices. This allows the Trust, as owner of the OrderComms system, to process this data on their behalf. The Trust, as a processor of the external organisations data, is not able to share the data that it does not own without permission from the Data Controllers. Data sharing agreements with Somerset Partnership and Yeovil District Hospital, to be able to present this same information via Streams, are in place to transfer data for this specific use. The Trust is actively pursuing the development of data sharing agreements with all Somerset GP practices, as individual Data Controllers, however until these additional agreements are established no GP generated results will be provided to DeepMind for data processing (Principle a and b of the GDPR, DPA).

The Streams application will also enable the patient's clinical observations to be captured electronically at the bedside on mobile devices and be presented digitally. The observation data captured will be used to calculate a National Early Warning Score (NEWS2) which will be presented in line with National and Trust guidance. This data will then be plotted in a graphical format and presented back to the clinical staff to assist with monitoring the patient's condition. The observation data may also be printed through a web interface, hosted by DeepMind, using the same login system. This is designed to facilitate patient transfer, and to meet national guidelines for providing data for complaints and legal review. These application accesses will be recorded in an audit log and will be reviewed as part of the Trust's information governance process.

This iteration details the PIA for

1. Live data validation and piloting of the observations functionality
2. Live data validation and piloting of the Streams views functionality
3. Use of the Streams viewer and observations recording for direct patient care for all inpatients and A & E attendances.

2. Need for a Privacy Impact Assessment

The Trust recognises that the processing of data by third parties on its behalf presents potential data privacy risks and concerns for patients. The Trust's partnership with DeepMind has and will continue to generate a large amount of interest and speculative narrative from third parties. This PIA aims to provide transparency, clarity, and assurances surrounding the data privacy risks to patients. It will outline what patient data is to be transferred, why it is being transferred, and how it will be processed and held within the DeepMind data centre. The Trust is committed to continually assess the Privacy Risks of this partnership to ensure patient data is protected (Principle a, b and f of the GDPR DPA).

2.1 Previous PIA iterations

The following PIA's have been issued for this project and have all been available on the Trust public internet site:
April 2017 – initial PIA prior to signing a contract with DeepMind
November 2017 – prior to the initial test of transfer of anonymised data to the Streams
January 2018 – prior to the anonymised testing of the observation functionality and further testing of anonymised data transfer

2.2 Future PIA iterations

The Trust is committed to publishing updated iterations / addendums of the PIA prior to any changes in patient data transfer scope, irrespective of whether it is identifiable or anonymised patient data.

2.3 Patient and Public Engagement

Taunton and Somerset NHS Foundation Trust is committed to putting patients at the core of digital developments, enabling patients to work alongside clinicians to develop the best solutions for the delivery of their care.

The Trust has already actively involved patients in a number of design workshops, product review sessions, and planning events. Our Musgrove Partners are involved in the project at all key stages. A digital open day was held on 29th September 2017 in the centre of Taunton, which provided the opportunity for members of the public to discuss any element of digitisation, including data privacy, with the Trust digital team. Paper copies of the active PIA were available to the public at the event and the digital team were present to capture and discuss any concerns raised. There are ongoing events designed to enable the public to engage directly with the Trust team that oversees the Streams Project and its associated data transfer activities (Principle a and b, DPA). In addition we are working with the Clinical Commissioning Group, (CCG) participating in a number of engagement events including meetings with persons / patients and with patient participation groups across Somerset.

The Trust is aware that the PIA in its current form contains a large amount of technical information of which non-subject matter experts may find difficult to interpret. The Trust has produced "patient/public" version of the PIA prior to the transfer of patient identifiable data to DeepMind, both versions of the PIA will be maintained and published on the Trust website.

2.4 Scope of this PIA

This PIA is designed to cover the privacy risks associated with the transfer of patient data to DeepMind for the clinical validation, pilot and deployment of the Streams Application to view our patient's pathology and radiology results, digital recording and viewing of patient observations.

