Dated: xx/xx/xxxx

Data Protection Agreement

Between

xxxx

&

Humber Teaching NHS Foundation Trust

For the Provision of the Processing of Data within System of Systems for the Yorkshire & Humber Care Record

Data Protection Agreement

1. DATED: xx/xx/xxxx

2. PARTIES:

This agreement is made between the following parties:-

[Insert Organisation Name], ("Partner Organisation"), whose registered office is [ADDRESS].

Humber Teaching NHS Foundation Trust (''Organisation'') Trust HQ, Willerby Hill | Beverley Road | Willerby | HU10 6ED.

3. RECITALS

(1) This agreement is for the sole purpose of carrying out The development of the Yorkshire and Humber Care record 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 YHCR

(2) The agreement shall be deemed to have commenced on **xx/xx/xxxx** and shall terminate upon 3 months written notice of either party to the other, such termination not to be effective before **xx/xx/xxxx** unless this agreement is terminated earlier in accordance with its terms.

4. STATUTARY PROVISIONS

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

4.1 Where it is a NHS agreement (a agreement between two health service bodies) the NHS Act 2006 section 9 shall apply insofar as a NHS agreement 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 agreement 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 agreement, 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 Humber Teaching NHS Foundation Trust.

"**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 Humber Teaching NHS Foundation Trust is bound to comply.

"**Partner Organisation Personal Data**" means Personal Data Processed by Humber Teaching NHS Foundation Trust on behalf of the Partner Organisation under or in connection with this agreement.

“**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 Humber Teaching NHS Foundation Trust to perform its obligations under the agreement together with Humber Teaching NHS Foundation Trust servants, agents, suppliers and sub-contractors used in the performance of any of its obligations whether or not under this agreement.

This agreement 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 agreement or which may come into the possession of Humber Teaching NHS Foundation Trust or any Staff as a result of or in connection with the agreement; and

(b) to provide all necessary precautions to ensure that all Partner Organisation Personal Data is treated as confidential by Humber Teaching NHS Foundation Trust 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 agreement; 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) Humber Teaching NHS Foundation Trust shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this contact 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 Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust:-

(i) shall be used by Humber Teaching NHS Foundation Trust (or by any Staff in connection with the agreement), solely for the purpose of tendering for or performance of the agreement;

(ii) shall not be disclosed by Humber Teaching NHS Foundation Trust], (or by Staff in connection with the agreement), 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 agreement; and

(c) to put in place all necessary procedures and precautions to comply with (a) and (b) above.

(2) Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust agrees:-

(a) that this agreement 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 Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust and this agreement either without consulting with Humber Teaching NHS Foundation Trust, or following consultation with Humber Teaching NHS Foundation Trust and having taken its views into account; and

(ed) 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 Humber Teaching NHS Foundation Trust acknowledge that for the purposes of the Data Protection Legislation (as amended from time to time), The Partner Organisation is the Data Controller and Humber Teaching NHS Foundation Trust is the Data Processor of any personal data. The details of the Processing carried out by Humber Teaching NHS Foundation Trust on behalf of the Partner Organisation are set out in Annexure 3 which forms part of this agreement.

2. Humber Teaching NHS Foundation Trust 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 3of this Agreement, or as provided in writing by the Partner Organisation to Humber Teaching NHS Foundation Trust 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 3 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. Humber Teaching NHS Foundation Trust 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 [Insert Organisation Name]. 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 partner organisation's Personal Data, exercising their rights under the Data Protection Legislation;

(d) become aware that in following the instructions of partner organisation it shall be breaching Data Protection Legislation.

Security

4. When Processing the Partner Organisation's Personal Data under this agreement Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust to assess the effectiveness of the measures in ensuring the security, confidentiality, integrity, availability and resilience of the Partner Organisation's Personal Data and Humber Teaching NHS Foundation Trust shall maintain records of the testing.

Records of processing

6. Humber Teaching NHS Foundation Trust shall maintain accurate written records of the Processing it undertakes in connection with this agreement 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) Humber Teaching NHS Foundation Trust 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) Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust who will liaise with the Partner Organisation concerning the breach;

(c) The remediation measures being taken to mitigate and contain the breach.

