



**Dated: XX/XX/2020**

**Data Protection Contract**

**Between**

**<Insert Practice Name>**

**&**

**The Leeds Teaching Hospitals  
NHS Trust**

# Data Protection Contract

1. **DATED:** **xxxxx**

2. **PARTIES:**

This contract is made between the following parties:-

**<Insert Practice Name>**, (**"Partner Organisation"**), incorporated and registered in England and Wales with company number **xxxxxxxx** whose registered office is **xxxxxxxx** and

The Leeds Teaching Hospitals NHS Trust ("LTHTrust") of Trust Headquarters, St James's University Hospital, Beckett Street, Leeds, LS9 7TF.

3. **RECITALS**

- (1) This contract is for the sole purpose of carrying out ..... which *inter alia* involves processing the personal data of patients of the Partner Organisation, a purpose which is specified in the document Schedule 1, this purpose is hereafter referred to as the .....
- (2) The contract shall be deemed to have commenced on **[insert date]** and shall terminate upon 3 months written notice of either party to the other, such termination not to be effective before **[insert date]** unless this contract is terminated earlier in accordance with its terms.

4. **STATUTARY PROVISIONS**

This contract is made in accordance with Article 28 of the General Data Protection Regulation.

- 4.1 Where it is a NHS contract (a contract between two health service bodies) the NHS Act 2006 section 9 shall apply insofar as a NHS contract must not be regarded for any purpose as giving rise to contractual rights or liabilities.
- 4.2 If any dispute arises between two (or more) health service bodies with respect to this Contract under this arrangement, either party may refer the matter to the Secretary of State for determination, including local resolution where the Secretary of State has made such arrangements.

## 5. DEFINITIONS

In this contract, unless the context otherwise requires, the following definitions shall apply:

**“Data Controller”** shall have the same meaning as set out in the Data Protection Legislation.

**“Data Processor”** shall have the same meaning as set out in the Data Protection Legislation.

**“Data Protection Legislation”** means (i) the General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (Directive (EU) 2016/680) and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or European Data Protection Board (all as amended from time to time).

**“Data Subject”** shall have the same meaning as set out in the Data Protection Legislation.

**“Due Diligence”** shall mean the due diligence undertaken by the Partner Organisation on the security and data processing systems of LTHTrust;

**“EIRs”** means the Environmental Information Regulations 2004, as amended from time to time.

**“FOI Act”** means the Freedom of Information Act 2000, as amended from time to time.

**“Law”** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which LTHTrust is bound to comply.

**“Partner Organisation Personal Data”** means Personal Data Processed by LTHTrust on behalf of the Partner Organisation under or in connection with this contract.

**“Personal Data”** has the same meaning as in the Data Protection Legislation.

**“Processing”** has the same meaning as in the Data Protection Legislation and means *inter alia* obtaining, recording, holding, alteration, manipulating, transmission, disclosure, erasure or destruction of data.

**“Regulator”** means the Information Commissioner's Office and the European Data Protection Board or any successor body to either regulator from time to time and any other supervisory authority with jurisdiction over either party;

**Staff"** means all persons employed by LTHTrust to perform its obligations under the contract together with LTHTrust's servants, agents, suppliers and sub-contractors used in the performance of any of its obligations whether or not under this contract.

This contract includes within it the annexures attached to it or any document referred to in it.

## **6. GENERAL OBLIGATIONS OF THE CONTRACTOR**

- (1) The Contractor warrants and undertakes:
  - (a) to treat as confidential all Partner Organisation Personal Data which may be derived from or obtained in the course of the contract or which may come into the possession of LTHTrust or any Staff as a result of or in connection with the contract; and
  - (b) to provide all necessary precautions to ensure that all Partner Organisation Personal Data is treated as confidential by LTHTrust or any Staff; and
  - (c) to make sure Partner Organisation Personal Data is only disclosed to persons specified by the Partner Organisation; and
  - (d) to allow access to any Partner Organisation Personal Data provided by the Partner Organisation only to persons who are involved in the provision of this contract; and
  - (e) to notify the Partner Organisation if any unauthorised use or disclosure of the data is made. This includes reporting of any incidents, their causes and resolving actions to the Partner Organisation.
- (2) LTHTrust shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this contract in such a way as to cause the Partner Organisation to breach any of its applicable obligations under the Data Protection Legislation.