Recording and viewing of patient observations functionality

In March 2018, the Trust will commence the piloting of Streams for the capture of patient observations, the calculation of a National Early Warning Score (NEWS) and presentation of graphical trends of observations. The pilot will be used to confirm that the direct patient care that Streams is facilitating is clinically safe, operationally sustainable and safe guarding patient information. The pilot will be on a 40 bedded surgical ward. The stages of piloting and deployment will progress through the following 4 main stages;

Stage	Data Scope	Purpose
1.Clinical data validation	Live feed of PAS ADT and patient demographics	To ensure that data feeds are clinical accurate and safe
2. Dual entry pilot	Patient observations captured in Streams, live feed of PAS ADT and patient demographics and on paper	To ensure that new process is clinically safe. Data transferred for the pilot will be limited to that required for the designated pilot ward.
3. Stand-alone pilot	Patient observations captured only in Streams, live feed of PAS ADT and patient demographics	To ensure that process is clinically safe and sustainable
4. Deployment	Patient observations captured in Streams, live feed of PAS ADT and patient demographics	Transition safely to organisation wide digital observations signs capture

Viewing of patient pathology and radiology results functionality

The Trust will pilot the Streams Application for the viewing of all pathology and radiology results and presentation of graphical trends. The pilot will be used to confirm that the direct patient care that Streams is facilitating is clinically safe, operationally sustainable and safeguarding patient information. The pilot will be on a ward / Consultant Team. The stages of piloting and deployment will progress through the following 5 main stages;

Stage	Data Scope	Purpose
1.Anonymised Testing	Anonymised pathology and radiology data	To test the data transfer process and the matching process with ADT data
2. Clinical data validation	Live feed of pathology and radiology data	To ensure that data feeds are clinical accurate and safe.
3. Dual view Pilot	Patient pathology and radiology results are viewed in the streams application for patient care. In addition the results are viewed in the usual electronic systems for comparison	To ensure that new process is clinically safe
4. Standalone pilot	Patient pathology and radiology results are viewed in the streams application for patient care	To ensure that process is clinically safe and sustainable
5. Deployment	Patient pathology and radiology results are viewed in the streams application for patient care	Transition safely to organisation wide digital pathology and radiology viewing on a mobile platform

3. Risks

It is recognised that the data being transferred, stored and processed by DeepMind is sensitive personal data and as such the Trust had considered a range of privacy concerns and related risks.

The table below contains the Trust's assessment of the key privacy risks associated with identifiable patient data;

Risk Description	Considerations & Mitigations
Data Security Breach Given the nature, sensitivity and volume of personal data involved, the consequences of any security breach could be very serious in terms of patient privacy (Principle f of the GDPR, DPA)	The Trust has a secure, locally managed data centre that is not accessible from any public network. Only authorised personnel have access to the resources within the datacentre. The Trust adheres to industry best practices regarding security and is currently seeking ISO 27001 accreditation. The Trust has carried out due diligence on DeepMind and the proposed DeepMind data centres to ensure that they meet the required security standards and that the correct policies and procedures are in place to ensure the safety of the data. Any transfer of data will be over secure NHS networks, to which the data centres are connected. The Trust has also ensured, by means of a written contract, that DeepMind can only use personal data on the instructions of the Trust and within the specific parameters of the agreed contract. This commits

