DO NOT USE – INFORMATION PURPOSES ONLY

**Dated: xx/xx/xxxx**

**Information Sharing Agreement**

**For**

**The Yorkshire and Humber Care Record**

Document Contol

|  |  |
| --- | --- |
| Version Number: | 1.1 |
| Author (name) | Johnny Chagger |
| Name of approving committee | YHCR Central Team |
| Date Issued: | 04/06/2019 |

**Documents should be accessed via the Adoption Library on MS Teams to ensure the current version is used.**

**Updates**

|  |  |  |
| --- | --- | --- |
| New Version Number | Date | Change |
| Version 0.1 | 30/01/2019 | First draft |
| Version 1.0 |  | Update against review comments |
| Version 1.1 | 04/06/2019 | Revised in accordance to the Yorkshire and Humber care record requirements |

**Background Information**

The provision of high quality, evidence-based care requires the right information to be available to the right person at the right time and this, in turn, requires patient information to be shared within the health and social care community in a lawful and ethical way to support the provision, management and quality assurance of that care.

Information sharing is crucial to the operation of comprehensive and continually improving health and social care provision through partnership working and embracing new technologies.

Health and social care service providers have a legal responsibility to ensure that their use of personal data is lawful, properly controlled and that individual rights are respected. (For the purpose of this Agreement the terms “data” and “information” are synonymous.)

The balance between the need to share personal data to provide a quality service and the protection of confidentiality can be difficult to achieve and it is important that our service users are confident that their personal information is safe and secure and will only be shared in transparent and appropriate circumstances.

The aim of this document is to facilitate the processing of relevant and proportional personal data and special categories of personal data between the participating health and social care providers, in line with the recommendations of Caldicott Reviews of 1997, 2013 and the provisions of the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR).

## Introduction

1.1 The objective of integrated health and social care is to move away from isolated episodic care to a holistic approach, where those responsible for providing health, care and support work together to tailor and deliver a combination of services to meet the needs of the individual patient or service user.[[1]](#footnote-2)

1.2 Sharing information is essential to ensure the provision of efficient joined-up services; designed to give the best care and outcomes to an individual based on their personal needs and circumstances. The motto for integrated care services should be: ‘To care appropriately, you must share appropriately’[[2]](#footnote-3).

1.3 The Yorkshire and Humber Care Record (YHCR) supports the delivery of integrated care by providing health and social care professionals with a single point of access to information about a service user, collected from their separate medical and care records.

1.4 Processing such information is subject to the Data Protection Act 2018.

1.5 Service users must be informed about the YHCR.

1. Feel confident that personal information about them is held safely and securely;
2. understand how it is being collected and used, why it is being shared and with whom;
3. trust that it will only be shared appropriately when it is in their best interests; and
4. know what choices they have regarding the use of their personal information, the consequence of their decisions and how to raise concerns or exercise their rights in that respect.

1.6 It is also important that health and social care professionals and supporting staff understand and apply their legal and contractual duty to ensure their use of personal confidential data (PCD)[[3]](#footnote-4) is ethical and lawful and the rights of the service user are respected.

1.7 Registered professionals are also bound by the ethical codes of practice of their regulatory body.

1.8 The purpose of this document is to set out a common set of information governance rules that each party subject to this agreement will adopt to enable health and social care professionals supporting individual service users to share PCD via the YHCR.

1.9 This document does notprovide the legal basis for PCD to be shared. Consideration still has to be given to the legal implications that ensure fair and lawful processing.

1.10 This document does not provide legal advice. In some circumstances, it may be necessary or prudent to seek legal advice. Nothing within this agreement would prevent or restrict a partner organisation from doing so, however it is advisable that the lawyer’s response to a request for advice is shared with the other parties and this agreement is revised accordingly in light of those recommendations.

1.11 Neither is this agreement legally binding or enforceable between the signatory partners. Each partner is a Data Controller[[4]](#footnote-5) and legally responsible for ensuring their processing of personal data is fair and lawful and complies with the Articles of the GDPR and the DPA.

