

# THE ROTHERHAM HEALTH RECORD

## PRIVACY IMPACT ASSESSMENT

On behalf of the Rotherham Integrated Care Partnership



## **Privacy Impact Assessment (PIA) Screening Questions**

The below screening questions should be used to inform whether a PIA is necessary. This is not an exhaustive list therefore in the event of uncertainty completion of a PIA is recommended.

|                          |  |
|--------------------------|--|
| <b>Project title</b>     | <b>Rotherham Health Record</b>   |
| <b>Brief description</b> | A view only portal accessed via a web browser that presents clinical information from a number of sources aggregated in various ways to provide relevant medical and demographic patient data to appropriate bodies who have a relevant and appropriate clinical need to view this data. |

*Screening completed by*

|                    |                                      |
|--------------------|--------------------------------------|
| <b>Name</b>        |                                      |
| <b>Title</b>       | Health Informatics Programme Manager |
| <b>Department</b>  | Health Informatics                   |
| <b>Telephone</b>   |                                      |
| <b>Email</b>       |                                      |
| <b>Review date</b> | 14.02.17                             |

Marking any of these questions is an indication that a PIA is required:

| <b>Screening Questions</b> |  | <b>Tick</b>                         |
|----------------------------|--|-------------------------------------|
| 1                          | Will the project involve the collection of identifiable or potentially identifiable information about individuals?   | <input checked="" type="checkbox"/> |
| 2                          | Will the project compel individuals to provide information about themselves?<br>i.e. where they will have little awareness or choice.  | <input type="checkbox"/>            |
| 3                          | Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?  | <input checked="" type="checkbox"/> |
| 4                          | Are you using information about individuals for a purpose it is not currently used for or in a new way?<br>i.e. using data collected to provide care for an evaluation of service development.   | <input type="checkbox"/>            |
| 5                          | Where information about individuals is being used, would this be likely to raise privacy concerns or expectations?<br>i.e. will it include health records, criminal records or other information that people would consider to be sensitive and private. | <input checked="" type="checkbox"/> |
| 6                          | Will the project require you to contact individuals in ways which they may find intrusive?<br>i.e. telephoning or emailing them without their prior consent.   | <input type="checkbox"/>            |
| 7                          | Will the project result in you making decisions in ways which can have a significant impact on individuals?<br>i.e. will it affect the care a person receives.   | <input type="checkbox"/>            |
| 8                          | Does the project involve you using new technology which might be perceived as being privacy intrusive?<br>i.e. using biometrics, facial recognition or automated decision making.  | <input type="checkbox"/>            |

***Please retain a copy of this questionnaire within your project documentation.***

***Please note that once completed the following sections (1 to 3) should be detached from the remaining document prior to being included in the RFT's Publication Scheme.***

## Privacy Impact Assessment (PIA)

### Section 1: System/Project General Details

Review Date: April 2019

|  |  |                                   |
|--|--|-----------------------------------|
| <b>Project title:</b>  | <b>Rotherham Health Record</b>   |                                   |
| <b>Objective:</b>  | To provide a web based, view only, secure portal accessible across relevant health care provider organisations across the Rotherham area containing patient information aggregated from multiple systems.  |                                   |
| <b>Background:</b><br>Why is the new system/change in system required? Is there an approved business case?   | The Rotherham Health Record is a programme of work that aims to provide all health and social care workers across Rotherham with relevant information about their patients/clients in an integrated electronic format or available from a single application. This information may be obtained directly from a back end system or may be provided using an integrated information set from a number of applications. The Health Record programme is being managed by the Rotherham Integrated Care Partnership (ICP) Digital Group (formerly the Rotherham Health and Care Interoperability Group) which sets out its goals and priorities and consists of representatives from the organisations listed below. Historically there have been two distinct data portals managed by TRFT. One was inwardly facing and used by TRFT staff (SEPIA) and one was externally facing and used by GP Practices (HIPPO). Work on these portals was undertaken independently of each other and the IT Infrastructure they operated from was also distinct and separate. When the Rotherham ICP Digital Group (formerly the Interoperability Group) was formed it was agreed that all such services should be provided from the same portal which will be the Rotherham Health Record. |                                   |
| <b>Relationships:</b><br>For example, with other Trust's, organisations.   | The Rotherham NHS Foundation Trust; NHS Rotherham CCG; Rotherham Doncaster and South Humber NHS Foundation Trust (RDaSH); Rotherham Hospice; Rotherham Metropolitan Borough Council, Connect Healthcare Rotherham CIC (GP Federation)  |                                   |
| <b>Other related projects:</b>   | N/A  |                                   |
| <b>Project Manager:</b>  | Name:  |                                   |
|  | Title:   | Project Manager                   |
|  | Department:  | Health Informatics                |
|  | Telephone:   |                                   |
|  | Email  |                                   |
| <b>Information Asset Owner:</b><br>All information systems/assets must have an Information Asset Owner (IAO). IAO's should normally be a Head of Department/Service.                           | Name:  |                                   |
|  | Title:   | Head of EPR                       |
|  | Department:  | Health Informatics                |
|  | Telephone:   |                                   |
|  | Email  |                                   |
| <b>Information Asset Administrator:</b><br>Information systems/assets may have an Information Asset Administrator (IAA) who reports the IAO. IAA's are normally System Managers/Project Leads. | Name:  |                                   |
|  | Title:   | Interfacing and Systems Developer |
|  | Department:  | Health Informatics                |
|  | Telephone:   |                                   |
|  | Email  |                                   |