	DeepMind to ensuring adequate technical and organisational data security measures. It should also be noted that DeepMind will store the Trust's patient data in England. The data will not be transferred outside of England. The Trust will undertake a regular review of its work with DeepMind to satisfy itself that those contractual and data security provisions are being complied with.
Use of patient data for other purposes Use of patient data outside of the terms agreed in the data sharing agreement could be considered a breach of the DPA (Principle b of the GDPR, DPA)	In order to ensure DPA compliance and maintain patients' trust, it is essential that the patient data provided to DeepMind will be processed for the purposes of providing data to the Streams application only, and not be used for any other purpose. The Trust's dialogue with DeepMind has resulted in a contractual agreement that this data may only be used for the purposes of data processing on behalf of the Trust. The data cannot be combined with other data, analysed outside of the boundaries of the services agreement (which includes an information processing agreement), or used for machine learning/AI. DeepMind cannot sell the data. If the Trust decides that any additional processing purposes are necessary, this would require a formal change of contract and as part of this process a new PIA would be developed to evaluate any associated risks.
Processing of excessive data Excessive volumes of data transfer could be considered a breach of the DPA (Principle c, DPA)	The Trust is mindful of the need to only process personal data to the extent that is needed for the intended clinical purposes of the Streams application, in compliance with contractual agreements and the DPA and not to process personal data for longer than is necessary. The Trust, in discussion with DeepMind, has carefully defined the data that is required for the application to function and specified the exact datasets which will be processed; this is set out in section 5. Additional patient demographics of address and GP will be sent to the DeepMind data centre but not surfaced in the Streams application in this iteration of the app. The patient address is required to allow clinically safe matching of patient records in the DeepMind data centre.
Inappropriate processing of personal data Data processing must be lawful under (Principle a of the DPA, Common Law and GDPR)	The Trust acknowledges the importance of ensuring that DeepMind's processing of personal data is not only fair and lawful, but that also conditions from Article 6 and 9 of the GDPR, DPA are met. The Trust is not soliciting for patient consent at this stage. Therefore, alternative conditions must be satisfied if DPA compliance is to be secured. The Trust is confident that Article 6 condition 6(1)(e) is satisfied. If the Trust is to discharge its statutory function under section 43 of the NHS Act 2006 effectively, it needs to ensure that it delivers patient care services to the best of its ability. The opportunity presented by technological developments, including this application, are reasonably necessary to ensure that these statutory functions are effectively discharged. It would be unreasonable for the Trust to turn down this

	opportunity to enhance the services it provides to the public, provided that its actions are lawful. On the same basis, conditions 9 (2)(h) (medical purposes) from Article 9 are also satisfied. The Trust has been mindful of the sensitive nature of the personal data which will be processed. It is satisfied that, for the reasons summarised in this PIA, its processing is justified and proportionate. All organisations that process personal data must comply with the GDPR and with the DPA(2018). They must also comply with common law requirements including the duty of confidence. Respecting confidentiality is a key safeguard in protecting the rights, freedoms and interests of data subjects that are referred to in many of the GDPR conditions that are applicable in health and social care contexts. Organisations must have robust and demonstrable measures in place to ensure that its employees respect confidentiality in order to achieve GDPR compliance. The common law duty of confidence (confidentiality) is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed: • Consent – whether express of implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected) • Authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings. • Overriding public interest, for example where a patient is contagious or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality The Trust has concluded that this arrangement is lawful under the DPA (2018) and also under the GDPR.
Reduction in patient/public confidence in Trust approach to data protection Patient/public confidence in the Trust will be undermined if they are not assured that personal data is being protected. (Principle a and b of the GDPR, DPA)	Patients need to be assured that the Trust, working with DeepMind as its Data Processor, is using their personal data fairly, lawfully, confidentially and for permissible purposes. As outlined in this PIA, the Trust is confident that any such concerns on the part of patients will be addressed comprehensively to provide the necessary reassurances for the genuine intentions for this partnership. Doctor-patient confidentiality will be preserved, in that DeepMind will be acting strictly as a Data Processor on the Trust's instructions. There will be no further data disclosure to any additional controller or any other external party. The data will only be used for the purposes described in this PIA.
Withdrawal of consent Patients withdrawing consent for their data to be transferred to DeepMind data Centre (Principle a and b of the GDPR, DPA)	The Trust has considered whether patients could be offered the opportunity to opt out of, or object to, the processing of their data for the purposes of this application. If patients have concerns about their data being used in this way, they will be put you in contact with the Trust's Caldicott Guardian so that they can discuss this. Patients who do not want their information included may need to understand the potential ways in which their care could be disadvantaged.