1.12 Each Data Controller must also be a signatory party of the supporting YHCR Data Processing Contract, which sets out the legal requirements for the operation of The Yorkshire and Humber Care Record to ensure compliance with the DPA and GDPR.

## Objectives

2.1 The objectives of this Agreement are to:

1. ensure service user rights are respected and to minimise the risk of breaking the law;
2. secure public trust by ensuring that legally required safeguards are in place and complied with;
3. define the purposes for processing PCD;
4. increase data processing by setting out the principle for sharing PCD about individual service users when it is in their best interest;
5. provide a framework for the secure management of PCD;
6. ensure staff have a better understanding of when and whether it is acceptable to process PCD;
7. harmonise where possible and support the policies and procedures of each partner organisation regarding the security and confidentiality of personal data; and
8. define how the Agreement will be authorised, implemented, published, monitored and reviewed.

## Duration and Scope

3.1 This document is an Information Sharing Agreement between the integrated health and social care partners in Yorkshire and Humber listed in Section 4 and will commence from xx/xx/xxxx.

3.2 It is specifically designed to support the development of the YHCR to enable lawful processing of PCD between the listed partner organisations to support integrated care where it is necessary for the safe, effective care of the individual service user.

3.3 This Agreement is supplemented by the policies, procedures and guidelines of the partner organisations.

3.4 This Agreement is owned by the signatory parties.

3.5 On behalf of the signatory parties the YHCR Steering Group will undertake responsibility for the development of jointly agreed policy and procedure that is necessary to support this Agreement and outlined in Section 10; monitoring subsequent external developments in information governance policy and law that may impact on the agreed terms and conditions.

3.6 The YHCR Steering Group will ensure any proposed changes and updates to this agreement are communicated to the signatory parties and to the YHCR Project Board.

3.7 The YHCR Project Board will undertake responsibility for signing off the proposed changes and updates on behalf of the signatory parties, ensuring a period of time has been allowed for consultation.

3.8 All signatories are responsible for communicating any concerns about the proposed changes and updates to the YHCR Board.

## The Conditions for Information Sharing

4.1 PCD should be processed between members of the care team when it is needed for the safe and effective care of the individual.

4.2 Information processing for the purpose of this agreement is dependent upon the individual service user being informed that their YHCR will be created and understand how and when their PCD will be used, who it will be shared with, and are aware of their rights in that respect and what actions they should take if they have any concerns or wish to exercise their right to object.

4.3 The agreed approach is to ensure all Yorkshire and Humber residents are informed via a series of planned Yorkshire and Humber communications, which gives people the right to object to the processing of the information if they so choose.

4.4 For the purpose of this pilot, communications materials, including fair processing notices and leaflets are provided in the Adoption YHCR Library, a copy of which is available at [www.yhcr.org](http://www.yhcr.org).

4.5 Each partner organisations will manage the objections made by individuals to the processing of data in the YHCR.

4.6 There is a dependency upon each separate organisation and GP Practice to ensure the service users have been adequately informed about the YHCR There is dependency on each separate organisation and GP Practice to advise service users on their options prior to them registering their objection in relation to the processing of information in the YHCR

4.7 Because there is a risk that the service user may not be aware of the YHCR or have had an opportunity to register their dissent prior to it being made available to the care team, staff are advised to ask the service user if they are aware that their YHCR has been created and do they have any objections to it being viewed prior to their record being accessed. This is referred to as “Approval to view” and is in-line with best practice and the national approach.

## The Purpose(s) for Information Sharing

5.1 Information should be processed between authorised health and social care professionals and their teams with whom the individual has a legitimate relationship where it is necessary for the primary purpose of their “direct care”.

5.2 “Direct care” is defined as a clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that contribute to the diagnosis, care and treatment of an individual) [[5]](#footnote-6). It includes:

* 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

5.3 It does not include research, teaching, financial audit or risk stratification.

5.4 Data will be effectively ‘de-identified’ for any other purpose that does not constitute a “direct care” purpose (a secondary purpose), unless the individual service user has provided their explicit consent or another lawful basis can be applied to support the justifiable use of that PCD.