## **7. OBLIGATIONS OF THE CONTRACTOR AS TO THE FOI**

- (1) Without prejudice to the requirements of the FOI Act and EIRs and in particular without prejudice to sections 41 and 43 of the FOI Act and Regulation 12(5)(e) of the EIRs LTHTrust undertakes:
  - (a) that any information, or type or class of information, of the Partner Organisation of a confidential nature which is not Personal Data; or

- (b) any information which is designated with a confidentiality, security or privacy restriction according to the Partner Organisations Standing Orders, Standing Financial Instructions or other regulations having similar status in the administration of the Partner Organisation which is not Personal Data shall, for a period of six (6) years from the date of its disclosure, be treated at all times in accordance with such Standing Orders, Standing Financial Instructions or other regulations insofar as such have been communicated to LTHTrust:
    - (i) shall be used by LTHTrust, (or by any Staff in connection with the contract), solely for the purpose of tendering for or performance of the contract;
    - (ii) shall not be disclosed by LTHTrust, (or by Staff in connection with the contract), without the consent of the Partner Organisation except to such third party and to such extent as may be necessary, on a need-to-know basis, in connection with the Contract; and
  - (c) to put in place all necessary procedures and precautions to comply with (a) and (b) above.
- (2) LTHTrust acknowledges that the Partner Organisation is subject to the requirements of the FOIA and EIRs and shall assist and co-operate with the Partner Organisation to enable the Partner Organisation to comply with its disclosure obligations under the FOIA and EIRs. Accordingly LTHTrust agrees:
- (a) that this contract is subject to the obligations and commitments of the Partner Organisation under the FOIA and EIRs;
  - (b) that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under the FOIA or EIRs is a decision solely for the Partner Organisation to whom the request is addressed;
  - (c) that where LTHTrust receives a request for information under the FOIA or EIRs, it will not respond to such request (unless directed to do so by the Partner Organisation) and will promptly (and in any event within 2 working days) transfer the request to the Partner Organisation;
  - (d) The Partner Organisation, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of the FOIA, and regulation 16 of the Environmental Information Regulations 2004, may disclose information concerning LTHTrust and this contract either without consulting with LTHTrust, or following consultation with LTHTrust and having taken its views into account; and
  - (d) to assist the Partner Organisation in responding to a request for information, by processing information or environmental information

(as the same are defined in the FOIA) and EIRs in accordance with a records management system that complies with all applicable records management recommendations including the code of conduct issued under section 46 of the FOIA, and providing copies of all information requested by the Partner Organisation within 5 working days of such request.

## **8. DATA PROCESSOR REQUIREMENTS**

### **General**

1. The Partner Organisation and LTHTrust acknowledge that for the purposes of the Data Protection Legislation (as amended from time to time), The Partner Organisation is the Data Controller and LTHTrust is the Data Processor of any personal data. The details of the Processing carried out by LTHTrust on behalf of the Partner Organisation are set out in Annexure 2 which forms part of this contract.
2. LTHTrust warrants and undertakes to:
  - (a) Process the Partner Organisation Personal Data only in accordance with instructions from the Partner Organisation which are set out in Annexure 2 of this Agreement, or as provided in writing by the Partner Organisation to LTHTrust from time to time;
  - (b) Process the Partner Organisation Personal Data only to the extent, and in such manner, as is necessary for the purposes detailed in Clause 3 (above) and Annexure 2, or as is required by law or any regulatory body and shall process such personal data in compliance with all applicable Data Protection Legislation, laws, enactments, regulations, orders, standards and other similar instruments;
  - (c) assist and fully co-operate with the Partner Organisation as requested by the Partner Organisation from time to time to ensure the Partner Organisation's compliance with its obligations under the Data Protection Legislation which shall include, but not be limited to:
    - (i) completing and reviewing data protection impact assessments;
    - (ii) implementing measures to mitigate against any data protection risks;
    - (iii) implementing such technical and organisational measures to enable the Partner Organisation to respond to requests from Data Subjects exercising their rights under the Data Protection Legislation
  - (d) assist with any enquires from Regulators.

3. LTHTrust shall notify the Partner Organisation promptly (but in any event within 24 hours) should it:
  - (a) receive notice of any complaint made to a Regulator or any finding by a Regulator in relation to its Processing of Personal Data, whether it is the Partner Organisation's Personal Data or otherwise;
  - (b) be under a legal obligation to process the Partner Organisation's Personal Data, other than under the instructions of LTHTrust. In which case it shall inform the Partner Organisation of the legal obligation, unless the law prohibits such information being shared on important grounds of public interest;
  - (c) receives any request on behalf of a Data Subject of LTHTrust Personal Data, exercising their rights under the Data Protection Legislation;
  - (d) become aware that in following the instructions of LTHTrust, it shall be breaching Data Protection Legislation.

### **Security**

4. When Processing the Partner Organisation's Personal Data under this contract LTHTrust shall take all necessary technical and organisational precautions and measures to preserve the confidentiality and integrity of the Partner Organisation's Personal Data and prevent any unlawful processing or disclosure taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects. These shall include, but not be limited to:
  - (a) Encrypting the Partner Organisation's Personal Data stored on any mobile media or transmitted over public or wireless networks;
  - (b) Implementing and maintaining business continuity, disaster recovery and other relevant policies and procedures to ensure:
    - (i) the confidentiality, integrity, availability and resilience of processing systems and services; and
    - (ii) the availability and access to the Partner Organisation's Personal Data in a timely manner in the event of a physical or technical incident
  - (c) Ensuring that all Staff, employees and contractors who are involved in the Processing of the Partner Organisation's Personal Data are trained in the policies and procedures set out in Clause 8(4)(b) and are under contractual or statutory obligations of confidentiality concerning the Partner Organisation's Personal Data;
  - (d) Pseudonymise the Partner Organisation's Personal Data on request by the Partner Organisation.