	The Trust has already engaged with patients at both Trust wide and public facing events, as well as with individual patients that have raised specific objections. Through these activities the Trust has been able to explore their concerns and wishes. The aim of this engagement with regard to consent is to co-produce (between the Trust and patients) a process of informed consent for those patients who have concerns about data processing or sharing. Where the proposed use of the application represents a systemic change to the Trust's data processing arrangements and clinical process the Trust will consider the clinical safety implications and technical feasibility of running parallel systems combining "old" and "new" systems. As explained above, the Trust will ensure that its processing of data for the purposes of this application is adequately explained to patients to ensure that any concerns are addressed.
Misuse of data by staff The Streams application will provide Staff with a new way to access patient data. (Principle f of the GDPR, DPA)	Access to the data is robustly controlled and inappropriate access or misuse of the data constitutes serious misconduct and is robustly dealt with by the Trust. There is an electronically auditable trail of who has accessed what information. The Trust carries out regular audits of system access to detect and deter any wrongdoing. The Trust will continue to proactively review staff's use of electronic systems. The ability to view the data on the mobile application outside of the Trust is controlled internally by role-based access and this will form part of information governance audits.
Inappropriate storage of Data from mobile application Mobile devices have the functionality to take a screenshot and save the information.	The Streams application captures an audit trail of users that have taken screenshots and presents a visible warning to users that take a screenshot which states 'Your Trust does not allow screenshots of Streams. All screenshots are logged and these logs are shared with the Trust's Caldicott Guardian.
Information held within the PIA The PIA could contain information which makes data security more vulnerable.	This PIA provides transparency relating to the privacy risks associated with the DeepMind data processing arrangements and the details of processes such as safe storage and anonymisation. The Trust recognises that the collaboration with DeepMind will be scrutinised to a much greater extent than most data processing relationships within the NHS. However, it has been considered that the publication of certain information in the public domain could in turn weaken the Trust and/or DeepMind's ability to protect patient data. The scope and detail of the PIA will be reviewed at every stage of the project and its associated data transfers. The Trust will continue to seek advice from its partners, patients, and the Information Commissioner's Office (ICO) regarding the content that should and should not be

	disclosed.

Conclusion on privacy and data protection risks:

The Information Processing Agreement between Taunton and Somerset NHS Foundation Trust and DeepMind clearly defines the Trust as the Data Controller and DeepMind as the Data Processor. This position has been further explored and confirmed through the production of this PIA. Assurance has also been sought to clarify that patient data will only be used for the purpose of providing direct clinical care and that data will not be used in breach of the Data Protection Act for activities such as development of artificial intelligence, machine learning or research. The Trust has received the necessary assurances that DeepMind will only act as a Data Processor as defined within the Information Processing Agreement and the Trust will ensure that the agreement is complied with.

The Trust acknowledges the concerns that have been raised that DeepMind will have "unvetted access to patient data". Access to data will be closely monitored and tightly controlled. DeepMind, as Data Processor, have robust access controls in place regulated under their Information Governance Process. The Trust is committed to continuing to work, in collaboration, with the people it serves to provide information to the public in a format that clarifies the ways in which the data can and will be used and to demonstrate that the data is safely and legally held.

Through this PIA process the Trust would hope to demonstrate that unauthorised access to, or use of, the data for any activity that falls outside of the data sharing agreement would be in breach of the Trust's contract with DeepMind, its associated data sharing agreement and the Data Protection Act. The Trust will continue to provide assurance to the public that it is monitoring usage of its patient data.

The Trust will be targeting communications and engagement activities directly at patients both before and during the deployment of Streams. There will be information presented directly to patients outlining the system purpose, the processing of their information and how they raise privacy concerns and the process for consent withdrawal.

In summary, the Trust is committed to ensuring that the prospective processing arrangements with DeepMind are fair, lawful, justified, proportionate and otherwise in compliance with the DPA, doctor-patient confidentiality and the Trust's statutory and common law duties. The Streams application will enhance patient care substantially without causing unjustified interference with patients' rights to privacy and to the lawful processing of their personal data.