## The Types of Information to be processed.

6.1 Only information that is necessary, relevant and proportionate to the direct care purpose will be processed.

6.2 A schedule of information items to satisfy this aim will be developed, agreed by the signatory partners and subsequently issued as Appendix B to this Agreement.

## Information Excluded from the YHCR:

7.1 Information of a highly sensitive nature will not be shared routinely via the YHCR which includes:

* Legally restricted data i.e.
* IVF, fertility treatment and Embryology[[6]](#footnote-7);
* HIV/AIDS;
* Venereal disease and STI’s[[7]](#footnote-8);
* Gender realignment[[8]](#footnote-9)
* Sensitive data that patients would not expect to be routinely disclosed i.e.
* Termination of pregnancy;
* Gender identity
* Specific information collected during an enquiry into safeguarding concerns
* Carer records
* Service user financial status

This list is not exclusive and will be further considered and completed during the development of the information sharing schedule (part 7 Appendix B).

7.2 This does not prohibit the information from being shared outside the YHCR. Information sharing agreements that cover the sharing of information for these purposes should be followed.

## Restrictions on the use of Information

8.1 All information that is processed, personal or otherwise, must only be used where it is necessary, relevant and proportionate for the purpose of direct care and in accordance with the service user’s expectations (as explained in the YHCR communications programme) and specified in this agreement.

8.2 Exceptions to this are only applicable when the disclosure is mandated by statute or regulation, under the instructions of a court or via obtaining the explicit consent of the service user.

8.3 Any further uses made of this data will not be covered by the Agreement and will be in breach of the Agreement and at risk of being unlawful. This would be managed in accordance with each partner organisations local incident management policies and procedures.

## Access to information

### 9.1 Authorised Health and Social Care Staff

Access to the YHCR will be provided to health and social care professionals and their teams involved in the provision of **direct care** to service users and controlled in accordance with the YHCR Access Management policy and procedure, developed by the Leeds Teaching Hospitals NHS Trusts Information Governance Team, agreed by the YHCR Project Board and issued as Appendix C of this Agreement.

The Data Consumer Organisations will manage the user access management procedures, including the registration and de-registration of access, on behalf of the YHCR partners.

**9.2 Individual service users**

Article 15 of the GDPR provides an individual with a right of access to their personal data.

It is the responsibility of each individual partner agency to manage subject access requests for the personal information they hold.

If The Data Consumer Organisations receive a subject access request for YHCR data, they will refer the service user to the relevant organisation.

**9.3 Access to PCD for non-direct care purposes**

9.3.1 Only professionals directly involved in the provision of direct care should see an individual’s confidential identifiable information held in the YHCR.

9.3.2 Identifiable information should not be accessed directly by, or passed to a third party, unless there is another legal basis can be applied to support the disclosure or the individual service user has been informed and given their explicit consent (which is recorded as evidence).

9.3.3 Where another legal basis does apply, the individual service user concerned must be informed of the intention to disclose, unless to do so would cause harm (either to the individual themselves or put another person at risk) or it would be detrimental for the purpose (e.g. it would prejudice the prevention or detection of a serious crime).

9.3.4 Any decision to disclose information about a service user for a non-direct care purpose (e.g. because the information is required by a court order/statute or there is an overriding public interest in doing so), must only be made by the organisation responsible for that information on a case-by-case basis, seeking additional legal or other specialist advice where appropriate.

9.3.5 If the Data Consumer Organisations receive a request for PCD for a non-direct care purpose, they will refer the requestor to the relevant organisation.

**9.4 Requests for Access to non-PCD Information**

9.4.1 The procedure for managing requests for information, including requests made under the Freedom of Information Act 2000, will be documented and approved by the YHCR Project Board.[[9]](#footnote-10)

9.4.2 The Data Consumer Organisations will manage requests for information concerning the YHCR in accordance with the approved YHCR Access Management policy and procedure (see 10.1) on behalf of the YHCR partner agencies.