(the "**Security Measures**").

5. The Security Measures shall be regularly tested by LTHTrust to assess the effectiveness of the measures in ensuring the security, confidentiality, integrity, availability and resilience of the Partner Organisation's Personal Data and LTHTrust shall maintain records of the testing.

### **Records of processing**

6. LTHTrust shall maintain accurate written records of the Processing it undertakes in connection with this contract which shall contain at a minimum:
  - (a) its details, the Partner Organisation's details, the details of its data protection officer;
  - (b) the categories of Processing carried out on behalf of the Partner Organisation;
  - (c) the details of any transfers to any third countries, where applicable, and the safeguards in place for that transfer; and
  - (d) an accurate record of the Security Measures it has in place.
- (7) LTHTrust shall provide the records set out in 8(4), 8(5) and (6) to the Partner Organisation or a Regulator on request.

### **Security breach notification**

- (8) The Partner Organisation shall notify the Partner Organisation promptly (and in any event no later than 24 hours of discovery) if it becomes aware of any actual, suspected or threatened unauthorised exposure, access, disclosure, Processing, use, communication, deletion, revision, encryption, reproduction or transmission of any component of the Partner Organisation's Personal Data, unauthorised access or attempted access or apparent attempted access (physical or otherwise) to the Partner Organisation's Personal Data or any loss of, damage to, corruption of or destruction of such Personal Data ("**Security Incident**");
9. The notification in Clause 8(8) shall include:
  - (a) The nature of the breach, including the categories and approximate number of Data Subjects and records concerned;
  - (b) The contact at LTHTrust who will liaise with the Partner Organisation concerning the breach;
  - (c) The remediation measures being taken to mitigate and contain the breach.



## **Audit**

10. LTHTrust shall provide all necessary information and assistance to the Partner Organisation in order for the Partner Organisation to verify LTHTrust's compliance with its obligations under this Agreement and the Data Protection Legislation including, without limitation:
  - (a) allowing the Partner Organisation and its advisors to inspect and make copies of the records required under this Clause 8; and
  - (b) allowing access to LTHTrust's premises on reasonable notice and provide all reasonable assistance to the Partner Organisation to enable the Partner Organisation to audit LTHTrust's compliance with the Security Measures.
11. The provisions of this Clause 8 (Data Processing Requirements) shall apply during the continuance of the contract and indefinitely after its expiry or termination.

## **9. TERMINATION OF THE CONTRACT AND LIABILITY**

- (1) If LTHTrust fails to comply with any provision of this contract then the Partner Organisation may summarily terminate the contract by notice given in writing to LTHTrust.
- (2) The Partner Organisation may terminate the contract if it deems the contract is completed to its satisfaction or if it deems that there is no further requirement to continue the contract.
- (3) Unless required by law, LTHTrust shall, upon termination or expiry of the contract for whatever reason, at the option of the Partner Organisation, either securely delete or return all the Partner Organisation's Personal Data to the Partner Organisation. If required by law to retain a copy, LTHTrust shall inform the Partner Organisation of what it is retaining and the legal reason why it needs to be retained.
- (4) LTHTrust will indemnify the Partner Organisation for any claims, direct or indirect costs, losses, damages, expenses (including legal expenses) and other outgoings sustained by or incurred by the Partner Organisation as a result of or arises out of LTHTrust's negligence or breach of this contract.
- (5) The Partner Organisation accepts legal liability for any inaccurate Partner Organisation personal data that is given to LTHTrust for the purpose of the contract to the extent it was aware of such inaccuracies.
- (6) The decision of the Partner Organisation upon matters arising under the conditions imposed by this clause 9 shall be final and conclusive.

## **10. CONFIDENTIALITY**

- (1) The Provisions of the Confidentiality Agreement detailed at Annexure 1 to this contract shall apply to the parties.

## **11. GENERAL**

- (1) No terms of this contract shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a third party.
- (2) This contract shall be governed by and construed in accordance with English law and each party agrees to submit to the non-exclusive jurisdiction of the English Courts over any claim or matter arising under or in connection with this contract.
- (3) In the event of any conflict between a term of this contract, a term of any software licence entered into between the parties, the following order of precedence shall apply:
  - (a) the term in this contract;
  - (b) the term in the relevant software licence entered into between the parties.
- (4) For the avoidance of doubt, the terms of this contract shall also apply to and be incorporated within (amended as applicable) any software licence, or other agreement made between the parties.
- (5) The Partner Organisation shall be entitled to assign, novate or otherwise dispose of its rights under this contract or any part thereof to any third party by giving LTHTrust prior notice of such assignment, novation or other disposal.
- (6) This contract is personal to LTHTrust. LTHTrust shall not assign, novate or otherwise dispose of this contract or any part thereof, or purport to do so, without the prior consent in writing of the Partner Organisation. LTHTrust shall not provide any third party with access to the Partner Organisation's Personal Data or sub-contract any of its obligations under this Agreement without the prior written approval of the Partner Organisation.
- (7) Where authority has been granted by the Partner Organisation to LTHTrust to engage any sub-contractor in accordance with clause 11(6), LTHTrust shall:
  - (a) Undertake due diligence on the sub-contractor equivalent to the Due Diligence undertaken on LTHTrust by the Partner Organisation under this contract; and
  - (b) Put in place contractual data processing provisions equivalent to those in place between LTHTrust and the Partner Organisation under this contract.

