Royal Free London NHS
NHS Foundation Trust

# INFORMATION SHARING AGREEMENT

## 1. Purpose of this document

This document describes the minimum arrangements for regularly or routinely sharing person identifiable information (PID) with non NHS bodies for the Direct Care of the Patient. It is to be used as the basis of agreements made about specific services with individual non NHS bodies and/or Data Processors. In those agreements all its provisions from paragraph 3 onwards must be included (unless otherwise approved by the trust's Caldicott Guardian or CISO). The sections in boxes are to be composed to suit the specific information sharing agreement.

### Parties to the agreement

| Party A | Party B |
|---|---|
| Royal Free, Barnet & Chase Farm Hospitals<br>Royal Free London NHS Foundation<br>TrustHS<br>Pond St<br>Hampstead<br>London NW2 2QG | Google UK Limited<br>Belgrave House<br>76 Buckingham Palace Road<br>London SW1W 9TQ |

## 2. Exclusions

Some bodies have rights in law in certain circumstances to be given certain patient identifiable information without an information sharing agreement being needed. Examples include the Audit Commission or other statutory auditor when undertaking an audit that requires such information, but there are many others. This subject is not covered in this agreement.

Information sharing between NHS bodies and NHS staff (whether directly employed or not) is governed by the trust's patient confidentiality policy and other advice given in the information governance portal on the Trust Intranet. The trust's policy on this subject is founded on the Caldicott principles.

Information exchanged as part of clinical research is covered by research governance, and not by this document.

Putting information directly into the public domain, for example to the media, is excluded from this agreement.

## 3. Definitions

Person identifiable information / data (PID)

This means information that can lead to the identification of an individual living person  or client.  It includes above all:

name (including initials)
address
NHS number
photographs or videos.

Other details may, especially in combination, enable an individual to be identified, such as:

full postcode
date of birth
telephone number
e-mail address.

Information sharing

This means the trust and third parties sending in either direction person identifiable information using any physical (including handwritten notes or completed forms) or encrypted electronic medium. **Electronic person identifiable data sent externally must be encrypted.** NHS.net to NHS.net email accounts provides a secure, encrypted method of sharing information. Note: the DoH has confirmed that organisations may send up to 5 patient's images via an unencrypted CD in one transfer.

## 4. Principles

Information sharing between organisations must always be consistent with the Caldicott principles. These are:

1. Justify the purpose(s) for using confidential information.
2. Use it only when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict "need to know" basis.
5. Everyone must understand their responsibilities.
6. Understand and comply with the law.

Staff must always abide by the trust's information governance policies and guidance, which is available on the Trust "Information governance" portal.

## 5. Details of the agreement

Purpose/s for sharing information

*Why is the information being shared?*

Patient Rescue is a Proof of Concept Technology Platform that enables Analytics as a Service for NHS Hospital Trusts. It has been developed by DeepMind, a group within Google UK Ltd.

Analyses are performed on both live and batch (intermittent) data streams. Outputs include tools to enhance adherence to, and implementation of, NHS/NICE guidelines. This will consist of: (i) Patient Safety Alerts for Acute Kidney Injury, and (ii) Real time clinical analytics, detection, diagnosis and decision support to support treatment and avert clinical deterioration across a range of diagnoses and organ systems.

Information to be shared

1. HL7 feeds: Live from either source system or integration engine - via VPN
   a. All ADT
   b. ORU-RO1 (Results)– Pathology and Radiology
   c. Relevant specification and mapping documents for all the above
2. CDS / SUS submission - via VPN or SFTP
   a. APC – Completed inpatient episodes
   b. CC – Critical Care
   c. AAE – Accident and Emergency
   d. Relevant specification and mapping documents for all the above
3. Last 5 years archival data of all the above, in any defined format, to aid service evaluation and audit of the new product.

Royal Free specific NHS.net email addresses to allow for sending and receipt of the Advanced Clinical Decision Support Document. These NHS.net addresses are for non-commercial use only.