## Data Protection Legislation

**19.1 Data Controllers**

10.1.1 In the terms of the GDPR a Data Controller works alone, jointly or in common with other data controllers, depending on the circumstances of the data processing activity[[10]](#footnote-11).

10.1.2 Each Health and Social Care partner is an individual Data Controller and is alone legally responsible for ensuring their processing of PCD is done fairly and lawfully in compliance with data protection legislation.

10.1.3 Any processing of personal data undertaken by a Data Controller and their staff, is undertaken in their own right and each Data Controller party to this Agreement is not liable for the actions of another.

10.1.4 The GDPR conditions for processing are listed in Appendix D.

10.1.5 The Data Controllers work jointly to decide and agree the policy under which the YHCR will operate.

10.1.6 The Data Controllers work in common sharing the pool of information held in the YHCR, which they process independently of each other under the terms of this Agreement and in accordance with the law.

**10.2 Data Processor**

10.2.1 Humber Teaching NHS Foundation Trust is a Data Controller in respect of the personal data held about their patients.

10.2.2 Humber Teaching NHS Foundation Trust also acts as the Data Processor in respect of their duties in the provision and hosting of the YHCR service and the management functions outlined in this document.

**10.3 Article 28 & 32 GDPR**

10.3.1 Article 32 of the GDPR requires an assessment to ensure that the appropriate level of security is applied to the processing of data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

10.3.2 In particular, where a Data Controller enters into an arrangement with a Data Processor to process personal data on their behalf, that arrangement must be supported by a written contract Article 28 of the GDPR states processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. takes all measures required pursuant to Article 32 of the GDPR;
4. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR;
5. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the processor;
6. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
7. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (g), the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

## Information Governance Agreement

11.1 An objective of this agreement is to provide assurance that all parties will work to the same level of information governance standards.

11.2 This is measured through the annual self-assessment audit against the service-specific standards set out in the Data Security and Protection Toolkit or equivalent standard. Non-compliant organisations will have their access revoked and would be required to have formal discussions regarding access.

11.3 In particular, to support the YHCR Information Sharing agreement, it is the responsibility of each partner to:

* Identify a named individual(s) who takes responsibility for this Agreement on behalf of the partner organisation;
* Identify a named individual to act as the organisation’s central point of contact to support the operation of YHCR information sharing;

Have procedures and policies in place to ensure:

* Staff (including temporary staff, agency staff, secondee’s, contractors, students, placements and volunteers) who have access to the YHCR have been trained and understand their legal and contractual duties for the protection and use of confidential information;
* Organisational and technical security measures protect the integrity, confidentiality and reliability of PCD held in the YHCR e.g. via documented access controls, contracts of employment, codes of conduct, information governance policies and education and training programmes;
* Information is of a quality fit for the purpose for which it is to be used; including being complete, accurate and up to date, otherwise any decision based on the information may be flawed and inappropriate actions may result;
* Policies and procedures are in place to detect, report, investigate and manage personal data breach incidents[[11]](#footnote-12), which include provisions for informing the Information Commissioner’s Office and the data subject(s) as appropriate;
* Appropriate Human Resources procedures are in place to deal with staff responsible for a personal data breach incident and all staff are made fully aware of those procedures;
* Procedures are in place and published to deal with individual service user’s rights i.e. procedures for dealing with requests for access to personal data, right to information, right to object to certain data sharing, queries and complaints.

## Information Sharing Agreement

12.1 All partners agree to uphold the common law duty of confidentiality, the GDPR and Human Rights Act 1998 and ensure PCD is shared fairly, lawfully and responsibly in accordance with the Caldicott Principles and NHS Digital Confidentiality Code of Practice.

12.2 All partners agree to implement the YHCR fair processing communications toolkit without exception to support fair and lawful information sharing for integrated care purposes.

12.3 All partners agree to publish this agreement in addition to other fair processing information to support openness and transparency.[[12]](#footnote-13)

12.4 All partners agree to work together to establish and implement technical and organisational policies and procedures that support the sharing of PCD in accordance with this Agreement.