- (8) Where authority has been granted by the Partner Organisation to LTHTrust to engage any sub-contractor in accordance with clause 11(6), the any such subcontracting shall not relieve LTHTrust from any of its liabilities, obligations and responsibilities hereunder. LTHTrust shall perform all liabilities, obligations and responsibilities under this contractor as prime contractor and shall remain primarily responsible and liable for the activities sub-contracted and for such of the acts and omissions of the sub-contractors in respect of such activities as would render LTHTrust liable to the Partner Organisation, had such acts or omissions been LTHTrust's own acts and omissions.
- (9) This contract constitutes the whole agreement between the parties and supersedes all previous contracts, agreements or understandings between the parties relating to the subject matter of this contract.

## **12. ACCESS CONTROLS**

The Data Processor will manage the access to Data held on behalf of the Data Controller as follows:

### **12.1 Authorised Users (Staff Access)**

- 12.1.1 The Data Controller will authorise those staff whose access to the Data they consider to be necessary in order to perform their responsibility for the provision of direct health or social care services to the Data Subject.
- 12.1.2 The Data Controller will confirm the access rights they have authorised in writing to the Data Processor.
- 12.1.3 The Data Controller requires the Data Processor to undertake the agreed technical and organisational measures for access controls and shall ensure that access to the Data is limited to:
- (a) those persons whose access has been authorised by the Data Controller; and
  - (b) such part or parts of the Data as is strictly necessary for performance of that employee's duties.

## SIGNATORIES

| <b>For and on behalf of the Data Controller</b>                                        |  |
|----------------------------------------------------------------------------------------|--|
| Organisation/GP Practice name:                                                         |  |
| Organisation/GP Practice Address:                                                      |  |
| Name:                                                                                  |  |
| Signature:                                                                             |  |
| Position: <i>(DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)</i> |  |
| Date:                                                                                  |  |

| <b>For and on behalf of the Data Processor</b>                                         |                                                                    |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Organisation name:                                                                     | <b>The Leeds Teaching Hospitals NHS Trust</b>                      |
| Organisation address:                                                                  | St James University Hospital<br>Beckett Street<br>Leeds<br>LS9 7TF |
| Name:                                                                                  | Jagjivan Chagger                                                   |
| Signature:                                                                             |                                                                    |
| Position: <i>(DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)</i> | Head of Information Governance & Data Protection Officer           |
| Date                                                                                   |                                                                    |

**Annexure 2**

**Confidentiality Agreement**

**Dated: xxxxx**

**Confidentiality Agreement**

between

**<Insert Practice Name>**

and

**The Leeds Teaching Hospitals NHS Trust**

*CONTENTS*

CLAUSE

|     |                                                |    |
|-----|------------------------------------------------|----|
| 1.  | Definitions and interpretation .....           | 15 |
| 2.  | Obligations of confidentiality .....           | 17 |
| 3.  | Return of information .....                    | 18 |
| 4.  | Reservation of rights and acknowledgement..... | 6  |
| 5.  | Warranty and indemnity .....                   | 7  |
| 6.  | Term and termination.....                      | 7  |
| 7.  | Entire agreement and variation.....            | 20 |
| 8.  | No waiver .....                                | 8  |
| 9.  | Assignment .....                               | 8  |
| 10. | Notices .....                                  | 8  |
| 11. | No partnership .....                           | 9  |
| 12. | Third party rights .....                       | 9  |
| 13. | Governing law and jurisdiction.....            | 9  |

**THIS AGREEMENT** is dated [DATE]

## **Parties**

- (1) <Insert Practice Name> incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (**Defined Term For Party**).
- (2) The Leeds Teaching Hospitals NHS Trust of Trust Headquarters, St James University Hospital, Beckett Street, Leeds LS9 7TF (**LTHTrust**);

## **Background**

Each party wishes to disclose to the other party Confidential Information in relation to the Purpose. Each party wishes to ensure that the other party maintains the confidentiality of its Confidential Information. In consideration of the benefits to the parties of the disclosure of the Confidential Information, the parties have agreed to comply with the following terms in connection with the use and disclosure of Confidential Information.