4. Data Transfer

4.1 Purpose of the data transfer

The transfer of anonymised data will enable the Trust and DeepMind to validate that the data messaging and matching processes (required to form accurate clinical records within the DeepMind data centre) are effective when data is provided in bulk.

The transfer of identifiable patient data to DeepMind will serve the sole purpose of enabling the safe, effective functioning of the Streams application for the delivery of direct patient care and the enabling of the Trust to complete defined elements of its statutory functions.

There are, approximately, an average of 7,500 admissions per month some of which will be readmissions and these patient records will already be held and updated as required for patient care.

4.2 Scope of data transfer

The full scope and detail of the data transfer of identifiable patient data to DeepMind is outlined below.

The transfer of live and anonymised patient data including patient demographics, admissions, transfer and discharge will be limited to patients who are admitted to the Trust. At the point of data transfer 3 years' worth of historical pathology and radiology data will be sent and after this any pathology and radiology update. The patient's observations will be recorded directly into the system.

All data generated by the Trust (See section 4.3) and only Pathology and Radiology data from the organisations that the Trust has a data sharing agreement with.

The rationale for this data transfer has been reviewed by the Chief Clinical Information Officers (CCIOs) to consider the clinical applicability and relevance of the data that is being utilised for clinical assessment of patients.

In the future, it may become apparent that patients who currently do not fit these inclusion criteria may need to be included. Patients excluded from the data transfer may be disadvantaged because their clinical data is not immediately available to clinicians managing their care, for example at the point of emergency presentation. At that point, it may be necessary to review the criteria for data transfer.

4.3 Data Sets and Data Sources

The table below details the source, associated data set and list of the individual data items that form the data set to be used within the Streams app:

Data Source	Data Set	Type of Data
IMS MAXIMS EPR	Demographic Data	● NHS Number ● Medical Record Number (MRN) ● Surname ● Forename ● Middle Name ● Title ● DOB ● Address ● GP Practice ● GP ● Date of death
IMS MAXIMS EPR	Activity data sets	● Admissions ● Transfers ● Discharges ● Responsible Health Care Professional
EMIS Order Comms	Pathology data sets	● Pathology results, taking into account the NHS National Laboratory Medicine Catalogue and NHS UK Read Pathology Bounded Code List (PBCL) ● Laboratory AKI calculation
CareStream RIS	Radiology reports	● Radiology textual reports (Results)

Direct Entry into the Streams application	Patient observations	The following patient observations will be captured: ● Respiration Rate ● Oxygen Saturations ● Inspired Oxygen FiO_2 (litres / min or percentage) ● Temperature (including temperature site) ● Systolic Blood Pressure ● Diastolic Blood Pressure ● Heart Rate ● Level of Consciousness (AVPU) ● Pain Score ● Urine (Y/N) ● Bowels opened (Y/N) ● Free text comment section ● Blood Glucose results
BioConnect (on completion of development)	Blood Glucose Result	• Blood Glucose results

In addition to the above, the following information will be made available:

- Reference Files - Trust Locations, Health Care Professionals, GPs and Treatment Function Codes (specific Sub Specialty of a Consultant) to be supplied as an initial data load.

The scope of the data sets is likely to increase, as the hospital progresses to achieve their 2020 vision of full electronic patient record. Any further scope increase / change will be subject to an addendum or further iteration of the PIA.

4.4 Demographics Matching, Data Linkages and Data Integrity

As noted in the section above, data comes from multiple source systems to form the Streams record. These datasets will be linked at the patient level using matching criteria to ensure that they can be presented through Streams as one patient record.

A key challenge of transferring data between different electronic health care systems is the ability to ensure that the correct information aligns to the correct patient records. This is carried out by a process of demographics matching as follows;

Where demographics are received from another source (e.g. Pathology/Radiology systems), DeepMind will match records with:

- An MRN/NHS Number and two of: First Name, Last Name, DOB and Post Code;
- All four of the following: First Name, Last Name, DOB and Post Code.

DeepMind will flag instances where records fail to process, to protect the integrity of the data.

DeepMind will also check data received against supplied reference files and where received data items are not in the reference files these will be added dynamically.