Audit

10. Humber Teaching NHS Foundation Trust shall provide all necessary information and assistance to the Partner Organisation in order for the Partner Organisation to verify Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust premises on reasonable notice and provide all reasonable assistance to the Partner Organisation to enable the Partner Organisation to audit Humber Teaching NHS Foundation Trust's compliance with the Security Measures.

11. The provisions of this Clause 8 (Data Processing Requirements) shall apply during the continuance of the agreement and indefinitely after its expiry or termination.

9. TERMINATION OF THE AGREEMENT AND LIABILITY

(1) If Humber Teaching NHS Foundation Trust fails to comply with any provision of this agreement, then the Partner Organisation may summarily terminate the agreement by giving 30 days' notice in writing to Humber Teaching NHS Foundation Trust.

(2) The Partner Organisation may terminate the agreement if it deems the agreement is completed to its satisfaction or if it deems that there is no further requirement to continue the agreement.

(3) Unless required by law, Humber Teaching NHS Foundation Trust shall, upon termination or expiry of the agreement 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, Humber Teaching NHS Foundation Trust shall inform the Partner Organisation of what it is retaining and the legal reason why it needs to be retained.

(4) Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust's negligence or breach of this agreement.

(5) The Partner Organisation accepts legal liability for any inaccurate Partner Organisation personal data that is given to Humber Teaching NHS Foundation Trust for the purpose of the agreement to the extent it was aware of such inaccuracies.

(6) The decision of the Partner Organisation to terminate the agreement shall be final and conclusive.

10. CONFIDENTIALITY

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

11. GENERAL

(1) No terms of this agreement shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a third party.

(2) This agreement 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 agreement.

(3) The Partner Organisation shall be entitled to assign, novate or otherwise dispose of its rights under this agreement t or any part thereof to any third party by giving Humber Teaching NHS Foundation Trust prior notice of such assignment, novation or other disposal.

(4) This agreement is personal to [Insert Organisation Name]. Humber Teaching NHS Foundation Trust shall not assign, novate or otherwise dispose of this agreement or any part thereof, or purport to do so, without the prior consent in writing of the Partner Organisation. Humber Teaching NHS Foundation Trust 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.

(5) Where authority has been granted by the Partner Organisation to Humber Teaching NHS Foundation Trust to engage any sub-contractor in accordance with clause 11(6), Humber Teaching NHS Foundation Trust shall:

(a) Undertake due diligence on the sub-contractor equivalent to the Due Diligence undertaken on Humber Teaching NHS Foundation Trust by the Partner Organisation under this agreement; and

(b) Put in place contractual data processing provisions equivalent to those in place between Humber Teaching NHS Foundation Trust and the Partner Organisation under this contract.

(6) Where authority has been granted by the Partner Organisation to Humber Teaching NHS Foundation Trust to engage any sub-contractor in accordance with clause 11(6), then any such subcontracting shall not relieve Humber Teaching NHS Foundation Trust from any of its liabilities, obligations and responsibilities hereunder. Humber Teaching NHS Foundation Trust 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 Humber Teaching NHS Foundation Trust liable to the Partner Organisation, had such acts or omissions been Humber Teaching NHS Foundation Trust 's own acts and omissions.

(7) This agreement constitutes the whole agreement between the parties and supersedes all previous agreement, agreements or understandings between the parties relating to the subject matter of this agreement.

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

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

For and on behalf of the Data Processor	
Organisation name:	
Organisation address:	
Name:	
Signature:	
Position:(*DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)*	
Date	

Annexure 2

Confidentiality Agreement

Dated: xx/xx/xxxx

Confidentiality Agreement

between

XXXX

and

XXXX

CONTENTS

CLAUSE

THIS AGREEMENT is dated xx/xx/xxxx

Parties

(1) <Insert Organisation Name> incorporated whose registered office is [ADDRESS] (**Defined Term For Party**).

(2) **Humber Teaching NHS Foundation Trust** (''Organisation'') Trust HQ | Willerby Hill | Beverley Road | Willerby | HU10 6ED

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: The YHCR 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 Yorkshire and Humber region area.

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 the confidential information;

(e) keep separate the Confidential Information from all documents and other records of the Recipient until the point of ‘direct care’ after which the records are then separated;

(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 agreement 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) Humber Teaching NHS Foundation Trust: Trust HQ | Willerby Hill | Beverley Road | Willerby | HU10 6ED

(b) <Insert Organisation 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) sent by pre-paid first class post or recorded delivery,

(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

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

For and on behalf of the Data Processor	
Organisation name:	Humber Teaching NHS Foundation Trust
Organisation address:	Trust HQ, Willerby Hill Beverley Road Willerby HU10 6ED
Name:	
Signature:	
Position:(*DPO/SIRO/Caldicott Guardian or equivalent senior accountable person)*	
Date	

SCHEDULE 1

The Yorkshire and Humber Care Record (YHCR)

The YHCR 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 Yorkshire and Humber Care Record area.

The YHCR 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 Yorkshire and Humber Care Record Health and Social Care Economy are Data Controllers.

Humber Teaching NHS Foundation Trust "hosts" the system and therefore acts as a 'Data Processor' to process personal data and sensitive personal data on behalf of the Yorkshire and Humber Care Record Health and Social Care Provider Data Controllers, in accordance with this agreement.

Humber Teaching NHS Foundation Trust is also the Data Controller for Humber Teaching NHS Foundation Trust patients' personal data.

For the development of the YHCR; The Rotherham NHS Foundation Trust (TRFT) acts as a sub-data processor to Humber Teaching NHS Foundation Trust in their provision of development resources for the construction of the system. The server(s) used for the development of the YHCR will be stored by Synanetics who are a sub-data processor of TRFT. 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;

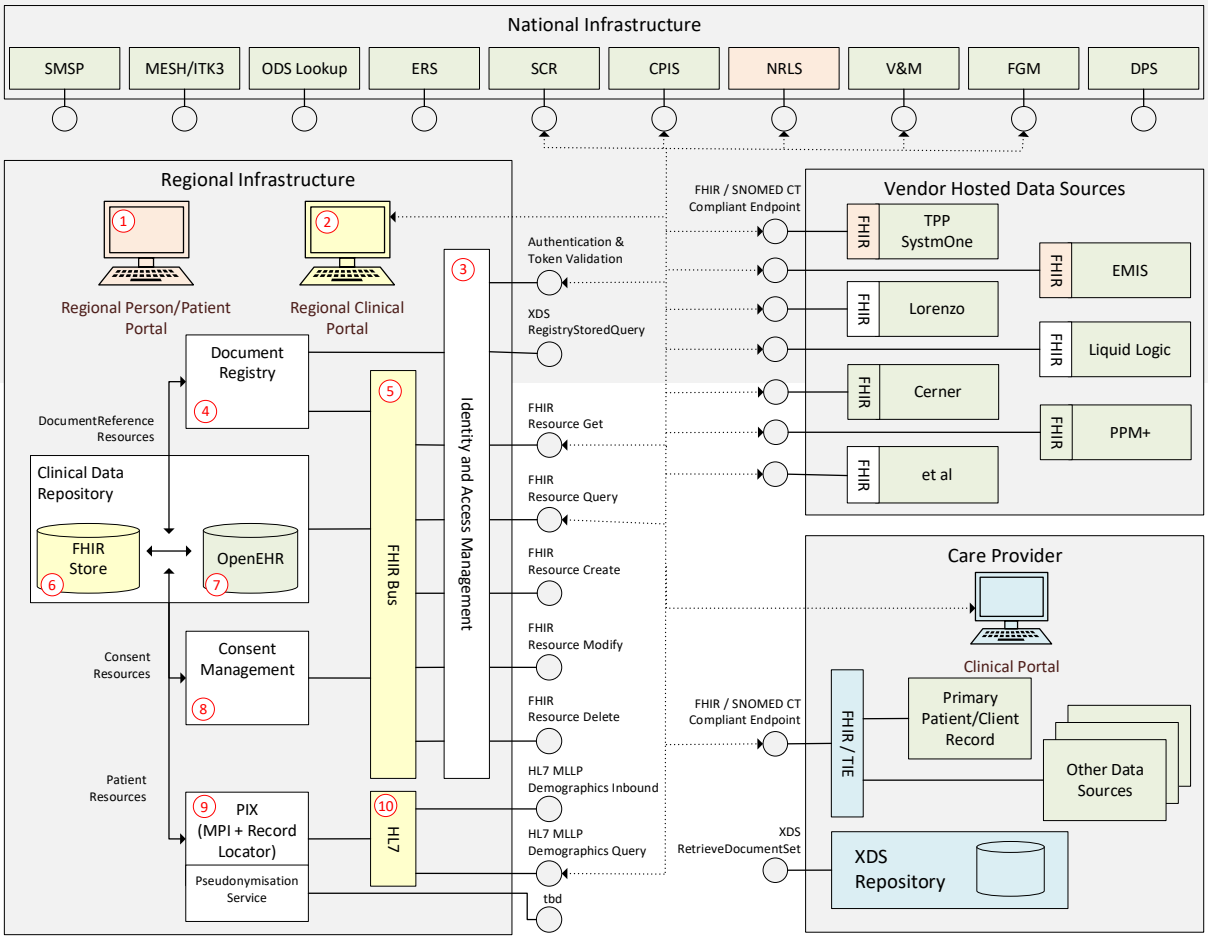
h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Overview of the Yorkshire & Humber Care Record Architecture

The architecture is a vendor neutral federated approach to sharing data between care providers.

The architecture enables existing systems to contribute to a shared care record. The architecture is designed to allow the shared care record to be displayed in any technically capable user interface and affords the possibility that different care providers will have different ways of making the record available for their care professionals.

The architecture is federated because it keeps data where it originates. Whilst some non-place-based data will be held regionally, there is no intention to create a central data lake. Instead, data is obtained when it is needed, on demand, from the organisation that created the data. This approach ensures that data is always current, ensures that there is one view of a patient, and places governance responsibility for data in the hands of the organisation that controls it.



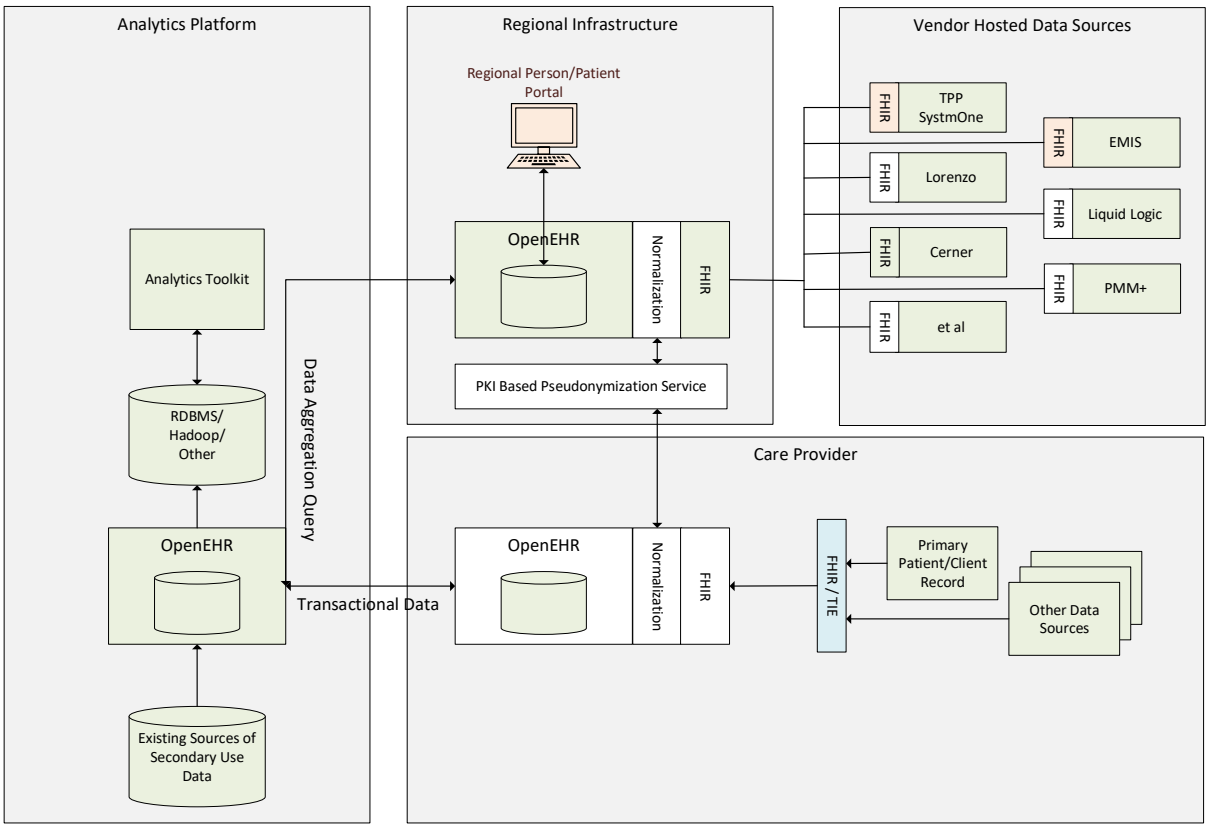
Data Providers and Data Consumers

Care settings are peers in the federated architecture. A care setting is a source of data which can be accessed by another care setting or data consumer. Regional systems act as orchestrators of this relationship.

The ultimate goal for the LHCRE is to provide full coverage across a clinical record regardless of where the parts of the record have been captured.

A data consumer is not restricted to a user interface which renders a consolidated care record. A data consumer may be a system that responds to, say, a diagnosis or observation being made in a care setting, perhaps auto-enrolling a patient on a care pathway or performing a safeguarding function. The Fast Healthcare Interoperability Resources (FHIR) standard specifies enabling mechanisms for data subscriptions such as messaging which will be adopted as regional standards. A data consumer may also be using data for secondary use purposes.

Data Flow Map



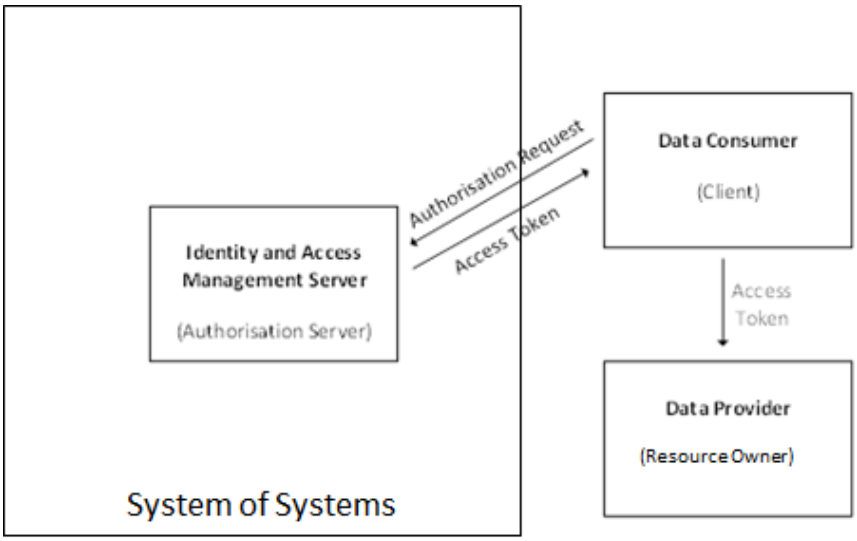
SCHEDULE 2

ACCESS CONTROLS

Data consumer organisations will manage the YHCR authentication and access control function on behalf of the joint Data Controllers.

User Authorisation and Access Token Management

Identity Access Management (IAM) adopts OAuth2 (https://oauth.net/2/) for its authorisation function. OAuth2 actors and their alignment with components of the system of systems is illustrated below.



The resource owner's authorisation is implied and the authorisation server will issue an access token without obtaining an authorisation grant from the resource owner.

Audit and breach reporting

Rotherham will report any detected or reported breach of access to the YHCR system to the relevant Data Controller responsible for the member of staff who committed the breach whilst the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.

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

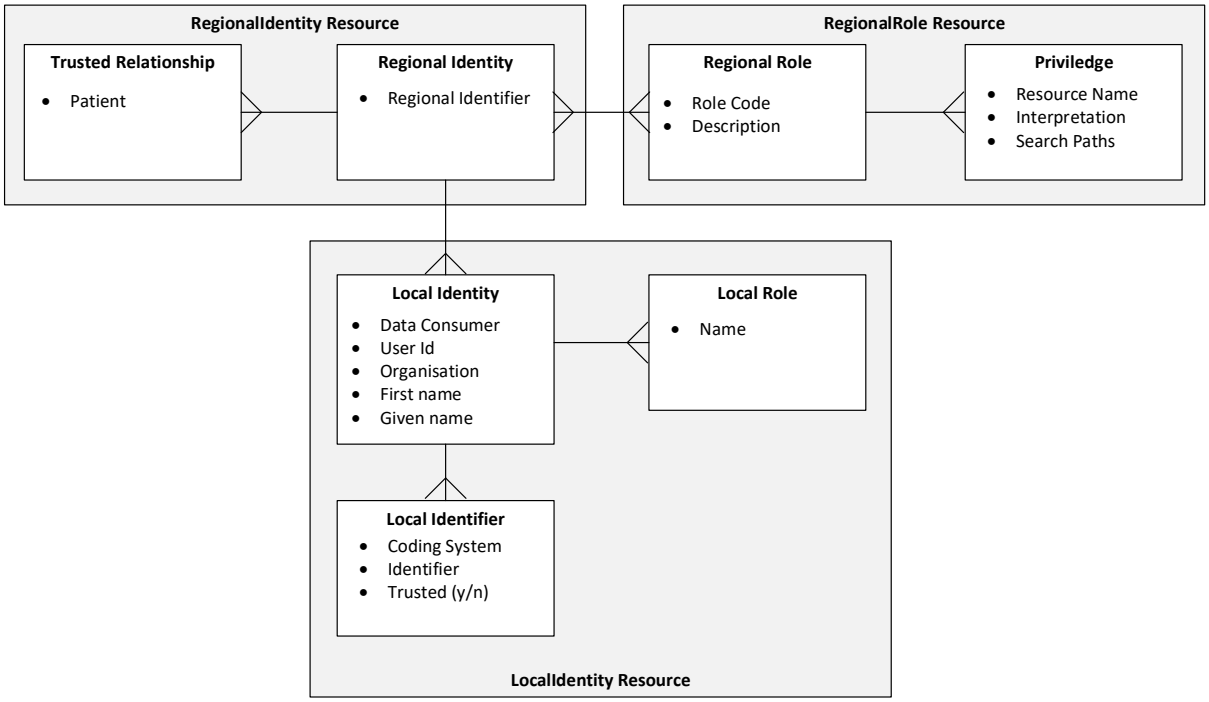
The Data Controller will be responsible for notifying any other Data Controller about the incident where it is appropriate to do so i.e. where the breach involves unauthorised access to personal data they are responsible for.

Rotherham will maintain a record of all detected or reported breaches and provide the YHCR Project Board with a quarterly report in order to monitor systemic problems, identify risks and

instigate remedial actions. See also Schedule 4. Rotherham will provide this function whilst the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.

Identity Management

IAM maintains an identity model to enable local identities to be consolidated into a regional identity and so enabling a full audit of all YHCR usage to be assembled for individuals regardless of how they access the YHCR. A consolidated regional identity also allows role-based access rights to be controlled for regionally held data. IAM manages the following identity model:



The model depicts the relationships between key data entities and the packaging of entities within a resource model.

When a data consumer invokes the service, IAM attempts to link the local identity of the user with a regional identity. IAM uses local identifiers (ERS number, NHS number NI number etc.) to match local identities.

IAM maintains identity demographics (organisation, first name and given name) and these are populated from the last demographic presented by a consumer. Local roles are an amalgamation of roles presented by the data consumer over different authorisation requests.

User Responsibilities

Everyone granted authorised access to the YHCR 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 YHCR 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 RAISE AN OBJECTION TO THE YORKSHIRE AND HUMBER CARE RECORD (YHCR)

The YHCR 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 Yorkshire and Humber region area.

The system allows Care Professionals within the Yorkshire and Humber region Health and Social Care community to view, 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 Yorkshire and Humber region 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)[1]

Leeds Teaching Hospitals NHS Trust (LTHTrust) will act as the lead organisation for managing all objection requests from an individual for the YHCR.

An individual can raise an objection of having a YHCR created.

Right to raise an objection:

- The service user will contact the Information Governance Team/Lead at LTHTrust to confirm that they would like the right to raise an objection of sharing their personal information or sensitive personal information relating to them via the YHCR system.
- The service user will be requested to verify their demographic details and date of birth, providing the service user with an application form to complete.
- The LTHTrust's Information Governance Team records the patient's NHS Number, Name, Address, and Date of Birth via an application form.
- The LTHTrust's Information Governance Team will provide a response letter to the service user notifying them that a decision will be made within one month from the day reported and they will be notified of the decision via their partner organisation.

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

- The LTHTrust's Information Governance Team will send the request for raising an objection to the service users for the attention of the Data Protection Officer and Caldicott Guardian at the partner organisation.
- The partner organisation's Data Protection Officer and Caldicott Guardian will review the service users request to raise an objection and assess if the objection is valid. .
- The partner organisation will notify the LTHTrust's Information Governance team of their decision and inform the service user of the decision by letter.
- The partner organisation's and LTHTrust's Information Governance Team will keep a record of the outcome.
- If upheld, the service user's details will then be forwarded to Rotherham's system administration team to disable the sharing for the service user record from the YHCR system. Currently the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.
- Rotherham's system administration will send confirmation when this has been completed to the partner organisation's and LTHTrust's Information Governance Team. Currently the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.
- Following this, the partner organisation and/or LTHTrust's Information Governance Team will send a letter to the service users to confirm this has been completed.

A patient's decision to object to the processing of their data by the YHCR, does not prevent information sharing that would normally take place to support patient care nor does it prevent the sharing of specific information in the public interest e.g. serious risk of harm / abuse. This should be explained to the patient.

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

Opt back in Process:

- The service user will contact the LTHTrust's Information Governance Team 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 YHCR system.
- The service user will be requested to verify their demographics details and date of birth.
- The LTHTrust's 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 YHCR system.

- The LTHTrust's Information Governance Team will keep a record that the patient has opted back in.
- LTHTrust's information Governance Team will contact the partner organization's Information Governance Team to notify them of the service users request.
- The service user's details will then be forwarded to Rotherham's system administration team to reactivate the sharing of the service user's record on the YHCR system. Currently the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.
- The service user will be sent a confirmation letter from the partner organisation informing them that their information will now be shared via the YHCR system.

SCHEDULE 4

INFORMATION GOVERNANCE BREACHES

This procedure describes the stages when a user of The YHCR accesses service user information within the YHCR to which they are not entitled.

Break Glass Function

The YHCR has a 'Break Glass' function will allow authorised users of the YHCR 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 YHCR will flag services user records where the break glass function has been invoked.
- If there is not a valid reason the system administration Team at Rotherham will contact the IG Organisational lead at the partner organisation for the YHCR user to inform them of the potential inappropriate access. Currently the site hosting of YHCR is sub-processed by Rotherham. When YHCR is hosted in the Cloud the nominated sub-processor will fulfil this obligation.

Complaint by a service user/YHCR user regarding YHCR access

A service user or YHCR user may have concerns in with regards to YHCR users accessing records where the YHCR 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/YHCR user regarding YHCR access:

- The IG Team for the YHCR user shall contact the LTHTrust IG Team to request an audit and any supporting documentation

- The LTHTrust IG will provide the requested documentation.

SCHEDULE 5

RBAC Roles

1.0 Background

Patients, care users and citizens must have confidence that data sharing is secure, and that confidential patient information is shared appropriately and only with individuals that have a legitimate relationship with the patient. Data sharing should meet the reasonable expectations of the patient

Partner organisations will manage the YHCR authentication and access control function.

RBAC Roles

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

The YHCR 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 YHCR can be assigned one or many roles. Access categories from each organisation will be approved by the YHCR Project Board.

An example of RBAC model is shown below.

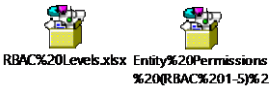
This model contains more RBAC clinical roles (RBAC 4.5, RBAC 5.0) with examples of job titles and whilst these roles are suited to an Acute setting, many of the roles or similar roles can be found in other settings. It will also show functionality of the roles beyond READ, READLIST.

It is **not** expected to replace existing RBAC arrangements to support local sharing within a YHCR. However, if there is no access control model in place, partner organisations can adopt this model.

RBAC role	Staff types (examples)	Read List [Summary information only]	Read [access to full record]
1	Receptionist	Demographic data only	
2	Role can be adapted for non-clinical use but is required for basic Admin	Yes	No
3	Senior Administrator	Yes	No
4+	Registered and Regulated Health Care Professional	Yes	Yes

There is the need to have a role that would work for social care. It is noted that the social worker is a regulated and registered professional.

Please see below links to spread sheets which show job titles that have been mapped to RBAC roles.



2.0 The Controls

Partner organisations will implement the following controls to ensure that access to patient care records is appropriately protected:

- **Authentication:** Partner organisations will need to ensure with their participating bodies the use of appropriate processes and mechanisms for identity verification of staff, assignment to roles and groups, and strong authentication. Initially, a Partner organisations access control policy may need to recognise password-based authentication with future support for strong authentication.
- **Authorisation:** Partner organisations will need to determine the degree of access to data that will be allowed by a member of staff within a participating body. Partner organisations will need to continue to keep local access controls and privileges current and up to date.
- **Audit:** Partner organisations will need to be able to audit and investigate access to a patient's care record.
- **Non-repudiation:** Robust systems in place for authorisation and authentication, and audit trails generated each time a care record is accessed, individuals will not be able to repudiate accessing care records.
- **Legitimate relationships:** Whilst healthcare professionals can access all records this does not mean that they should. "Legitimate Relationship" confirms that the viewer has a justifiable reason to view the patient record as they are involved in their care. Legitimate relationship as defined in Caldicott Information Governance Review 2013[2] is *"The legal relationship that exists between an individual and the health and social care professionals and staffing providing or support their care".* This term is well adopted and understood assuring confidentiality within health and care organisation.

  Legitimate relationships are created by patient or care events and it is only whilst the legitimate relationship exists that the care record should be accessed by the healthcare professional.

  Legitimate relationship is managed locally, and healthcare professionals will access the LCHR via the patient record. This creates an audit trail of the access.
- **Conformance with IG Framework and Data Security and Protection Toolkit:** All LHCRS will achieve the minimum mandatory requirements for the DSPT which will be audited. LHCRs will also have assured information governance activities against the IG Framework
- **Professional standards and ethics**: all registered and regulated health and care professionals are bound by a code of ethics which set out acceptable behaviours. In the LHCRs all healthcare professional staff that have full access to the patient care record will be a registered and regulated professional. They will be subject to investigation by

[2] The Information Governance Review: To Share or Not to Share

the professional body with a risk of being sanctioned, if they are reported for professional misconduct.

- **Staff training on confidentiality:** All staff in the LHCR will receive confidentiality training. This training will be refreshed at regular agreed intervals. This is important to raise awareness and ensure that staff understand how to handle confidential patient information appropriately, to reduce the risk of breaching patient records by inappropriate access or handling.
- **Patient / Carer authentication:** patients and carers will be required to authenticate themselves prior to accessing patient care record. Authentication is vital to protect the individual's privacy.
- **Sanctions:** If a patient record is inappropriately accessed, the staff member will be sanctioned.

SCHEDULE 6

Clinical Safety Care Report

Clinical Safety
Closure Report YHCR

SCHEDULE 7

Management of Accounts

All access accounts for the YHCR will be managed by the Partner Organisations.

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 [Insert Organisation Name].

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	The creating a joint electronic care record for service users (patients and social care clients) within the Yorkshire and Humber region area.
Duration of the processing	Duration of agreement.
Nature and purposes of the processing	The YHCR 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 Humber Teaching NHS Foundation Trust will host and be the Data Processors on behalf of the Yorkshire and Humber region area. The server(s) used for the development of the YHCR will be stored by Humber Teaching NHS Foundation Trust who are a sub-data Processor of The Rotherham NHS Foundation Trust. Humber Teaching NHS Foundation Trust is also the Data Controller Humber Teaching NHS Foundation Trust patients' personal data. The Legal basis for processing this data is cover by GDPR Article 6.1(e) and Article 9.2(h).
Type of Personal Data	Name, address, demographics and health & social care records except where information is restricted by law
Categories of Data Subject	Citizens included in the geographic footprint of the Yorkshire & Humber region as outlined in the Yorkshire & Humber

	Care Record literature.
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	N/A