## **Agreed terms**

### **1. Definitions and interpretation**

- 1.1 The following definitions and rules of interpretation in this clause apply in this agreement:

**Business Day:** a day (other than a Saturday, Sunday or public holiday) when banks in London are open for business.

**Confidential Information:** all information, which is by its nature confidential, (however recorded, preserved or disclosed) disclosed by a party or its employees, officers, representatives or advisers (together, its Representatives) to the other party and that party's Representatives including but not limited to:

- (a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;
- (b) any information that would be regarded as confidential by a reasonable business person relating to:
  - (i) the business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Disclosing Party; and
  - (ii) the operations, processes, product information, know-how, designs, trade secrets or software of the Disclosing Party;
- (c) any information or analysis derived from Confidential Information; and
- (d) any information detailed in Schedule [1];

but not including any information that:

- (e) is or becomes generally available to the public other than as a result of its disclosure by the Recipient or its Representatives in breach of this agreement or of any other undertaking of confidentiality addressed to the party to whom the information relates (except that any compilation of otherwise public information in a form inaccessible to the public shall nevertheless be treated as Confidential Information); or
- (f) was available to the Recipient on a non-confidential basis prior to disclosure by the Disclosing Party; or
- (g) was, is or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's knowledge, is not bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient; or
- (h) was lawfully in the possession of the Recipient before the information was disclosed to it by the Disclosing Party; or
- (i) the parties agree in writing is not confidential or may be disclosed; or
- (j) is developed by or for the Recipient independently of the information disclosed by the Disclosing Party; or
- (k) is trivial, obvious or useless.

**Disclosing Party:** a party to this agreement which discloses or makes available directly or indirectly Confidential Information.

**Purpose:** [STATE THE PURPOSE, FOR EXAMPLE, THE EVALUATION OR ESTABLISHMENT OF A COLLABORATION IN RESPECT OF A PARTICULAR PROJECT].

**Recipient:** a party to this agreement which receives or obtains directly or indirectly Confidential Information.

**Representative:** employees, agents and other representatives acting on behalf of a party.

- 1.2 Clause, schedule and paragraph headings shall not affect the interpretation of this agreement.
- 1.3 A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors and permitted assigns.
- 1.4 The schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the schedules.



- 1.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural include the singular.
- 1.6 A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment, and includes any subordinate legislation for the time being in force made under it.
- 1.7 Any obligation in this agreement on a person not to do something includes an obligation not to agree or allow that thing to be done.
- 1.8 References to clauses and schedules are to the clauses and schedules of this agreement; references to paragraphs are to paragraphs of the relevant schedule.
- 1.9 To the extent there is any inconsistency between the provisions of the main body of this agreement and any schedule to this agreement, the front end of this agreement shall prevail.

## **2. Obligations of confidentiality**

- 2.1 The Recipient shall, and shall procure that its Representatives shall, keep the Disclosing Party's Confidential Information confidential and, except with the prior written consent of the Disclosing Party, shall:
  - (a) not use or exploit the Confidential Information in any way except for the Purpose;
  - (b) not disclose or make available the Confidential Information in whole or in part to any third party, except as expressly permitted by this agreement;
  - (c) not copy, reduce to writing or otherwise record the Confidential Information except as strictly necessary for the Purpose (and any such copies, reductions to writing and records shall be the property of the Disclosing Party);
  - (d) not use, reproduce, transform, or store the Confidential Information in an externally accessible computer or electronic information retrieval system or transmit it in any form or by any means whatsoever outside of its usual place of business;
  - (e) keep separate the Confidential Information from all documents and other records of the Recipient;
  - (f) apply the same security measures and degree of care to the Confidential Information as the Recipient applies to its own confidential information, which the Recipient warrants as providing adequate protection from unauthorised disclosure, copying or use;
  - (g) keep a written record of: any document or other Confidential Information received from the other in tangible form; any copy made of the Confidential Information; and

- 2.2 The Recipient may only disclose the Disclosing Party's Confidential Information to those of its Representatives who need to know this Confidential Information for the Purpose, provided that:
- (a) it informs these Representatives of the confidential nature of the Confidential Information before disclosure and obtains from its Representatives enforceable undertakings to keep the Confidential Information confidential in terms at least as extensive and binding upon the Representatives as the terms of this agreement are upon the parties; and
  - (b) at all times, it is responsible for these Representatives' compliance with the obligations set out in this agreement.
- 2.3 A party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority (including, without limitation, by a court or other authority of competent jurisdiction) provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of this disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause 2.3, it takes into account the reasonable requests of the other party in relation to the content of this disclosure.
- 2.4 The Recipient shall establish and maintain adequate security measures (including any reasonable security measures proposed by the Disclosing Party from time to time) to safeguard the Confidential Information from unauthorised access or use.
- 2.5 No party shall make, or permit any person to make, any public announcement concerning this agreement, the Purpose or its prospective interest in the Purpose without the prior written consent of the other party (such consent not to be unreasonably withheld or delayed) except as required by law or any governmental or regulatory authority (including, without limitation, any relevant securities exchange) or by any court or other authority of competent jurisdiction. No party shall make use of the other party's name or any information acquired through its dealings with the other party for publicity or marketing purposes without the prior written consent of the other party.
- 2.6 The Recipient shall ensure that incident reporting mechanisms are in place with the Trust which ensures the reporting of any incidents, their causes and resolving actions pertaining related to this contract and its purpose are communicated to the Trust.