4.5 Clinical Use of Data

Below are a series of scenarios which provide clinical examples that illustrate how data processed by DeepMind and presented by Streams will enable the delivery of safer patient care.

Example 1: Clinical context for viewing historical abnormal results and provisional diagnoses.

A patient is reviewed in the admissions unit following a collapse at home. At the bedside, the Streams app allows the clinical staff to review the most recent and the previous blood test results. Comparison of these results reveals a previous episode of a low haemoglobin level caused by a gastric bleed. The combination of their clinical presentation and their digital observations suggests that they need to consider this as a cause for the current presentation.

Example 2: Clinical context for viewing historical normal results.

A man presenting with joint pain has small rise in his liver tests. By reviewing his historical blood tests the attending clinician confirms that these changes have been present for five years and she is able to reassure the patient that is this abnormality is unlikely to be relevant to his current problem.

Example 3: Clinical context for use of demographic data.

Correct patient identification of patients on available digital systems is essential. Reviewing the full name, date of birth, hospital number (MRN), NHS number, title and address ensures that the patient is correctly identified, duplicate patient entries can be dealt with safely without losing important data, and patients with similar identifiers can be distinguished and managed safely without incurring a safety risk (e.g. when two patients with the same name and similar ages are treated on the same ward at the same time).

Example 4: Clinical context for transfer of extended patient demographic data.

A patient has presented with sudden collapse. They are weak on one side and a stroke is suspected. A stroke is caused by loss of blood supply to the brain and urgent potentially lifesaving treatment is required. Rapid identification of the community doctor can help to ensure that an accurate history and diagnosis is made and therefore improve patient care.

Example 5: Set of patient observations

A patient has been admitted to a ward and a routine set of observations have been captured, calculating a NEWS score of 5 for that set of observations. An advice screen is displayed showing that the frequency of monitoring is required to be completed 1 hourly with consideration of completing a fluid balance chart. The advice also includes guidance on which professionals need to be contacted to review the patient and the relevant timescales. This set of observations can then be reviewed against previous observations taken within the graphical format.

Example 6: Monitoring for future care

A patient is admitted with a fall and found to have iron deficiency anaemia which is investigated and no cause found. The anaemia is treated and the patient discharged with a recommendation for community monitoring via the GP. These results would be continually updated to Streams. Having initially maintained stable haemoglobin over duration of 12 months the anaemia reoccurs to a point that needs readmission. The admitting team are able to see the initial investigations and the trends of the blood test over the last 12 months which informs the choices that the clinicians take on the subsequent admission to ensure timely care.

4.6 Changes in data scope between PIA's

The scope of data to be transferred to DeepMind has increased from the previous PIA (published Jan 2018) to include:

1. Live data validation and piloting of the observations functionality;
2. Live data validation and piloting of the streams views functionality;
3. Use of the streams viewer and observations recording for direct patient care for all inpatients and A & E attendances.

4.7 Testing & Validation

Testing on the anonymised data set will be as defined in the documents embedded in section 7. In order to validate the system is clinically safe the system will have patient data transfer for a limited set of patients as defined by the pilot scope. This is to validate that the system accurately displays and processes the patient data as designed.

5. Data Flows, Access and Security (Principle f of the GDPR, DPA)

5.1 Data Flows

This section has been redacted as it relates to Data Security and it is commercially sensitive.

5.2 Data Transformation

At this stage, there will be no data transformation within the DeepMind data centre. The technical transformation of messaging data within the DeepMind data centre from HL7 to FHIR will be considered a later stage.

5.3 Data Processing

Data processing within the DeepMind data centre will be limited. The analytics processor will process the data as per contractual agreement. Clinical staff using Streams will be presented with the outcome of the AKI algorithm (previously viewable and calculated in the Trust's existing OrderComms system); users will be able to see how the algorithm outcome is determined and then apply their clinical judgement in delivery of the appropriate clinical care.