The Trust permits data to be anonymised for research under formal research ethics as approved by either the **National Research Ethics Service** or the Joint **UCL**, UCLH and **Royal Free** Biomedical Research Unit.

RFL remain the Data Controller.

When and how often is the information to be shared?

Streaming data – as per 5.2
SUS data: monthly.

What media is used for transferring the data (format *and* method)?

Streaming is via TCP/IP encrypted channel
SFTP secure transfer.

How is the information to be stored?

Data is stored at ISO27001 accredited location [redacted] – a contracted party to Party B. Data will not be stored or processed at the DeepMind offices, except for ordinary remote development and administration

Who will handle the data? Please state the authorised users.

DeepMind, Google UK Ltd. appointed staff, who have undergone information governance training and signed a confidentiality agreement as part of their employment contract.

How long will the data be held i.e. Retention period? – duration of the approved project.

*Any information held will not be retained for any longer than is necessary for the purpose that it was obtained for. Please give details.*
Unless otherwise specified, data will be retained as per RFL Records Management and Retention Policy, version 1.1, as issued on 1 October 2014, or other reasonably similar document as may be issued from time to time.

The End Date for the project is 29/09/2017, before which all PID held by the Patient Rescue project will be transferred back to the RFH, and any residual data destroyed.

What is the destruction process?

*How will the information be destroyed when no longer required? (e.g. shredding) Please give details.*

Any PID related to the project held on electronic media will be overwritten so that it is not recoverable; PID related to the project held on paper or disposable media will be shredded.

Will any of the data be transferred **outside** the European Economic Area (EEA)?

*If yes, please provide details of the recipients of the data and the country they are based in*

No.

Data to be processed for purposes other than for the direct care of the patient **must be pseudonymised** in line with NHS Act 2006 (NHS Care Record Guarantee) and Information Governance toolkit requirement.

Identifiable data will be retained by the system for up to 5 years from creation of the record, or until the End Date for the project, whichever comes first, in order to facilitate algorithms requiring historical data in order to correctly generate an alert. As this data is being held for direct patient care purposes, pseudonimisation is not required. Should a pseudonimised copy be created for non-direct care purposes, then it would be done in line with the HSCIC guidelines (NPFIT-FNT-TO-BPR-0023.01)

## 6. Responsibilities

The employees of Party B must treat the patient identifiable information received from the trust with a level of confidentiality that is at least equivalent to all the Caldicott and Caldicott 2 principles.

Assurance by the receiving organisation that it has confidentiality policies in place and that their employees have received information governance (confidentiality) training. Sanctions exist for staff that fail to comply with this agreement including citation of the relevant policies.

Verified on 22/09/2015.

### Data Protection Act and security.

### Compliance with the Data Protection Act 1998

- Under the terms of this agreement between the data processor Google UK Ltd. and the Data Controller dated 24/09/2015, the Processor provides the patient data analysis & alerting functions described above (section 5) for the processing of personal data under the Data Controller's control. For the avoidance of doubt, in relation to the Data Protection Act 1998, it is accepted by both parties that Google UK Ltd. is operating as the Data Processor and the The Royal Free London NHS Foundation Trust as a Data Controller.

- UK law does not permit the Data Controller to allow the Processor to process such personal data unless the Data Controller complies, and can demonstrate that the Data Controller complies, with certain requirements as set out in the seventh Data Protection principle. This agreement places obligations on the Data Controller and the Processor to discharge their respective obligations under the Data Protection Act 1998 ('the Act').

### Security

- The Processor will take appropriate technical and organisational measures against unlawful and unauthorised processing of personal data and against accidental loss, destruction of and damage to the personal data. In particular, the Processor is required to:

- Keep the personal data private and confidential by secure transfer such as N3 and/or AES 256 bit encryption; pseudonymisation, anonymisation or other information security techniques agreed between the parties;

- Using all reasonable endeavours minimise disclosure of the personal data to third parties to the fullest extent possible by use of techniques and controls.
- Allow access to the personal data on a 'need to know' basis and use appropriate technical and organisational controls to ensure this requirement is satisfied;
- Ensure that any recipients of the personal data are subject to a binding duty of confidentiality in relation to the data.

