PRIVACY IMPACT ASSESSMENT (PIA)
Collaboration with DeepMind for Delivery of Mobile Platform and Streams App

1. Background

Yeovil District Hospital NHS Foundation Trust (the Trust) is in discussion with DeepMind Technologies to become an anchor partner in developing a mobile application that will support its transition to a digitally maturity in line with the wider 2020 strategy.

Paper and electronic records regarding the health, care and treatment provided to patients are already kept to ensure that patients receive the best possible care; through the increased use of technology, the safety, experience and outcome of this care can be greatly improved. The Trust considers that such opportunities for improvement should be taken up where possible, in the interests of patient care and the Trust's discharge of its statutory duties.

Working with DeepMind, alongside existing system suppliers, the Trust is looking to deliver a truly integrated Electronic Patient Record (EPR). It proposes to use DeepMind as a data processor acting on its behalf to deliver a mobile interface to facilitate the increased access and usability of the information contained within the EPR and to also enter data for incorporation into the EPR

In order for the mobile application to function, personal 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. The scope of this data upload is defined below and has been restricted to 'active' patients under the care of the Trust.

Neither the mobile application nor Trust data will use DeepMind's machine learning, Artificial Intelligence or unauthorised algorithm/processing, and will solely be used for the purposes of direct patient care. The Trust, as data controller, will define any decision tree based algorithms to be applied to defined datasets or patient cohorts in line with NHS clinical guidance and will instructed DeepMind on all future developments.

The purpose of the mobile application is to re-present clinical information from existing systems in a user-friendly collated view. Data will be captured by users into a mobile solution to support the delivery of patient care and will be stored within the DeepMind data centre and fed into the Trusts EPR. The design of the mobile platform will be in line with NHS Common User Interface Guidelines.

The development and implementation of this mobile application therefore does not constitute any fundamental novelty in terms of what the Trust already does with patients' personal information. The innovation comes in terms of how that data is presented, in order to make substantial improvements to patient care and the Trust's discharge of its functions.

2. Need for a PIA

The Trust considered the implications of the proposal and confirmed the need for a privacy impact assessment. Following review at the clinical design authority with relevant staff groups and consultation with partner organisations and Deep Mind the trust developed this detailed Privacy Impact Assessment.

Anthony Smith

Chief Clinical Information Officer/Clinical Safety Officer

3. Overall objective: Supporting Care Delivery

The mobile application will be used by named clinical staff as part of direct care activity for identified patients for whom the user is providing care and/or treatment. The mobile application will present the user with a consolidated view of the patients' record, enabling timely access to information and enabling informed decisions to be made on the move. An example of this will be the capturing of a patient's observations and vital signs to determine if the patient is at risk of clinical deterioration and thus enabling faster intervention to safely manage the patient's condition.

Captured data will be processed and stored within the DeepMind data centre in line with specific instructions from the Trust, with duties enshrined in the contract between the Trust and DeepMind. Where mobile applications are considered to be medical devices, they will go through the same rigorous testing as any other medical device.

4. Benefits

The benefits of technology in healthcare are vast: deteriorating patients can be identified sooner; adverse drug and allergy interactions can be avoided; the transcription and subsequent errors of information is reduced; clinical time is freed up to spend with patients; and information is available to staff with a legitimate need, at any time and from anywhere within the Trusts secured network and from a Trust secured device.

Data will be displayed in the mobile application from a range of systems, reducing the need for users to log into and access multiple systems. Decision support can be applied when these datasets are utilised in defined evidence based algorithms. An example of this will be the identification of patients at risk of Acute Kidney Injury (AKI), whereby defined triggers and rules can be applied to laboratory results, enabling the early identification of patients at risk of AKI so that treatment can be provided. The AKI algorithm that will be applied by the Trust is not fundamentally different from the algorithm that is currently applied by the Trust Order Comms solution and is a published NHS England algorithm.

The data collected within the mobile application will be stored in a data centre as well as being stored within the Trust's EPR. This parallel storage will provide the Trust with a continuity of care should either system or interfaces be unavailable through planned or unplanned downtime.

5. 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 all privacy concerns and related risks.
The Trust's assessment of the key risks is as follows:

- **Data Security:** 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.

  Mitigation: 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. ISO 27001 accreditation has been achieved by DeepMind and any transfer of data will be encrypted

over secure NHS networks. All data will also be encrypted on disk whilst stored in DeepMind's data centres. It should also be noted that DeepMind will store the Trust's patient data in England and the data will not be transferred outside of the UK. Daily backups of the data will be taken by DeepMind which are also encrypted.

The Trust has ensured by means of a written contract that commits DeepMind to ensuring adequate technical and organisational data security measures. As part of this DeepMind will maintain NHS Information Governance Toolkit Level 2 or above accreditation.

The Trust will undertake an annual 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 incompatible purposes:** for the purposes of DPA compliance as well as patient trust, it is important that the patient data which will be processed for the purposes of this application not be used for any other purpose.

  Mitigation: the Trust's dialogue with DeepMind has resulted in an agreement, embodied in its contract, that this data may only be used for the purposes of DeepMind's provision of this application as a data processor. It may not be combined with other data, analysed or otherwise used in any way. If the Trust decides that any additional processing purposes are necessary, a new PIA will be developed to evaluate the associated risks.

- **Patient expectations and confidence:** patients need to be confident that the Trust, working with DeepMind as its data processor, is using their personal data fairly, lawfully, confidentially and for permissible purposes. If that confidence is undermined by patients feeling that their data is being used in ways which do not accord with their expectations, this would undermine the Trust's relationship with its patients and also its compliance with the data protection principles (in particular, the first principle).

  Mitigation: as explained in this PIA, the Trust is confident that any such concerns on the part of patients would be unfounded. 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 disclosure to any data controller or any other external party. The data will only be used for the purposes described above. This will be explained in press releases and accompanying information which the Trust will publish when the application is launched.

- **Processing of excessive data:** the Trust is mindful of the need only to process personal data to the extent that this is needed for the purposes behind this application, and not to process personal data for longer than is necessary.

  Mitigation: the Trust, in discussion with DeepMind, has carefully specified the exact datasets (which patients, which data, from which source, for which periods) which will be processed, as set out below. It has ensured that it will process the data which is needed for this application to function and not any unnecessary data.

- **Patient Consent:** the Trust has considered the use of the mobile application and has concluded that there are no fundamental differences in the DeepMind mobile application and associated data centre arrangements compared with existing systems within the Trust or previous arrangements whereby data was held on behalf of the Trust in a third party data centre. As patient data will be used for the purposes of direct care, patient consent will not be explicitly sought. Moreover, the Trust has considered whether patient consent - even if

not necessary - could in any event be sought. It has concluded that this would not be practicable as the necessary datasets would not be available for the application to be launched if data were only processed on a patient-by-patient basis as and when consent was forthcoming.

Mitigation: the Trust has ensured that alternative justifications (in particular, conditions from Schedules 2 and 3 to the DPA) are satisfied here. In addition, patient communication and engagement will form part of the implementation to ensure that patients are informed of the Trust's plans and the steps that have been taken to ensure their data remains confidential and safe.

- **Ensuring adequate justification for processing**: the Trust acknowledges the importance of ensuring that it's processing of personal data is not only fair and lawful, but also that conditions from Schedule 2 and 3 to the DPA are met. As set out above, the Trust has decided not to base its processing on patient consent. This means that alternative conditions must be satisfied if DPA compliance is to be secured.

  Mitigation: the Trust is confident that condition 5(b) (statutory functions) from Schedule 2 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. In addition, condition 6(1) (legitimate interests) from Schedule 2 DPA would also be satisfied.

  On the same basis, conditions 7(b) (statutory functions) and 8 (medical purposes) from Schedule 3 would be 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.

- **Respecting patients' rights and wishes:** 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. It would not be practicable to do so in this case: it would not be safe to revert to paper for some patients and use electronic systems for others. Electronic observations, order communications, diagnostic results and patient correspondence are already in place digitally at the Trust.

  Mitigation: 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.

- **Ensuring ongoing data protection compliance:** the analysis in this PIA focuses on the DPA 1998. The Trust is mindful that, with effect from May 2018, the new regime will be the EU's General Data Protection Regulation. The Trust has considered the risk that the change in regime would undermine its compliance with its data protection duties.

  Mitigation: the Trust has considered whether the enhanced and additional requirements of the GDPR would be likely to render the proposed processing arrangements unlawful. It has concluded that this arrangement would be lawful under the DPA and also under the GDPR.

It will, however, review the position once the GDPR is in force and in light of any further guidance on the GDPR to confirm that this remains the case.

- **Conclusion on privacy and data protection risks:** the Information Processing Agreement (IPA) with DeepMind clearly defines the Trust as the Data Controller and DeepMind Technologies 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 or research. The Trust has received the necessary assurances that DeepMind will only act as a data processor as defined within the service agreement, and it will ensure that the agreement is complied with.

  The Trust has also considered all aspects of data protection compliance and sought to identify the key potential risks and concerns in terms of patients' right. These have been highlighted above, together with mitigating measures. In summary, the Trust is satisfied 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 mobile application will enhance patient care substantially without causing unjustified interference with patients' rights to privacy and to the lawful processing of their personal data.

6. Scope of Data Transfer

As part of the implementation, an initial data load will be taken based on current patient activity within the Trust in order to minimise the data transfer as far as is reasonably possible.

The data transfer will be limited to:

- Patients with open elective pathways;
- Patients with emergency admission pathways with unscheduled pending activity;
- Patients with emergency admissions within the 6 months prior at the point of data transfer (i.e. before Streams go-live).

Radiology and pathology requests and results for the 5 years prior to the point of data transfer will be included in the data load for the above patient cohort.

The rationale for this data acquisition has been reviewed by the Chief Clinical Information Officer (CCIO) in conjunction with the Clinical Design Authority (CDA) and the Information Governance Steering Group to consider clinical applicability and relevance of the data that is being utilised for clinical assessment of patients. The above criteria have been selected to ensure that only clinically relevant data is displayed for patients who are undergoing or have had prior care within the Trust. Data transfer of pathology and radiology requests and reports for a period of five years has been selected to ensure that both normal and abnormal results can be assessed from both the community and hospital; this is also in keeping with available information on current systems (current time limits are selected between 10-1000 days for pathology reporting, with charting functionality for historical results for >5 years).

It is recognised that in the future, it may become apparent that patients who currently do not fit these inclusion criteria are 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.

7. Clinical Use of Data:

Below are 2 examples of where the mobile app and associated data will be used in the delivery of clinical care.

Example 1:
A patient is reviewed on the admissions unit with collapse and a longer history of fatigue. Review of prior results 4 years previously reveals a prior low blood level following a gastric bleed for which they had a blood transfusion. This would be relevant to their current presentation and assessment with early consideration of whether their current presentation and fall is compatible with acute blood loss. Similarly prior normal results would also be relevant in this scenario and may point to an alternative diagnosis, for example a progressive reduction in sodium levels caused by an underlying lung tumour, where review of prior radiology revealed a previously normal CXR where the result could be compared to the current imaging. Equally it would be relevant to be aware of previous scan results which highlight alternative explanations, for example, an enlarging abdominal aortic aneurysm.

Example 2:
A man presenting with joint pain has small rise in his liver tests and platelet (blood count). To determine whether this is incidental or part of his current problem review of historical blood tests is required. This demonstrates a long term change in blood tests over the last five years and hence provides confirmation of an incidental rise in the tests that is not significant to his current problem.

Upon presentation to the Trust (either by referral or as an emergency) patients that have not previously met the inclusion criteria for data transfer will have their data transferred to the DeepMind data centre for processing within the mobile application. As with the pre-transferred cohort, this will be in adherence with Principle 3 of the Data Protection Act, ensuring that only adequate, relevant and not excessive data is transferred.

Example 3:
A man presents with shortness of breath and an abnormal ECG is seen with left bundle branch block. The man has recently attended as an outpatient for a cardiology appointment. In the letter is a description of the ECG findings at the time and a care plan to manage his heart failure. To determine the care plan agreed in the outpatients it is necessary to review the outpatient letter available in the patient centre. Having this available in Streams would make the ability to review this information more efficient and safer as the link would be in patient context.