## Responsibility for this Agreement

13.1 Each partner takes responsibility for ensuring the application of the terms and conditions of this Agreement within their organisation.

13.2 The YHCR Project Board will take responsibility for ensuring the overall management of this Agreement, including its continual monitoring, revision and updates.

13.3 Additional supporting materials, such as policy, procedure or subsequent amendments to this Agreement will only be approved by the YHCR Project Board following consultation with all signatory partner organisations and issued as agreed supplementary appendices.

13.4 This Agreement will be subject to a formal annual review by the YHCR Project Board, taking into consideration:

* non-compliance issues with this Agreement, logged and reported by any party (including complaints arising from information sharing);
* non-compliance with any supplemental policies, procedures and guidelines, logged and reported by any party (including complaints arising from information sharing);
* any general difficulties encountered in applying this Agreement, logged and reported by any party.

13.5 An earlier review may be necessary to take changes in the law and/or national policy into account. The YHCR Project Board will be advised by the Data Consumer Organisation’s Information Governance Team/Lead of any such change and will decide whether or not a formal review is required. All signatory parties will be advised accordingly.

**15. Signatories, Publication and Review**

This Agreement shall be signed on behalf of each party by its Caldicott Guardian.

This Agreement will be published in accordance with the terms of the Freedom of Information Act 2000.

This Agreement may be executed in counterparts, each of which shall be deemed to be an original document but all of which taken together shall constitute one single agreement between the Parties.

**On behalf of >name of organisation< the following authorised signatories agree to the terms set out in this Agreement.**

**Name:**

**Designation:**

**Signature: - Date:**

**Organisation Address:**

**The following person will act as the organisation’s central point of contact for matters concerning this Agreement:**

**Name:**

**Contact details:**

**Email:**

**Telephone:**

**Glossary:**

**Anonymisation:** The process of removing identifiers from a set of data so that there is little or no risk of the individual being identified from that data or by matching it to other data (identification is not likely to take place).

**Caldicott Guardian:** A senior person within an organisation who is responsible for ensuring the protection of confidentiality of patient and service-user information and enabling appropriate information sharing.

**Consent:** The approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be ‘no surprises’) and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

**Data Controller:** (DPA Part 2 Ch. 2)& (GDPR Ch. 1 Art. 4) A person (individual or organisation) who determines the purposes for which and the manner in which any PCD are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA and GDPR.

**Identifiable Information: also Personal Data, Confidential Data etc.** See ‘PCD’.

**Information Governance (IG):** How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

**Personal Confidential Data (PCD):** This term describes personal information about identified or identifiable individuals, which should be kept private or secret. ‘Personal’ includes the DPA and GDPR definition of personal data, but it is adapted to include deceased as well as living people. ‘Confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’ and is adapted to include ‘special categories’ as defined in the Data Protection Act and GDPR.

**Personal data** (DPA Part 2 Ch. 2) & (GDPR Ch. 1 Art. 4) Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

**Personal data breach incident**: A data breach is any failure to meet the requirements of the DPA & GDPR. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data and inappropriate invasion of people’s privacy. It includes paper-based information (such as a letter going to the wrong address) as well as electronic data. (Source: Independent Information Governance Review Department of Health March 2013).

**Processing:** Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

* organisation, adaptation or alteration of the information or data;
* retrieval, consultation or use of the information or data;
* disclosure of the information or data by transmission, dissemination or otherwise making available; or
* alignment, combination, blocking, erasure or destruction of the information or data.

**Pseudonymisation:** Data in which individuals are distinguished through the use of a unique identifier, which does not reveal their ‘real world’ identity, but identity, can be determined by reversing the process. It is considered to be anonymised data where the recipient of the pseudonymised data set has no means of access to the algorithmic key to re-identify individuals.

**Special Categories of Personal Data/Information:** (DPA Part 2 Ch. 2) &(GDPR Ch. 2 Art. 9) Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual. See also ‘PCD’.

**Appendix A:**

**List of Organisations signed up to this Agreement**

For the purpose of this pilot, the full list of participating organisations can be found at the following public facing web address for the project:

<https://yhcr.org/>

**Appendix B**

**Information Schedule**

**(The categories of information to be shared and excluded from the YHCR)**

**Information being shared**

|  |  |  |
| --- | --- | --- |
| Data\* | Date | GPCare Setting |
| Patients (which includes >>  o   Appointments  o   Encounters  o   Allergy Intolerances  o   Conditions  o   Clinical Impressions  o   Observations  o   Diagnostic Reports  o   Medication Statements  o   Care Plans Presence (that incorporate End of life)  o   Questionnaires (that incorporates End of Life)  o   Care Teams  o   Referral Requests  o   Flags |  | Multiple - could be, acute, general practice, community, mental health or social care |

This list is consistent with Professional Records Standards Body (PRSB) guidance on data inclusion in health and care records. The list is not exhaustive nor will all data items be provided by all data controllers.

To support transparency and fair processing, the public facing website will be kept up to date with significant enhancements to the system once live data is flowing which can be found at:

<https://yhcr.org/>

**Information being excluded**

Please see section 7

**Appendix C**

**Yorkshire and Humber Care Record** **Access Management Policy & Procedure**

**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 organisationswill needto 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[[13]](#footnote-14) 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 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.

**Appendix D**

**The GDPR Conditions for Processing for the Purposes of the First Principle.**

Article 5 of the GDPR requires personal data to be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

**Fairly.**

The requirement to process PCD fairly will be met by informing all Yorkshire and Humber citizens about the YHCR the benefits and their right to raise an objection to how their data is processed by using the fair processing materials provided in the YHCR Communications Toolkit.

In addition to this commitment to transparency, PCD will only be shared where it is necessary, relevant and proportionate for the purpose of direct care in accordance with the service user’s expectations and specified in this Agreement.

**Lawfully.**

Each organisation party to this Agreement is established to provide health care or social care services to the local population.

Each organisation will ensure that their processing of PCD is fair and lawful, taking into account their respective duties under the common law duty of confidence, the principles of the Article 6 and 9 of the GDPR, Article 1, 8 and 10 of the Human Rights Act 1998.

**GDPR Article 6.**

Paragraph (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;

**GDPR Article 9.**

Paragraph (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.

**-----END-----**

1. The term “service user” is a general term used within this document to mean any individual, patient, social care client or user of services – anyone who receives health and social care services. [↑](#footnote-ref-2)
2. Information Governance Review: Information: To Share or Not to Share? Department of Health March 2013 also referred to as “Caldicott 2”. [↑](#footnote-ref-3)
3. Personal Confidential Data is a term introduced by Caldicott 2 to describe the full range of information about an individual used within health and social care. See glossary for the full definition. [↑](#footnote-ref-4)
4. 4 A person (individual or organisation) who determines the purposes for which and the manner in which any PCD are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA and GDPR. [↑](#footnote-ref-5)
5. Health and Social Care Information Centre Confidentiality Guidance for Health and Social Care - references [↑](#footnote-ref-6)
6. Restricted by the Human Fertilisation Act 1990 as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992 [↑](#footnote-ref-7)
7. NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000 [↑](#footnote-ref-8)
8. Gender Recognition Act 2004 [↑](#footnote-ref-9)
9. As part of the YHCR Access Management policy under 7 [↑](#footnote-ref-10)
10. GDPR Ch. 2 Art. 5 - 11 [↑](#footnote-ref-11)
11. The Independent Information Governance Review Panel recommended the term “personal data breach incident” to be used as the standard term for health and social care services to cover ‘data losses’, ‘personal data breaches’ and ‘information governance serious incidents’ etc. See Glossary. [↑](#footnote-ref-12)
12. Fair processing is a requirement of Article 6 of GDPR (Lawfulness of processing) [↑](#footnote-ref-13)
13. [The Information Governance Review: To Share or Not to Share](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf) [↑](#footnote-ref-14)