### **3. Return of information**

- 3.1 At the request of the Disclosing Party, the Recipient shall:
- (a) destroy or return to the Disclosing Party all documents and materials (and any copies) containing, reflecting, incorporating, or based on the Disclosing Party's Confidential Information;

- (b) erase all the Disclosing Party's Confidential Information from its computer systems or which is stored in electronic form (to the extent possible); and
  - (c) certify in writing to the Disclosing Party that it has complied with the requirements of this clause, provided that the Recipient may retain documents and materials containing, reflecting, incorporating, or based on the Disclosing Party's Confidential Information to the extent required by law or any applicable governmental or regulatory authority and to the extent reasonable to permit the Recipient to keep evidence that it has performed its obligations under this agreement. The provisions of this clause 3 shall continue to apply to any such documents and materials retained by the Recipient, subject to clause 6.1.
- 3.2 If the Recipient develops or uses a product or a process which, in the reasonable opinion of the Disclosing Party, might have involved the use of any of the Disclosing Party's Confidential Information, the Recipient shall, at the request of the Disclosing Party, supply to the Disclosing Party information reasonably necessary to establish that the Disclosing Party's Confidential Information has not been used or disclosed.

#### **4. Reservation of rights and acknowledgement**

- 4.1 All Confidential Information shall remain the property of the Disclosing Party. Each party reserves all rights in its Confidential Information. No rights, including, but not limited to, intellectual property rights, in respect of a party's Confidential Information are granted to the other party and no obligations are imposed on the Disclosing Party other than those expressly stated in this agreement.
- 4.2 Except as expressly stated in this agreement, no party makes any express or implied warranty or representation concerning its Confidential Information, or the accuracy or completeness of the Confidential Information.
- 4.3 The disclosure of Confidential Information by the Disclosing Party shall not form any offer by, or representation or warranty on the part of, the Disclosing Party to enter into any further agreement in relation to the Purpose, or the development or supply of any product or service to which the Confidential Information relates.
- 4.4 The Recipient acknowledges that damages alone would not be an adequate remedy for the breach of any of the provisions of this agreement. Accordingly, without prejudice to any other rights and remedies it may have, the Disclosing Party shall be entitled to the granting of equitable relief (including without limitation injunctive relief) concerning any threatened or actual breach of any of the provisions of this agreement.
- 4.5 The Recipient shall be liable to the Disclosing Party for the actions or omissions of the Recipient's Representatives under this agreement, as if they were the actions or omissions of the Recipient.

## **5. Warranty and indemnity**

- 5.1 Each Disclosing Party warrants that it has the right to disclose its Confidential Information to the Recipient and to authorise the Recipient to use such Confidential Information for the Purpose.
- 5.2 Each Recipient shall indemnify and keep fully indemnified the Disclosing Party at all times against all liabilities, costs (including legal costs on an indemnity basis), expenses, damages and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and other reasonable costs and expenses suffered or incurred by the Disclosing Party) arising from any breach of this agreement by the Recipient and from the actions or omissions of any Representative of the Recipient.

## **6. Term and termination**

- 6.1 If either party decides not to become, or continue to be involved in the Purpose with the other party it shall notify the other party in writing immediately. The obligations of each party shall, notwithstanding any earlier termination of negotiations or discussions between the parties in relation to the Purpose, continue for a period of **3** years from the termination of this agreement.
- 6.2 Termination of this agreement shall not affect any accrued rights or remedies to which either party is entitled.

## **7. Entire agreement and variation**

- 7.1 This agreement constitutes the whole agreement between the parties and supersedes all previous agreements between the parties relating to its subject matter. Each party acknowledges that, in entering into this agreement, it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in this agreement. Nothing in this clause shall limit or exclude any liability for fraud or for fraudulent misrepresentation.
- 7.2 No variation of this agreement shall be effective unless it is in writing and signed by each of the parties (or their authorised representatives).

## **8. No waiver**

- 8.1 Failure to exercise, or any delay in exercising, any right or remedy provided under this agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict any further exercise of that or any other right or remedy.
- 8.2 No single or partial exercise of any right or remedy provided under this agreement or by law shall preclude or restrict the further exercise of that or any other right or remedy.

## 9. Assignment

Except as otherwise provided in this agreement, no party may assign, sub-contract or deal in any way with, any of its rights or obligations under this agreement or any document referred to in it.

## 10. Notices

10.1 Any notice required to be given under this agreement, shall be in writing and shall be delivered personally, or sent by pre-paid first class post or recorded delivery or by commercial courier, to each party required to receive the notice [or communication] at its address as set out below:

- (a) LTHTrust: Mr Jagjivan Chagger, Head of Information Governance & Data Protection Officer, 2nd Floor, Trust Headquarters, St James University Hospital, Beckett Street, Leeds, LS9 7TF.
- (b) <Insert Practice Name>: [CONTACT NAME] [ADDRESS]

or as otherwise specified by the relevant party by notice in writing to each other party.