**Personnel**

- The Processor will ensure the reliability of all of its personnel (whether employees or contractors) that personal data is treated in compliance of the Data Protection Act 1998. If the Processor's staff is in breach of any of the aforementioned technical and organisational controls they will be subject to the Processor's disciplinary procedures. [For the avoidance of doubt the Data Controller will have the authority to demand that the Processor's staff concerned, subject to any acceptable re-training, do not have any further access to the Data Controller's personal data.]

**Procedure for Sharing Information**

- It is accepted that where the personal data is provided for the purpose of Non Healthcare Medical purpose (aka secondary use) and therefore each party will act in accordance with the requirements contained in Connecting for Health document NPFIT-FNT-TO-BPR-0023.01, "Pseudonymisation Implementation Project (PIP), Guidance on Terminology" dated 20/11/2009, in relation to the personal data and will only use the personal data to provide the services under this Agreement.

- The Processor will act in accordance with the Data Controller's instructions in relation to the personal data and will only use the personal data to provide the services under this Agreement.

**External Requests**

- The Processor will assist the Data Controller promptly with all subject access re-quests which may be received from individuals whose personal data the Processor is processing on behalf of the Data Controller;
- The Processor will promptly amend, transfer or delete any personal data that the Processor is processing for the Data Controller if the Data Controller requires the Processor to do so;
- The Processor will notify the Data Controller immediately of all communications the Processor receives from any person which suggests non-compliance with the Act and the Processor will not do anything or enter into any communication about it unless the Data Controller expressly authorises the Processor to do so;

- The Processor will provide the Data Controller with a copy of the personal data as soon as possible if the Data Controller asks the Processor to do so in the format and on the media which is specified in the Data Controller's reasonable request;
- The Processor will promptly inform the Data Controller of any breach or suspected breach of the Data Protection Act involving the Data Controller's personal data.
- The Processor will promptly inform the Data Controller of any information security incident or suspected information security incident involving the Data Controller's personal data.

**Data Processor Responsibilities**

- That all relevant staff are aware of this agreement's legal obligations and their responsibilities in discharging their duties.
- Ensure by all reasonable endeavours that a local procedure is in place to facilitate timely approval of requests for data sharing in respect of this agreement.
- Ensure that appropriate training is provided to all relevant personnel in relation to Information Governance and using all reasonable endeavours that they comply with the legal obligations of this agreement.
- Ensure that the incident management procedures are followed, that the Controller is briefed without delay and any corrective action is taken to redress any failures within a reasonable period of time.
- Ensure that standards and procedures are implemented to facilitate consent to disclose personal data constitutes informed consent and is given freely. A record should be kept of service users' consent given or withdrawn.
- Adequate, accessible, efficient and effective procedures have been implemented to address complaints for unauthorised disclosures or use of personal data.

**Audit**

- The Processor will permit the Data Controller to monitor compliance with the terms of this agreement, which may involve the Data Controller or its nominated representative coming onto any premises where the personal data are being processed with at least 10 working days' notice.

**Agreement formalities**

| | |
|---|---|
| Signed for and on behalf of the Data Controller | Signed for and on behalf of the Processor: |
| Signature: ……………………………………………… (Authorised signatory) | Signature: ……………………………… (Authorised signatory) |
| Print name: ……………………………………………… | Print name: MUSTAFA SULEYMAN |
| Position: ……………………………………………… | Position: CO-FOUNDER / HEAD OF APPLIED AI |
| Date: ……………………………………………… | Date: 29/09/2015 |

Review date………………………………………………

**Copy of agreement to be provided to the trust's Head of Information Governance for inclusion in the information sharing register.**