8. Data Sets and Data Sources

Data sets and data sources are detailed below:

Data Source	Data Set	Type of Data
Intersystems Trakcare EPR	Demographic Data	• NHS Number • Medical Record Number (MRN) • Surname • Forename • Middle Name • Title • Preferred Names • Previous Names

		• DOB • Address • GP Practice • GP • Next Of Kin
Intersystems Trakcare EPR	Activity Data	• Referrals • Outpatient Attendances • Admissions • Transfers • Discharges • Responsible Health Care Professional
Labcentre Ordercomms	Pathology Data	• Pathology Orders • Pathology Results
Carestream RIS/Trakcare Ordercomms	Radiology Data	• Radiology Orders
CareStream RIS	Radiology Data	• Radiology Textual Reports (Results)
Patient centre	Discharge Summaries/clinic letters	• Read-only view of discharge summaries and outpatient clinic letters via hyperlink to the Trusts Correspondence system Patient Centre

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

- Reference Files - Trust Locations, Health Care Professionals, GPs and Treatment Function Codes to be supplied as an initial data load.

- Vital Signs - no historic data to be provided.

  The following data items will be captured for vital signs:
  - Respiration Rate
  - Oxygen Saturations
  - Any Supplemental Oxygen
  - FiO2
  - Oxygen Delivery Device
  - Oxygen flow rate (L/min)
  - Temperature
  - Systolic BP
  - Diastolic BP
  - Mean Arterial BP
  - BP Recorded Manually (Y/N)
  - BP limb used (Left or Right Arm) and position of patient (Lying/Standing)
  - Heart Rate
  - Pulse Irregular (Y/N)
  - Level of Consciousness (AVPU) + Confusion
  - New deterioration of mental state
  - Pain Score (0-10)
  - Treatment Escalation Plan completed (Y/N/n/a)
  - Urine Output consideration
  - Blood Glucose
  - Bowels open (Y/N)
  - Peak expiratory flow rate (PEFR)

9. Data Linkages and Data Integrity

All datasets will be linked at the patient level using the matching criteria defined below.

DeepMind will check data received against supplied reference files and will flag where received data items are not in the reference files for:

- General Practitioner;
- Health Care Professionals;
- Point of Care (Location);
- Specialty Code;
- Main Treatment Function Code;
- Discharge Destination.

Additionally data validation will flag:

- Future dates/far past dates;
- Invalid NHS Numbers.

10. Demographics Matching

Where demographics are received from the master patient index (MPI), DeepMind will assume them to be correct and update the records accordingly.

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

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

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

11. Data processing

For the purposes of this Agreement, Data relating to Patients which is provided by the Controller to the Processor is strictly limited to Active Patients. Data relating to Patients who are not Active Patients shall not be transferred to the Processor by the Controller.

The Controller will provide the following Data on the dates and in the manner specified in the Roadmap:

- HL7 feeds: and live data via HL7 MLLP (Minimal Lower Layer Protocol);

- HL7 message types (e.g. ADT, ORU, ORM) and sources required on the feed will be determined by the roadmap of resources to be provided by the API in the Project roadmap;

- Text files exported from existing hospital systems defining fixed (non-patient) resources (e.g. Consultants, General Practitioners, Beds) as part of an initial bulk upload thereafter updated will be provided in real-time messaging; and

- Historic encounter, diagnostic information in an agreed format (e.g. HES-APC
- 6.2 single line fixed width) for 5 years of data.

- Electronic Patient Record database (sub-set of data as defined in schedule 4).

The data sets may be varied in accordance with the Change Control Procedure set out in the Services Agreement and will be subject to the September 2017 PIA and any additional Privacy Impact Assessment.

The Data will be transferred over secure N3 connections between the Trust and designated data centres.

12. Security Measures

The Processor shall implement and maintain adequate security measures to standards no less than those imposed on the Controller under the seventh data protection principle set out the Data Protection Act 1998 whilst it continues to Process the Data on behalf of the Controller, such measures shall include (but not be limited to):

Data Centre - Data is stored at an ISO27001 accredited colocation facility.

Encryption - Data will be delivered to the Processor over an encrypted channel. Where required by the Controller, connections will be limited to the Controller's N3 Network and/or encapsulated, for example in an encrypted Internet Protocol Security tunnel. The API will be accessible from the Controller via an encrypted HTTPS connection, secured via an authentication and authorisation system linked to the Controller, such as its LDAP servers. Data is secured on disk with AES-256 encryption and in-transit at the colocation facility with TLS v1.2.

Backup - The Processor will use an encrypted file-based backup with full and incremental backups daily.

Resilience - The Processor will use reasonable measures to seek to ensure that there is sufficient additional server and other hardware capacity to continue operations of the systems. Where technically feasible failover mechanisms will be in place to ensure that in the event of hardware or software failure the Services will transition to other available systems.

Disaster Recovery - The Processor has undertaken and continuously undertakes disaster recovery planning exercises. The Processor and the Controller will agree a formal service level agreement to cover any deployment with critical clinical dependencies on or prior to the relevant date in the Roadmap.

Incident Notification - The Processor will promptly inform the Controller of any Security Incident in accordance with Clause 4.10 of the IPA.

NHS Information Governance Requirements The Processor shall maintain NHS Information Governance Toolkit level 2 or above accreditation, or such equivalent measures as may from time to time be specified.

13. Data Flow Map

14. Multi-User Devices

DeepMind's user-experience team are exploring the use of a second-factor in-app PIN code which is sync'd to backend servers for use in the multi-user device scenario. Authentication will be pushed via the app so that the user for that shift is logged in correctly for clinical safety and audit purposes. DeepMind are also exploring the use of name badge barcode scanning with PIN to enable log in to multi-user devices.

15. Account Validity Checking

Active Directory (AD) Group membership is verified at the point of login. The mobile application continues functioning for the period of validity of their access token (configurable, but typically 13 hrs for single-user devices). If an account was disabled during this period (e.g. for gross misconduct), and the device could not be remote-wiped via the MDM a P0 support ticket would need to be raised with the DMH support desk to disable the user's session.

Continuous checking of account validity has been shown to place an unacceptably high load on the Trust LDAP servers. DeepMind intend to build functionality for disabling active login sessions via their admin console.

16. Data Transformation

The only transformation of data with the DeepMind data centre will be the technical transformation of messaging from HL7 to FHIR.

17. Data Analytics

The analytics processer will process the data required for the AKI algorithm. Front end clinical staff using the mobile application will be presented with the outcome of the AKI algorithm; 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 application of algorithm beyond AKI will need to be specified by the Trust in capacity of data controller and actioned as part of change control processes via a change control notice.

See section 4 Schedule 1 of the Information Processing Agreement for details of the data processing agreement.

18. Retention

As data controller, the Trust retains sole control in determining data retention and destruction criteria as set out in Section 30.8 of the service agreement. Destruction will be witnessed at cease of service agreement.

19. Testing

Testing will be performed in a User Acceptance Testing (UAT) environment using dummy patients until at which point the system is handed over to the Trust. At no point will testing be performed using live patient data.

20. Validation

Validation will be performed using identifiable data on go live by those users who have legitimate relationships; any problems following this are treated as issues and fixes applied.

21. Disclosure

All disclosure of data is under the Trust's control.

22. Privacy Solutions

The above sections identify and detail privacy and related risks, establishing the case for intended processing operations.

Actions undertaken 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 annually or in the event of a change of scope or legislation to ensure existing and emerging privacy and related risks are assessed and appropriate activities to minimise risk undertaken

23. Conclusion / Outcome

The Yeovil District Hospital NHS Foundation Trust - DeepMind Technologies Ltd 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.

The AKI algorithm that the Trust would deploy is not fundamentally dissimilar to that currently used by clinicians through the existing Order Comms system and is likely to bring a greater level of transparency to the algorithm result than clinicians presently have access too. 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 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 high profile of DeepMind has led to a variety of opinion papers published surrounding their work. It is recognised that these publications may impact patient perceptions of the privacy and security of their personal sensitive data. The Trust and DeepMind must ensure concerns from individual patients are addressed in a timely manner.

The benefits of the partnership outweigh the risks and it is therefore the intention of the Trust to proceed with the service agreement as an anchor partner with DeepMind Technologies.