Any further changes will need to be specified by the Trust in its capacity as Data Controller and actioned as part of change control processes via a change control notice and will trigger an update to this PIA. There will be no pre loading of data for the observations functionality and this only involves the patients which have direct clinical inpatient care.

5.4 Access / Security

This section has been redacted as it relates to Data Security.

5.5 Account Validity Checking

The Trust uses Microsoft Active Directory as its primary method of managing access to electronic resources and validating users. Active Directory access is tightly controlled and linked with

processes such as recruitment starters and leavers to ensure only authorised individuals have an account. Mobile devices configured to access the Trust network are aligned to user active directory accounts. Active Directory (AD) Group membership is verified at the point of login and only those users that have a valid Active Directory account and the appropriate group membership are allowed access. The mobile application continues functioning for the period of validity of their access token (configurable, but typically 13 hrs). If an account was disabled during this period (e.g. for gross misconduct), the device could be remote-wiped via the Trust's Mobile Device Management (MDM) system. Streams also checks that logged in user accounts are still active on the trust Active Directory every 10 minutes when there is a request for fresh information. If a user account is determined to have become inactive the user's access token will be invalidated, and on their next request they will be returned to the login screen.

6. Data Disclosure and Retention (Principle e of the GDPR, DPA)

This section outlines the Trust position in relation to disclosure of data held within the DeepMind data centre and the retention of data by DeepMind.

6.1 Data Disclosure

Disclosure of data is under the Trust's control. The only circumstance in which DeepMind would disclose the Trust's data is if required by law or expressly instructed by the Trust (for example, to a patient to comply with a subject access request).

6.2 Retention

As Data Controller, the Trust retains sole control in determining data retention and destruction criteria as set out in Clause 30.8.3 of the Service Agreement. Destruction will be witnessed at the ceasing of the service agreement.
Should the Trust end user access to Streams; the Trust will request via email that DeepMind remove the Taunton data; DeepMind will remove the Trust data including any back-ups; and DeepMind will confirm deletion with the Trust via email.

7. Data Anonymisation

The Trust gives assurance any testing of the application will be carried out using anonymised data. The Trust has developed its own data an anonymisation process and testing process. The process is described in the files below:

Anonymisation Deepmind v1.3.pdf

Interface Testing Process v1.2.docx

The Trust recognises that there are potential limitations with the anonymisation process. There is a balance to be reached to enable anonymisation to protect patient data, but to enable effective validation of the data transfer and record matching processes. Results will not be valid if the data cannot replicate the behaviour of live data throughout the patient pathway. Failure to replicate realistic scenarios has the potential to constitute a safety risk to patients through failure to detect system or process errors.

The Trust has identified the following privacy risks in relation to the anonymisation process and the associated data transfer to DeepMind;

Risk Description	Considerations & Mitigations
Publication of anonymisation process The release of the anonymisation process into the public domain as part of the PIA could make it easier for the data to be re-identified.	The Trust is balancing the need to be as transparent as possible with regards to its privacy risks and commercial relationship with DeepMind against the privacy risks created through disclosure of detailed process. The Trust is confident that the document containing the data anonymisation process provides an expected level of transparency whilst not providing the technical algorithms needed to re-identify the data. No further mitigations are planned, unless the Trust is specifically advised to redact content.
Loss of anonymisation key The anonymisation process uses a data key (mapping) to replace the demographics for the same person with the same anonymised identifiers. If this key is lost or shared with third parties the data could be re-identified.	The anonymisation key remains under the sole possession of the Trust and (as described in the process document) will be deleted as part of the process, before any data is transferred outside the Trust. No further mitigations are planned.
Combined data sets 3rd parties with sufficient additional data sets might be able to re-identify some or all of the data set.	The data to be transferred is of limited scope both in terms of data items and time frame. The Trust has not shared any additional data sets with DeepMind and will not be sharing this anonymised data set with any other 3rd parties. The Trust is confident that its data will be safe and secure in the DeepMind data centre, therefore preventing unauthorised access. At this stage, no further mitigations are planned.
Extreme of data There could be information in the public domain that could facilitate the re-identification of anonymised patients at the very extreme of age or with a rare clinical condition.	The Trust acknowledges that there is patient data within the public domain which could, in theory, be used to try and re-identify specific individual records. For example; it is not unusual for the press to publish articles relating to, and identifying (with permission) members of the public. The Trust is confident that this theoretical risk is mitigated by its Information Procession Agreement with DeepMind.

	No further mitigations are planned, unless the Trust is specifically advised to limit the patient cohort.
Unstructured Data fields Unstructured data fields could inadvertently contain a patient identifier.	There is a small risk that unstructured data fields could contain some form of patient identifier. It is unlikely that these fields would contain more than a single data item and it would not be in a structured format. At this stage, no mitigation is planned.

8. Privacy Actions

The prior sections identify and detail privacy considerations and related risks, establishing the case for the intended data transfer of patient data and processing operations.

This section lists the key actions undertaken by the Trust at this stage to minimise privacy and related risks;

1. Minimise scope of data transferred to DeepMind data centre based on clinical need;
2. Store data in a secure data centre, deemed appropriate and DPA compliant by Trust Technical and Information Governance leads;
3. Ensure access to patient data is restricted to only those staff that have a legitimate healthcare relationship with the patient;
4. Monitor access to patient data at both the DeepMind data centre and front facing mobile application;
5. Review PIA on a regular basis to ensure existing and emerging privacy and related risks are assessed and appropriate activities to minimise risk undertaken;
6. Continue to engage with the public through a thorough, transparent process, putting patients at the core of digital developments. Enabling patients/the public to guide the protection and use of their data.

9. Conclusion / Outcome

The Taunton and Somerset NHS Foundation Trust - DeepMind Technologies Limited service agreement and associated Information Processing Agreement clearly establishes the Data Controller - Data Processor relationship. The PIA process has examined in detail the privacy risks to the patient; these risks are not new or unfamiliar risks to the organisation, which had until 2015 kept the majority of its patient data in an off-site 3rd party data centre.

The AKI algorithm that the Trust will eventually deploy is not fundamentally dissimilar to that currently used by clinicians through the existing OrderComms system and is likely to bring a greater level of transparency to the algorithm result than clinicians presently have access to. The Trust is assured that DeepMind as a Data Processor will not be applying machine learning, artificial intelligence or unauthorised algorithm/processing activities to its data.

The deployment of the DeepMind mobile application can be viewed as a continuation of business as usual processes, albeit with an increased use of a mobile platform to access and capture patient data at the point of care. Clinical data is currently accessible to clinicians via both authorised mobile devices and remotely via secure VPN connections. Communication to patients will focus on the shift

towards mobile technology use and the safety gains that can be made by applying standardised rules-based algorithms to clinical data sets.

The Trust has taken all reasonable steps to limit the data scope of the initial transfer of patient data and will continue to re-assess privacy risks at every stage of the project.

The Trust recognises the implications of external parties analysing the relationship between the Trust and DeepMind and drawing conclusions around the data processing agreement and activities. The Trust and DeepMind must ensure concerns from individual patients are addressed in a timely manner. The Trust will continue to actively engage with the ICO to ensure lessons are learned and best practice applied.

The benefits of the partnership outweigh the risks and it is therefore the intention of the Trust to proceed under the service agreement with DeepMind Technologies Limited. They are considered to be an anchor partner in the delivery of the Trust NHS Global Digital Exemplar vision.

10. Legal Requirements

This document has been written to meet the following legal requirements.

Caldicott Reports 1997, 2013, 2016
Data Protection Act 2018/General Data Protection Regulation
NHS Confidentiality Code of Practice 2003
Computer Misuse Act 1990
Common Law Duty of Confidence
Care Quality Commission standards
NHS The Care Record Guarantee
Freedom of Information Act 2000

11. APPENDIX 1

DeepMind Streams
PIA anny test Versior

Revision History

Approvers

Andrew Forrest
Tom Edwards
Luke Gompels
Mark Dayer
Louise Coppin