10.2 Any notice shall be deemed to have been duly received:

- (a) if delivered personally, when left at the address and for the contact referred to in this clause; or
- (b) if sent by pre-paid first class post or recorded delivery, at [9.00 am] on the [second] Business Day after posting; or
- (c) if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed.

10.3 A notice required to be given under this agreement shall not be validly given if sent by e-mail.

## 11. No partnership

Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party as the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

## 12. Third party rights

A person who is not a party to this agreement shall not have any rights under or in connection with it.

## 13. Governing law and jurisdiction

13.1 This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.

- 13.2 The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This agreement has been entered into on the date stated at the beginning of it.

### SIGNATORIES

| <b>For and on behalf of the Data Controller</b>                                        |  |
|----------------------------------------------------------------------------------------|--|
| Organisation/GP Practice name:                                                         |  |
| Organisation/GP Practice Address:                                                      |  |
| Name:                                                                                  |  |
| Signature:                                                                             |  |
| Position: <i>(DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)</i> |  |
| Date:                                                                                  |  |

| <b>For and on behalf of the Data Processor</b>                                         |                                                                    |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Organisation name:                                                                     | <b>The Leeds Teaching Hospitals NHS Trust</b>                      |
| Organisation address:                                                                  | St James University Hospital<br>Beckett Street<br>Leeds<br>LS9 7TF |
| Name:                                                                                  | Jagjivan Chagger                                                   |
| Signature:                                                                             |                                                                    |
| Position: <i>(DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)</i> | Head of Information Governance & Data Protection Officer           |
| Date                                                                                   |                                                                    |

## SCHEDULE 1

### The Leeds Care Record

The Leeds Care Record (LCR) system is being developed by the health and social care partners with the intention of creating a joint electronic care record for service users (patients and social care clients) within the Leeds area.

The LCR will support the delivery of integrated care by providing health and social care teams working together with a single point of access to information about the service user, collected from their separate medical and social care records.

For the purpose of this agreement, the Health and Social Care partners within Leeds Health and Social Care Economy are Data Controllers.

LTHTrust “hosts” the system and therefore acts as a ‘Data Processor’ to process personal data and sensitive personal data on behalf of the Leeds Health and Social Care Provider Data Controllers, in accordance with this contract.

LTHTrust is also the Data Controller for LTHTrusts patients’ personal data.

For the development of the LCR; Ocean Informatics UK act as a sub-Data Processor to LTHTrust in their provision of development resources for the construction of the system. The server used for the development of the Leeds Care Record will be stored by Tactix4 who are a sub-Data Processor of Ocean Informatics UK. It is vital that the developers share access to the information in order to ensure that the software product meets the highest standards of security, integrity and reliability.

The Legal basis for processing this data is cover by GDPR Article 6.1 (e) and Article 9.2(h).

- e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*



## **SCHEDULE 2**

### **ACCESS CONTROLS**

LTHTrust will manage the Leeds Care Record (LCR) authentication and access control function on behalf of the joint Data Controllers.

#### **RBAC Roles**

Access to the LCR will only be permitted to staff authorised by the Data Controllers, who have completed the registration process and obtained their own unique personal username and password.

Access to the LCR will be regulated under Role Bases Access Controls (RBAC)

The LCR RBAC functionality provides the ability to create “Roles” associated with specific activities that allow the user to perform tasks relevant to their role. Roles contain the various permissions available within the system. Roles can be edited once created. Users created on LCR can be assigned one or many roles. Access categories from each organisation will be approved by the LCR Project Board.

#### **Audit and breach reporting**

LTHTrust will report any detected or reported breach of access to the LCR system to the relevant Data Controller responsible for the member of staff who committed the breach.

The Data Controller will be responsible for investigating and managing the incident in accordance with NHS procedures and for instigating appropriate disciplinary proceedings.

The Data Controller will be responsible for notifying any other Data Controller about the incident where it is appropriate to do so i.e. where the breach involves unauthorised access to personal data they are responsible for.

LTHTrust will maintain a record of all detected or reported breaches and provide the LCR Project Board with a quarterly report in order to monitor systemic problems, identify risks and instigate remedial actions. See also Schedule 4.

#### **User Responsibilities**

Everyone granted authorised access to the LCR is issued a personal password, which forms part of their personal access credentials.

All personal password holders are responsible for:

- Changing their supplied password upon first log in to a unique personal password to make it secure.
- Always keeping their password private and confidential.

- Never sharing their password with anyone, this includes managers.
- Never writing down or recording their password where it can be accessed by anyone other than themselves. Recording passwords is not recommended; therefore passwords should only be recorded when absolutely necessary.
- Changing each of their passwords on a regular basis.

Accessing or attempting to access any part of the LCR other than your authorised personal user Identity without the appropriate authority will constitute an Information Governance breach.

It is not permitted at any time to use another person's personal username and password. The person whose log on credentials are used will be held accountable for all actions during access; inappropriate access will result in disciplinary action for both parties.