|  |   |
|--|---|
| <b>Customers and other stakeholders:</b> | Health and Social Care providers within the Rotherham area; Citizens within the Rotherham area. |
|--|---|

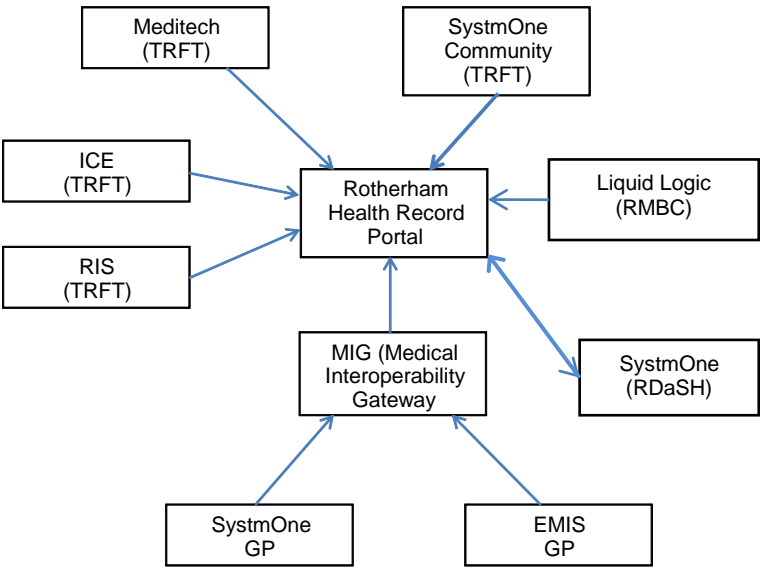
## Section 2: Privacy Impact Assessment Key Questions

|                   | Question  | Response  |
|-------------------|---|---|
| <b>Data Items</b> |   |   |
| 1.                | <b>Will the system/project/process (referred to thereafter as 'project') contain identifiable or Personal Confidential Data (PCD)?</b><br>If answered 'No' then a PIA is not required.  | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br><br>If yes, who will this data relate to:<br><input checked="" type="checkbox"/> Patient<br><input type="checkbox"/> Staff<br><input type="checkbox"/> Other: <a href="#">Click here to enter text.</a>  |
| 2.                | <b>Please state purpose for the collection of the data:</b><br>For example, patient care, commissioning, research, audit, evaluation.   | To provide all health and social care workers across Rotherham with relevant information about their patients/clients in an integrated electronic format or available from a single application.  |
| 3.                | <b>Please tick the data items that are held in the system</b><br><br><div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <b>Personal</b> </div> <div style="font-size: 3em; margin-right: 10px;">}</div> </div> <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <b>Sensitive</b> </div> <div style="font-size: 3em; margin-right: 10px;">}</div> </div> | <div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"> <input checked="" type="checkbox"/> Name<br/> <input checked="" type="checkbox"/> Post Code<br/> <input checked="" type="checkbox"/> GP Practice<br/> <input checked="" type="checkbox"/> NHS Number         </div> <div style="width: 50%;"> <input checked="" type="checkbox"/> Address<br/> <input checked="" type="checkbox"/> Date of Birth<br/> <input checked="" type="checkbox"/> Date of Death<br/> <input type="checkbox"/> NI Number         </div> </div> <div style="display: flex; flex-wrap: wrap; margin-top: 10px;"> <div style="width: 50%;"> <input checked="" type="checkbox"/> Medical History<br/> <input type="checkbox"/> Political opinions<br/> <input checked="" type="checkbox"/> Ethnic Origin<br/> <input type="checkbox"/> Criminal offences         </div> <div style="width: 50%;"> <input type="checkbox"/> Trade Union membership<br/> <input checked="" type="checkbox"/> Religion<br/> <input checked="" type="checkbox"/> Sexuality         </div> </div> <input type="checkbox"/> Other: |
| 4.                | <b>What consultation/checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this project?</b>   | This project is being undertaken at the request of the Rotherham ICP Digital Group (formerly the Rotherham Health & Care Interoperability Group). Access to the RHR shall be granted using the principle of 'Least Privilege', meaning that every user of the RHR should operate using the least set of privileges necessary to complete the job. All changes to the RBAC model must be authorised by the <del>Interoperability</del> Rotherham ICP Digital Group.  |
| 5.                | <b>How will the information be kept up to date and checked for accuracy and completeness?</b>   | The RHR portal receives data only from existing systems and does not retain any clinical patient information locally within the portal. Existing system processes managed by the respective services maintain data accuracy and completeness. System testing against the RHR portal prior to product release confirms the expected data is being received and displayed.  |

|                        | Question  | Response  |
|------------------------|---|---|
| <b>Data processing</b> |   |   |
| 6.                     | <b>Will a third party be processing data?</b>   | <input checked="" type="checkbox"/> Yes (TRFT as host) <input type="checkbox"/> No<br>If no, please go to the Confidentiality section.  |
| 7.                     | <b>Is the third party contract/supplier of the project registered with the Information Commissioner?</b>  | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br><br>Organisation: The Rotherham NHS Foundation Trust<br>Data Protection Registration Number: ZA067076  |
| 8.                     | <b>Has the third party supplier completed a Data Security and Protection Toolkit Return?</b>  | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, please give organisation code:<br>RFR<br><i>DSP Toolkit Score:</i><br><input checked="" type="checkbox"/> Standards Met <input type="checkbox"/> Standards Not Met<br>If 'Standards Not Met', please request a copy of the improvement plan and provide it with this assessment.   |
| 9.                     | <b>Does the third party/supplier contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?</b>                         | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>Data Processing Deed in place  |
| 10.                    | <b>Will other third parties (not already identified) have access to the project?</b><br>Include any external organisations.   | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>If so, for what purpose?<br><a href="#">Click here to enter text.</a><br>Please list organisations and by what means of transfer:<br><a href="#">Click here to enter text.</a>   |
| <b>Confidentiality</b> |   |   |
| 11.                    | <b>Please outline what privacy/fair processing notices and leaflets will be provided.</b><br>A copy of the privacy/fair processing notice and leaflets must be provided.                | The use of the RHR will be reflected in the privacy notices of all partner organisations – in addition to this, an extensive communications programme will be developed to inform members of the public in Rotherham about the RHR and how they can opt out – will be in a variety of forms including on the CCG's website (and links in other organisations), leaflets, posters, banner stands, letters to new patients, media briefings/releases, engagement with voluntary/community groups, factsheets and videos/vlogs/animations. |
| 12.                    | <b>Does the project involve the collection of data that may be unclear or intrusive?</b><br>Are all data items clearly defined? Is there a wide range of sensitive data being included? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No   |

|     | Question   | Response  |
|-----|--|---|
| 13. | What legal basis is being relied upon for the processing of personal identifiable or sensitive data? | <p><b>GDPR Article 6:</b> <i>Necessary for the performance of a task carried out in the exercise of official authority vested in the controller</i></p> <p>For the purposes of the Rotherham Health Record this is in the form of the NHS Act 2006, Health and Social Care Act 2012, Health and Social Care Act (Safety and Quality) 2015 and the Human Rights Act.</p> <p><b>GDPR Article 9:</b> <i>Necessary for the provision of health or social care or the treatment or the management of health or social care systems and services (where processed by or under responsibility of a professional subject to a duty of confidentiality)</i></p> <p><b>Data Protection Act Schedule 1 Part 1 Condition for Processing:</b></p> <p>Processing in connection with employment, health and research - health or social care</p> <p><b>Common Law Duty of Confidentiality (to satisfy fair and lawful processing under Data Protection Act/GDPR):</b> The sharing of personal confidential data into the Rotherham Health Record and the viewing of information within the Rotherham Health Record are for the purposes of Direct Care <b>only</b>. Accordingly, the patient's consent to such sharing may be implied. As set out above, fair processing notices are required and the nature of the sharing will be communicated to patients by a variety of means, and all patients will have the opportunity to opt-out.</p> |
| 14. | How will consent, non-consent, objections or opt-outs be recorded and respected?                     | <p>As per the Common Law Duty of Confidentiality, opt out is permissible due to the provision of direct care and the use of implied consent. Individuals will contact TRFT requesting opt out and will complete either an eForm or paper form. Staff at TRFT (possibly Access to Records team – to be determined) will administer this process. Identity of those requesting opt out will be verified and opt-out will be recorded on the RHR. Organisational visibility controls will be deselected on the RHR in accordance with the Individual's wishes. An opt-out database table will hold any patient identifiers where an opt-out request has been received. Opt outs are recorded in RHR database. The opt-outs are data set specific and therefore opt out can be recorded to exclude the data from one or multiple source systems.</p>  |

|                     | Question   | Response   |
|---------------------|--|--|
| 15.                 | Will the consent cover all processing and sharing/disclosures?   | <input type="checkbox"/> Yes <input type="checkbox"/> No<br>If not, please detail: <b>Not applicable – consent not sought</b>  |
| 16.                 | What process is in place for rectifying/blocking data?<br>What would happen if such a request were made? | Data would be rectified in the local source system. If required data would be blocked using the opt-out table as above. This would block data from all sources used.   |
| <b>Engagement</b>   |  |  |
| 17.                 | Has stakeholder engagement taken place?  | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>If yes, how have any issues identified by stakeholders been considered?<br><a href="#">Click here to enter text.</a><br>If no, please outline any plans in the near future to seek stakeholder feedback:  |
| <b>Data Sharing</b> |  |  |
| 18.                 | Does the project involve any new information sharing between organisations?                              | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, please describe:<br>Due to COVID19, there has been a need to provide interim measurements in the form of temporary care providers (3 Care Homes, Layden Court, Clifton Meadows and Ackroyd House) as Intermediate Care Providers. These 3 Care Providers have been allocated to 3 GP Practices namely (Blyth Road, Stag and St. Ann's) and coded using the GP Practice Code.<br><br>Service Users moved to these locations may not be a registered patient of the GP Practice and therefore, discharge information would not be viewable. In order to overcome this, whilst still relying on access being for 'Direct or Ongoing Clinical Care Only', it is necessary to extend the access to TRFT patient data accessed through the RHR, to all GP Practices in the Rotherham area and not just the GP Practice where the patient is registered.<br><br>This access will be removed once the need for these temporary interim discharge areas are no longer required.<br><br>This decision will be based on the COVID19 restrictions being removed and the requirement for temporary care providers no longer being a requirement. |
| <b>Data Linkage</b> |  |  |

|                             | Question  | Response   |
|-----------------------------|---|--|
| 19.                         | <p><b>Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?</b></p> <p>The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously)</p> | <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, please provide a data flow diagram.</p>  <pre> graph TD     Meditech["Meditech (TRFT)"] --&gt; RHP["Rotherham Health Record Portal"]     SystmOneComm["SystmOne Community (TRFT)"] --&gt; RHP     ICE["ICE (TRFT)"] --&gt; RHP     RIS["RIS (TRFT)"] --&gt; RHP     LiquidLogic["Liquid Logic (RMBC)"] --&gt; RHP     RHP --&gt; SystmOneRDASH["SystmOne (RDASH)"]     RHP &lt;--&gt; MIG["MIG (Medical Interoperability Gateway)"]     MIG &lt;--&gt; SystmOneGP["SystmOne GP"]     MIG &lt;--&gt; EMISGP["EMIS GP"] </pre>   |
| <b>Information Security</b> |   |  |
| 20.                         | <p><b>Who will have access to the information within the system?</b></p> <p>Please refer to roles/job titles.</p>   | <p>Clinicians and Health workers across the organisations listed above can have access to the system if appropriate for their role in providing patient care. RBAC matrix in place. Access to the RHR shall be granted using the principle of ‘Least Privilege’, meaning that every user of the RHR should operate using the least set of privileges necessary to complete the job</p>   |
| 21.                         | <p><b>Is there a useable audit trail in place for the project?</b></p> <p>For example, to identify who has accessed a record?</p>   | <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Not applicable</p> <p>If yes, please outline the audit plan: Each access to a record is registered to the identifiable portal account viewing the information. Audits can be run either by username (every click recorded including which record user has accessed) or by patient record (who has accessed that individual’s record). In addition access where user accounts cannot be controlled by a restricted patient/client list (such as those of the Hospice or Social Services) will have a search that email’s a privacy officer to verify the relevance of the search. However a dashboard of Social Services referrals/ current list of inpatients at the Hospice will be displayed on the first page of those respective organisations.</p> |

|  | Question   | Response  |
|--|--|---|
| 22.  | <b>Describe where will the information be kept/stored/accessed?</b>  | All information used for User Accounts (access list for users), Opt Outs and Audits is stored [REDACTED] at The Rotherham NHS Foundation Trust premises. Access to the information [REDACTED]. No copies of records from the source systems are stored in the RHR (view only).  |
| 23.  | <b>Please indicate all methods in which information will be transferred</b>  | <input type="checkbox"/> Fax <input type="checkbox"/> Email (Unsecure/Personal) <input type="checkbox"/> Email (Secure/nhs.net) <input type="checkbox"/> Internet (unsecure – e.g. http) <input type="checkbox"/> Telephone <input checked="" type="checkbox"/> Internet (secure – e.g. https) <input type="checkbox"/> By hand <input type="checkbox"/> Courier <input type="checkbox"/> Post – track/traceable <input type="checkbox"/> Post – normal <input type="checkbox"/> Other: |
| 24.  | <b>Does the project involve privacy enhancing technologies?</b><br>Encryption; 2 factor authentication, new forms of pseudonymisation.   | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, please give details: A secure certificate registered to TRFT is used for access to the portal via HTTPS.   |
| 25.  | <b>Is there a documented System Level Security Policy (SLSP) or process for this project?</b><br>A SLSP is required for new systems.   | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, please provide a copy.<br>Redacted   |
| <b>Privacy and Electronic Communications Regulations</b> |  |   |
| 26.  | <b>Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?</b><br>Please note that seeking to influence an individual is considered to be marketing. | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>If yes, what communications will be sent?<br>Click here to enter text.<br>Will consent be sought prior to this?<br><input type="checkbox"/> Yes <input type="checkbox"/> No  |
| <b>Records Management</b>                                |  |   |

|   | Question  | Response   |
|---|---|--|
| 27.                                       | What are the retention periods for this data?   | The RHR Portal does not hold any patient data locally. All data used is contained within existing systems. Data relating to audit trails will be retained as per the requirements of the Records Management Code of Practice for Health and Social Care 2016 (for the life of the system plus the relevant retention period for the last record accessed). |
| 28.                                       | How will the data be destroyed when it is no longer required?   | Database maintenance plans for internal data. Hosted system data as per contractual arrangements with the provider.  |
| <b>Information Assets and Data Flows</b>  |   |  |
| 29.                                       | Has an Information Asset Owner been identified and does the Information Asset Register require updating?                                    | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No  |
| 30.                                       | Have the data flows been captured?  | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>Data does not flow from the RHR. It is a view only system with restricted RBAC (Role Based Access Control) in place.  |
| <b>Business Continuity</b>                |   |  |
| 31.                                       | Have the requirements for business continuity been considered?  | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, please detail: System is on resilient infrastructure and provides for view only access to data available on other systems. If RHR becomes unavailable then existing processes for obtaining this information can be used.   |
| <b>Open Data</b>                          |   |  |
| 32.                                       | Will (potentially) identifiable and/or sensitive information from the project be released as Open Data (be placed in to the public domain)? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>If yes, please describe: <a href="#">Click here to enter text.</a>  |
| <b>Data Processing Outside of the EEA</b> |   |  |
| 33.                                       | Are you transferring any personal and/or sensitive data to a country outside the European Economic Area (EEA)?                              | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>If yes, which data and to which country?<br><a href="#">Click here to enter text.</a>   |

|     | Question   | Response   |
|-----|--|--|
| 34. | Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country? | <input checked="" type="checkbox"/> Not applicable<br><input type="checkbox"/> Yes <input type="checkbox"/> No<br>If yes, who completed the assessment?<br><a href="#">Click here to enter text.</a> |

### **Section 3: Review and Approval**

#### **Assessment completed by**

|                                       |                                      |
|---------------------------------------|--------------------------------------|
| <b>Name:</b>                          |                                      |
| <b>Title:</b>                         | Health Informatics Programme Manager |
| <b>Sent electronically or Signed:</b> | <input checked="" type="checkbox"/>  |
| <b>Date:</b>                          | 14 February 2017                     |

#### **Assessment reviewed (IG) by**

|                                       |  |
|---------------------------------------|--|
| <b>Name:</b>                          |  |
| <b>Sent electronically or Signed:</b> | Amendment of Section 18 to accommodate temporary requirement due to COVID19. |
| <b>Date:</b>                          | 21/04/2020   |

#### **Information Governance Approval from the Rotherham Interoperability Group**

|                                      |   |
|--------------------------------------|---|
| <b>Name:</b>                         | <a href="#">Click here to enter text.</a> |
| <b>Title:</b>                        | <a href="#">Click here to enter text.</a> |
| <b>Electronic Approval or Signed</b> | N/A                                       |
| <b>Date:</b>                         | <a href="#">Click here to enter text.</a> |

#### **Information Governance Approval from the Integrated Care System Board**

|                                      |   |
|--------------------------------------|---|
| <b>Name:</b>                         | <a href="#">Click here to enter text.</a> |
| <b>Title:</b>                        | <a href="#">Click here to enter text.</a> |
| <b>Electronic Approval or Signed</b> | N/A                                       |
| <b>Date:</b>                         | <a href="#">Click here to enter text.</a> |

#### **Approval from the SIRO/Caldicott Guardian for The Rotherham NHS Foundation Trust**

|                                      |   |
|--------------------------------------|---|
| <b>Name:</b>                         |   |
| <b>Title:</b>                        | Executive Medical Director / Caldicott Guardian |
| <b>Electronic Approval or Signed</b> |   |
| <b>Date:</b>                         | 21/04/2020                                      |

**Approval from the SIRO/Caldicott Guardian for Rotherham CCG**

|                                      |                           |
|--------------------------------------|---------------------------|
| <b>Name:</b>                         | Click here to enter text. |
| <b>Title:</b>                        | Click here to enter text. |
| <b>Electronic Approval or Signed</b> |                           |
| <b>Date:</b>                         | Click here to enter text. |

**Approval from the SIRO/Caldicott Guardian for Rotherham Doncaster and South Humber NHS Foundation Trust**

|                                      |                           |
|--------------------------------------|---------------------------|
| <b>Name:</b>                         | Click here to enter text. |
| <b>Title:</b>                        | Click here to enter text. |
| <b>Electronic Approval or Signed</b> |                           |
| <b>Date:</b>                         | Click here to enter text. |

**Approval from the SIRO/Caldicott Guardian for Rotherham Metropolitan Borough Council**

|                                      |                           |
|--------------------------------------|---------------------------|
| <b>Name:</b>                         | Click here to enter text. |
| <b>Title:</b>                        | Click here to enter text. |
| <b>Electronic Approval or Signed</b> |                           |
| <b>Date:</b>                         | Click here to enter text. |

**Approval from the SIRO/Caldicott Guardian for Rotherham Hospice**

|                                      |   |
|--------------------------------------|---|
| <b>Name:</b>                         | Click here to enter text.   |
| <b>Title:</b>                        | Click here to enter text.   |
| <b>Electronic Approval or Signed</b> | <input type="checkbox"/> The Information Governance Approval is attached. |
| <b>Date:</b>                         | Click here to enter text.   |

**Date reviewed: April 2020**

Appendix A

*The Rotherham Health Record*

***Key privacy risks and the associated compliance and corporate risks***

|                  | Privacy issue  | Risk to individuals  | Compliance risk   | Associated organisation / corporate risk  |
|------------------|--|--|---|---|
| <b><u>A.</u></b> | <p><b><u>SHARING DATA:</u></b></p> <p>Inadequate sharing / disclosure controls increase the likelihood of information being shared inappropriately.</p> <p>Ambiguities within the Information Governance legislation means data could be shared inappropriately or insufficient data be shared to provide improved care for individuals.</p> <p>(Relates to questions 4 and 20 of the PIA)</p> | Individuals' data is shared beyond the organisations they expect to receive their data | <p>Reliance on all organisations to comply with data sharing agreements.</p> <p>Breach of Article 5 Principles 1 (a), (b) and (c) of the General Data Protection Regulation (GDPR).</p> <p>Regulatory action.</p> | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Regulator action if data is shared inappropriately or with wrong organisations.</p> <p>Civil action can be taken based on distress caused.</p> <p>Financial costs and reputational damage.</p> |

|                  | Privacy issue  | Risk to individuals  | Compliance risk   | Associated organisation / corporate risk   |
|------------------|--|--|---|--|
| <b><u>B.</u></b> | <p><b><u>DATA QUALITY:</u></b></p> <p>Multiple and varied systems used within participating organisations impacts on the effectiveness of the programme and means data quality is impacted in the sharing process</p> <p>Poor data quality will diminish the benefits of any reporting. Improving data quality has been an on-going challenge within the Health &amp; Social Care sectors.</p> <p>Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to health and care services.</p> <p>(Linking to Question 5 of the PIA)</p> | <p>Data shared about individuals is incomplete or inaccurate, or out of date, or there are multiple versions, therefore individuals may not receive the improvement in care that the programme intends.</p> <p>Inappropriate care could be provided.</p> | <p>Reliance on all organisations to comply with data sharing agreements.</p> <p>Breach of Article 5 1(d) of the GDPR.</p> <p>Regulatory action.</p>     | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Civil action can be taken based on harm caused.</p> <p>Financial costs and reputational damage.</p> |
| <b><u>C.</u></b> | <p><b><u>CONSENT MODEL:</u></b></p> <p>Our communication campaign to support implied consent may not reach all of the Rotherham population.</p> <p>Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.</p> <p>(Links in to questions 11 and 14 of the PIA)</p>   | <p>Data is used in ways unacceptable or unexpected by the individual it is about.</p>  | <p>Potential breach of Articles 5 1 (a) and 12-14 of the GDPR if potential uses of data is not communicated effectively, and to appropriate groups.</p> | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p>  |
| <b><u>D.</u></b> | <p><b><u>DATA SECURITY:</u></b></p> <p>Regulatory action if sufficient security measures are not applied to the processing of the data.</p> <p>(Links to questions 4, 20, 22, 23, 24, 31 and 33 of the PIA)</p>  | <p>Large numbers of individuals may choose to opt out.</p>   | <p>Breach of Article 5 1 (f) of the GDPR.</p> <p>Regulatory action.</p>   | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Financial costs and reputational damage.</p>  |

|                  | Privacy issue   | Risk to individuals   | Compliance risk  | Associated organisation / corporate risk  |
|------------------|---|---|--|---|
| <b><u>E.</u></b> | <p><b><u>DATA RETENTION:</u></b></p> <p>If a retention period is not established information might be retained for longer than necessary.</p> <p>(Question 27 of the PIA for retention periods)</p> <p>The RHR will hold details of audit trails (see question 21 of the PIA)</p>   | Data becomes out of date and inaccurate.  | Breach of Article 5 1 (a) and 5 1 (c) of the GDPR  | Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.  |
| <b><u>F.</u></b> | <p><b><u>USE OF DATA:</u></b></p> <p>The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.</p> <p>(Link to question 13 of the PIA)</p>  | Data is used in ways unacceptable or unexpected by the individual it is about, or in ways to which they have not consented. | <p>Breach of Article 5 1 (a), 5 1 (b) and 5 1 (c) GDPR and Human Rights Act Article 8.</p> <p>Regulatory action.</p> | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Public distrust about how information is used can damage an organisation's reputation and lead to reduced participation.</p> |
| <b><u>G.</u></b> | <p><b><u>LEGISLATIVE COMPLIANCE:</u></b></p> <p>Non-compliance with legislation: Data Protection Act, General Data Protection Regulation, Privacy and Electronic Communications Regulations (PECR), sector specific legislation or standards, human rights legislation.</p> <p>(Link to questions 13 and 26 within the PIA)</p> | Individual privacy is compromised.  | <p>Breach of Principles of the GDPR and Human Rights Act.</p> <p>Regulatory action.</p>                              | <p>Non-compliance with the Data Protection Act, General Data Protection Regulation or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Financial costs and reputational damage.</p>   |

Appendix B  
*The Rotherham Health Record*  
**Privacy risks and solutions**

|             | <b>Risk</b>   | <b>Solution(s)</b>  | <b>Result</b><br>(Is the risk eliminated, reduced, or accepted?) | <b>Evaluation</b><br>(Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)                          |
|-------------|---|---|--|---|
| A, C, F, G. | Data is used in ways unacceptable or unexpected by the individual it is about, or in ways to which they have not consented. | Work with Rotherham ICP Digital Group (formerly Interoperability Group) and IG advisors to ensure members of the public whose information is to be shared through the Rotherham Health Record are informed about all of the potential uses of their data and given adequate opportunity to opt out. Ensure the project has the best understanding of the data sharing restrictions and legislations to avoid the inappropriate sharing of data. A process will be required for additional organisations to be considered for joining, including Integrated Care Partnerships. | Reduced  | Solutions are in line with the aims of the project and will not impact on the technical implementation of the project. Impact on individuals will be minimised.                                   |
| B, G.       | Data shared about individuals is incomplete, inaccurate or insufficient.  | The master patient index within the Rotherham Health Record will match and combine individual patient data where appropriate to provide the maximum available information. Where source data quality is lacking the Rotherham Health Record cannot make any changes, although it is hoped that use of the Master Patient Index will enable problems to be identified. Matching within RHR is based upon an exact match of NHS number. Responsibility for data quality, NHS number completeness and validation, remains with the Data Controller.                              | Accepted   | The solutions are in line with the aims of the programme to provide accurate and useful data although there is an acceptance that a large part of this lies with the participating organisations. |

|             | <b>Risk</b>  | <b>Solution(s)</b>  | <b>Result</b><br>(Is the risk eliminated, reduced, or accepted?) | <b>Evaluation</b><br>(Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)   |
|-------------|--|---|--|--|
| A, C, F, G. | Sharing of data and access to it beyond the boundaries of individual authorities requires that Information Governance (IG) policies and procedures are adhered to at multiple organisations. | Ensure that the Data Sharing Agreements are in place and co-opt additional agreements only once the IG approval is in place. Ensure that there is IG representation from all organisations involved in the governance of the project. Guidance will be given to each organisation under the programme to ensure new or existing Data Sharing Agreements cover all intended data sharing activity.   | Accepted   | The actions of participating organisations is largely outside of the projects control, however guidance and agreements will be put in place to support appropriate behaviour. It is in the interests of the programme to work with organisations adhering to legislations and regulations. |
| A, D, G.    | Data security is compromised and data is accessed illegally or illegitimately.   | Robust security measures will be employed to protect the data processed by the Rotherham Health Record.<br><br>Work with IG and information security leads from the participating organisations to ensure their processes are robust and staff are appropriately trained.   | Reduced  | It is in line with the aims of the project to provide a robust and secure platform.  |
| A, B, G.    | Data shared via the Rotherham Health Record means someone acts in a way they would not have previously, in a way that is harmful to an individual.   | User acceptance testing to ensure data is shared clearly and accurately. Dissemination of information including offering training where new uses of a system or of data within a system are provided. Guidance will be offered for use of the Rotherham Health Record and end user training should be provided to ensure the safe and appropriate use of the data provided. It is the responsibility of individual staff members and their organisations to ensure that individuals are not harmed through their behaviour. | Reduced  | The solution fits with the intentions of the project to ensure that the RHR is used appropriately and safely and any changes to available data as a result of the platform are understood by participating organisations and end users.  |

|   | <b>Risk</b>   | <b>Solution(s)</b>  | <b>Result</b><br>(Is the risk eliminated, reduced, or accepted?) | <b>Evaluation</b><br>(Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)                                   |
|---|---|---|--|--|
| A | Free text within correspondence in respective source records may contain excluded conditions which may lead to incidental access by staff without a need to know. | Introduction of coded correspondence within clinical systems will reduce the reliance on free text sections on correspondence. Work with staff to ensure full awareness of their responsibilities if incidental access to sensitive information occurs. | Reduced  | Free text still available to clinicians. All staff however bound by confidentiality clauses in their contracts of employment. Access to RHR is strictly controlled on a role based, least privilege basis. |