## SCHEDULE 3

### MANAGEMENT PROCEDURES FOR REQUESTS TO OPT-OUT OF THE LCR.

The Leeds Care Record (LCR) system is being jointly developed by Health and Social Care providers with the intention of creating a joint electronic record for service providers within the Leeds area.

The system allows Care Professionals within the Leeds Health and Social Care community to view, and where appropriate update, personal and sensitive information about service users. The information held on this system will include Social Care data, as well as data provided by other primary and secondary healthcare providers in the Leeds Health community.

The NHS Constitution established the following rights:

- You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure.
- You have the right to be informed about how your information is used.
- Where identifiable information has to be used, to give you the chance to object wherever possible (pledge)<sup>1</sup>

An individual can chose to opt-out of having a LCR created.

LTHT will manage the opt-out process on behalf of the joint Data Controllers as follows.

Opt Out Process:

- The service user will contact the Information Governance Team at Leeds Teaching Hospitals NHS Trust (LTHT) to confirm that they would like to Opt Out of sharing their personal information or sensitive personal information relating to them via the LCR system.
- The service user will be requested to verify their demographics details and date of birth.
- The Information Governance Team records the patient's NHS Number, Name, Address, and Date of Birth and will advise the patient that it will take up to 2 working days to remove them from the LCR system.
- The LTHT Information Governance Team will keep a record that the patient has Opted Out.
- The service users details will then be forwarded to LTHT system administration team to action the removal from the LCR system.

---

<sup>1</sup> NHS Constitution for England 2013 Section 3a Patients and the Public – your rights and NHS pledges to you. Department of Health March 2013.

- The GP for the service user will be sent a letter to confirm that their patient has opted out of the LCR.
- The service user will be sent a confirmation letter informing them that their information will not be shared via the LCR system. Within the letter the service user will be advised upon the potential negative impact to their health care as a result of opting out of the LCR. The letter will also include instructions on how to 'Opt In' to the LCR.
- If a request for removal is made on behalf of a child/young person or an individual who is unable to make decisions is received, the LTHT's Information Governance Team will seek guidance from the service user's GP to ensure so that an assessment can be made, to ensure that the requester is acting in the best interests of the patient.

An individual at any time can chose to opt back into having a LCR created.

LTHT will manage the Opt-In process on behalf of the joint Data Controllers as follows.

Opt back in Process:

- The service user will contact the Information Governance Team at Leeds Teaching Hospitals NHS Trust (LTHT) to confirm that they would like to Opt back in to the sharing their personal information or sensitive personal information relating to them via the LCR system.
- The service user will be requested to verify their demographics details and date of birth.
- The Information Governance Team records the patient's NHS Number, Name, Address, and Date of Birth and will advise the patient that it will take up to 2 working days to reinstate their record into the LCR system.
- The LTHT Information Governance Team will keep a record that the patient has Opted back in.
- The service users details will then be forwarded to LTHT system administration team to action the removal of the Opt Out status from the LCR system.
- The GP for the service user will be sent a letter to confirm that their patient has opted back in to the LCR.

- The service user will be sent a confirmation letter informing them that their information will now be shared via the LCR system.

## **SCHEDULE 4**

### **INFORMATION GOVERNANCE BREACHES**

This procedure describes the stages when a user of The Leeds Care Record (LCR) accesses service user information within the LCR to which they are not entitled.

#### **Break Glass Function**

The LCR has a 'Break Glass' function which allows authorised users of the LCR to access service user information that is restricted. The stages outlined below define the process for the data processor in relation to the Break Glass function:

- The LCR will flag service user records where the break glass function has been invoked.
- If there is not a valid reason the LTHT IG Team will contact the GP Practice or the IG Organisational lead for the LCR user to inform them of the potential inappropriate access.

#### **Complaint by a service user/LCR user regarding LCR access**

A service user or LCR user may have concerns in with regards to LCR users accessing records where the LCR user is not involved in the direct care for the service user or there is no legitimate reason for access. The stages outlined below define the process for the Data Processor in relation to the Complaint by a service user/LCR user regarding LCR access:

- The IG Team for the LCR user shall contact the LTHT IG Team to request an audit and any supporting documentation
- The LTHT IG will provide the requested documentation.

### Annexure 3

#### Schedule of Processing, Personal Data and Data Subjects

1. The Contractor shall comply with any further written instructions with respect to processing by LTHTrust.
2. Any such further instructions shall be incorporated into this Schedule.

| Description                                                                                                                                                  | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject matter of the processing                                                                                                                             | <i>[This should be a high level, short description of what the processing is about i.e. its subject matter]</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Duration of the processing                                                                                                                                   | <i>Duration of contract.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Nature and purposes of the processing                                                                                                                        | <p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.]</i></p> <p><i>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p> |
| Type of Personal Data                                                                                                                                        | <i>Name, address, demographics and medical records</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Categories of Data Subject                                                                                                                                   | <i>Patients, members of the public, etc</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | <i>N/A</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |