NHS Rotherham Clinical Commissioning Group

AQuA – 3rd March 2020

Governing Body – 5th August 2020

REVIEWED AND AMENDED: DATA PROTECTION AND ACCESS TO HEALTH RECORDS POLICY

Lead Executive:	Ian Atkinson, SIRO & Deputy Chief Officer
Lead Officer:	Andrew Clayton, Head of Digital
Lead GP:	Not Applicable

Purpose:
It is good practice to regularly review policies, practices and procedures. Policy reviews ensure the policies are consistent and effective which is especially important for high-risk or highly regulated industries such as healthcare.
Background:
The Data Protection and Access to Health Records Policy explicitly recognises Rotherham CCG's obligations under the Data Protection Act 2018 (DPA) alongside the requirements of the General Data Protection Regulation (GDPR).
Analysis of key issues and of risks
The policy continues to address the information security risks to Rotherham CCG's information assets.
Patient, Public and Stakeholder Involvement:
No Patient, Public and Stakeholder Involvement required
Equality Impact:
Updated the applied and review date
Financial Implications:
There are currently no additional financial implications associated with the item as presented.
Human Resource Implications:
No Human Resource Implications
Procurement Advice:
No Procurement
Data Protection Impact Assessment:
No Data Protection Impact Assessment Required
Approval history:
IG Group – 25.02.2020 AQuA – 03.03.2020
Recommendations:
Governing Body are asked to ratify the changes to the amended Data Protection and Access to

Health Records Policy as per in the amendments summary below.
Paper is for Ratification

Data Protection and Access to Health Records Policy Amendments Summary

Ref./ Change	Reason
Updated Table of Contents	Reflect changes in amended document, page numbers and format
Key Legislation and Guidance Updated references to include all 3 Caldicott Guardian Reports and the latest Caldicott Guardian Manual 2017	Since the original paper there have been 3 Caldicott Guardian Report and the latest Manual is 2017
Definitions Section (pg 5) Included Data Protection Impact Assessment and definition.	Data Protection Impact Assessment term is used in policy but doesn't provide definition.
Removed: A number of references to GDPR becoming applicable on the 25th May 2018	Past 25th May 2018
Removed: Reference to the DPA 1999 and its 8 principles (1.2); and Replaced with: GDPR and DPA 2018 6 Principles.	No longer relevant. Document now covers the 6 principles in GDPR and DPA 2018 (See 1.2)
Removed: Information Governance frameworks issued by the Department of Health. (1.6) Replaced with: Requirements of NHS Digital's Data Security Protection Toolkit and NHS England guidance (1.6)	Reference to IG Frameworks and Department of Health involvement out-dated. Updated to cover current requirements.
Registration and Notification to the Information Commissioner (pg9) Included: The Data Protection Officer is responsible for maintaining a record of the CCG's processing of personal data	Included the responsibility of the DPO for maintaining records and ICO involvement.
Record Keeping and Storage of Personal Data (pg 10) Updated: Reference to where data will not be disclosed and where health and social care data is processed by a court; and included reference to section 9.2 Withholding Data.	GDPR strengthened the rights of Individuals including right of access, however the GDPR allowed a number of derogations. The DPA 2018 used the derogations and included a wide range of exceptions to providing data. Changes here include where healthcare or social care information is requested but where there is an ongoing court case which may require restrictions.
Included: 7.4 statement re National data opt out	7.4 statement to comply with National data opt out and to be consistent with Information Asset Register, DPIA and Privacy Notice.
Reworded: Upon a written request from the Data Subject to *Upon a valid request from the Data Subject*	Replace written with valid as GDPR doesn't state that a SAR or ROA needs to be in a written form. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ The CCG still needs to apply the appropriate technical and organisational measures to protect data.
Reworded: 9.1.3 References to charges and changes on the 25th May 2018.	Reference to 25th May 2018 no longer relevant.
Reworded: 9.1.4 and proof of identity regarding staff	GDPR states that you only need sufficient

members requests.	proof to establish an identity to provide them with the information requested therefore if an existing employee requests their information the employer then asking for excessive proof of identity would not be compliant with legislation.
9.2 Withholding Information (pg 13) Reworded: Whole Section See Appendix A below	There is insufficient information to support the CCG in its decision making to be compliant with the transparency principle 1 GDPR and the Right of Access where information is being withheld. The decision to withhold is a serious one as it leaves the CCG vulnerable to Data Subjects claims to breaches of their rights under legislation and the ICO enforcement powers.
Appendix 1 Procedure for responding to Data Subject Access Requests (pg17) Reworded: 4th Process on flow chart. Notes copied and passed to the Governance Officer or originals passed to the Governance Officer for copying - information which may cause distress or relating to third parties to be withheld/redacted as appropriate To *Notes copied and passed to the Governance Officer or originals passed to the Governance Officer for copying –Withholding or redacting information as agreed per section 9.2*	Included reference to Section 9.2 when withholding information.

Original Wording	New Wording
9.2 Withholding Data 9.2.1 Data may be withheld if: • the Subject agrees. • it identifies a third party • whereit has been decided that giving access would disclose information likely to cause serious harm to the physical or mental health of any individual. 9.2.2 It is possible to refuse to respond to manifestly unfounded or excessive requests under GDPR but the CCG must explain to the individual of their right to	9.2 Withholding Data 9.2.1 The decision to withhold data following the making of a legitimate subject access request is a complex one based on a number of legal exemptions[1]which require consideration including the balancing of rights of individuals and public interest. Therefore each request needs to be considered on a case by case basis. <u>Decision making and involvement</u> 9.2.2 Each decision to withhold information would need the following decision making involvement • The decision to withhold health and/or social care information must involve the CCG's Caldicott Guardian. • All decisions to withhold information must have involved the CCGs Data Protection Officer (DPO).

[1] Exemptions to the DPA 2018 are detailed in Schedules 2-4 of the DPA 2018.

complain to the Information Commissioners Office as soon as possible and at the latest within one month.	• The Chief Officer (Accountable Officer) can decide to withhold data that is contrary to the advice of the Caldicott or DPO however this needs to be reported to the Governing Body and state the reason(s) why. <u>Decision making considerations</u> 9.2.3 Further considerations may include: • whether to seek legal advice; and • the legal timescales to respond to the request To assist in consideration of withholding information the CCG will consider: a) the data subject agrees to the withholding. b) if the data identifies a third party c) if the health or social care data is being processed by a court d) if a third party would suffer serious harm as a result of disclosure e) if there could be serious harm to the physical or mental state of the data subject would result from the disclosure f) if the information was provided on the strict understanding that it would not be disclosed to the data subject g) if information relates to negotiations e.g. employment negotiations h) if the request is manifestly unfounded i) if the request is excessive Other exemptions considerations could include the areas of: • Crime, law and public protection • Regulation, parliament and the judiciary • Journalism, research and archiving • Finance, management and negotiations • References and exams Exemption c. only applies if the health or social care data is: • supplied in a report or evidence given to the court in the course of proceedings; and • those proceedings are subject to certain specific statutory rules that allow the data to be withheld from the individual it relates to. <u>Information to be provided to the Data Subject</u> 9.2.3 If partial data (redacted) or whole data is withheld then unless under exceptional legal circumstances the Data Subject will need to be informed of:

	• The reason why the data has been withheld. • Their right to make a complaint to the ICO; and • Their ability to seek to enforce this right through a judicial remedy The requestor must be informed of this as soon as possible and at the latest within one month. Further guidance can be found on the ICO's Guide to the General Data Protection Regulation (GDPR)[2]

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

NHS
Rotherham
Clinical Commissioning Group

Title:	**Data Protection and Access to Health Records Policy**
Reference No:	001-IT
Owner:	Deputy Chief Officer
Author	Information Governance Lead
First Issued On:	April 2013
Latest Issue Date:	February 2018
Operational Date:	March 2020
Review Date:	March 2022
Consultation Process	IG Group to AQuA via OE
Ratified and approved by:	Governing Body TBC
Distribution:	All staff and GP members of the CCG.
Compliance:	Mandatory for all permanent and temporary employees of Rotherham
Equality & Diversity Statement:	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

Associated Documentation:

Legislation and Guidance key to allow information sharing to take place:

- Access to Health Records Act 1990
- Caldicott Guardian Manual 2017
- Caldicott Reports 1998, 2012, 2016
- Code of Professional Conduct NMC 2004
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990 (as amended by the Serious Crime Act 2015)
- Confidentiality and Disclosure of Information BMA 2008
- Confidentiality Guidance for Doctors GMC 2009
- Crime and Disorder Act 1998
- Data Security and Protection Toolkit
- Data Protection Good Practice – Information Commissioners Office
- Environmental Information Regulations 2004
- Fraud Act 2006
- Freedom of Information Act 2000
- Guide to The General Data Protection Regulation – Information Commissioners Office
- Health and Social Care (Safety and Quality) Act 2015
- Health and Social Care Acts 2001 and 2008 and 2012
- Human Rights Act 1998
- Limitations Act 1980
- Mental Capacity Act 1995 and Code of Practice 2007
- NHS Act 2006
- NHS Confidentiality Code of Practice 2003
- NHS Resolution Standards
- Public Records Acts 1958 and 1967
- Regulatory and Investigatory Powers Act 2000
- The Data Protection Act 2018
- The General Data Protection Regulation 2016/679
- The Law of Confidentiality
- Records Management Code of Practice for Health and Social Care 2016

Commissioning Organisation and Related Policies:

- Conditions of Contract
- Information Security Policy
- Safe Haven Policy
- Portable Data Policy
- E-mail Policy
- Freedom of Information Policy
- Conditions of Contract
- Information Security Policy
- Safe Haven Policy
- Portable Devices and Smartphone & Tablet Policy
- Email Policy
- Records Management Policy
- Freedom of Information Policy

Revision History

Date of this revision: February 2020

Revision date	Previous revision date	Summary of Changes
26th February 2002		First Draft
August 2010	26th February 2002	Aligned with Rotherham Foundation Commissioning Organisation Policy. Dissemination plan. Extra Training requirements Additional compliance monitoring and reporting.
March 2011	August 2010	Final approved document
July 2012	March 2011	Review in preparation for organisation change to CCG status: replacement of "Trust" with "Commissioning Organisation". Addition of: • Mobile device as media on which information is held or processed. • Related legislation • Definitions page Replacement of : • "Chief Executive" with "Accountable Officer" • Specific job titles with roles. • Some job roles replaced by "provider" or "nominated lead" Reference to CCTV added. Appendices updated to reflect current practice.
October 2014	July 2012	Minor formatting changes and update Commissioning Organisation to Clinical Commissioning Group (CCG)
April 2015 and July 2015	October 2014	Inclusion of a flow chart and minor formatting changes to highlight additional detail re subject access requests
October 2016	July 2015	Updated list of relevant legislation to include Health and Social Care Acts 2012 and 2015 and new Records Management Code of Practice Removed reference to Sub-AQuA – replaced with IG Group Updated SAR process flow chart to reflect changes to CHC
October 2017	October 2016	Updated in line with General Data Protection Regulation which comes into force on 25th May 2018
February 2020	October 2017	Removed out dated references Reworded 9.1.3; 9.1.4; 9.2 and process in Appendix 1

Contents

DEFINITIONS

Term	Definition
Data Users	Employees of the Commissioning Organisation or independent contractors who record, store and/or process personal data in any form.
Data Subjects	Individuals who are the subjects of personal data.
Personal Data	Data relating to a living individual who can be identified from the information, or any other data 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.
Record of Processing Activities (ROPA)	It is a tool to help you to be compliant with the DPA and GDPR (Art. 30) by creating an inventory of data processes including personal data.
Data Protection Impact Assessment	A Data Protection Impact Assessment (DPIA) is a process which helps to identify and minimise the data protection risks of a project. Organisations must conduct a DPIA for processing that is likely to result in a high risk to individuals.
Data processing	Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data e.g. adaptation, alteration, retrieval, disclosure, dissemination, blocking, or destruction.
Sensitive data (special category data under General Data Protection Regulation (GDPR))	The Data Protection Act and GDPR defines categories of sensitive personal data, namely, personal data consisting of information as to:- a) the racial or ethnic origin of the data subject, b) their political opinions, c) their religious beliefs or other beliefs of a similar nature, d) whether they are a member of a trade union, e) their physical or mental health or condition, f) their sexual life, g) the commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. Under GDPR this also includes: h) Genetic Data and i) Biometric data
Access to Health Records of a Deceased Person	The Data Protection Act 2018 and GDPR excludes deceased persons but a duty of confidentiality extends beyond death for health records and the above definitions are still relevant although access is granted through the Access to Health Records Act 1990
Information Asset Owner	Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for.

1. Aims and Purpose of the Policy

1.1 The purpose of this policy is to explicitly recognise Rotherham CCG's obligations under the Data Protection Act 2018 (DPA) alongside the requirements of the General Data Protection Regulation (GDPR). This will be achieved by setting a framework that aims to ensure that all employees, contractors, agents, elected members, partners or other service providers are fully aware of and abide by their duties and responsibilities under the DPA and GDPR and also taking account requirements set out in the following legislation:

- Crime and Disorder Act 1998
- Human Rights Act 1998
- Police Act 1997
- Access to Health Records Act 1990

1.2 The CCG will ensure that personal data is handled, legally, securely, efficiently and effectively and in accordance with the DPA 2018 and GDPR principles:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of the data subject for no longer than is necessary
- processed in a manner that ensures appropriate security of the personal data

1.3 The DPA and GDPR does not have principles relating to individuals' rights or overseas transfers of personal data as these are specifically addressed in separate articles within the GDPR (Chapter 3 and 4 respectively). The GDPR requires organisations to show how they comply with the principles – for example by documenting the decisions taken about a processing activity.

1.4 This Policy additionally sets out the process for responding to Subject Access requests (**see Appendix 1**).

1.5 In order to operate efficiently the CCG will, where necessary collect and use data relating to patients receiving care and the people with whom it collaborates including members of the public, current, past and prospective employees, suppliers and other visitors. In addition, it may be required by law to collect and use data in order to comply with the statutory requirements of NHS England

1.6 All personal data, regardless of how it is collected, recorded, utilised, transferred and disposed of, and stored on whatever media, will be handled by the CCG within the safeguarding principles of the DPA, GDPR and by the requirements of NHS Digital's Data Security Protection Toolkit and NHS England guidance.

2. Scope of Policy

2.1 This policy applies to all employees carrying out work on behalf of the CCG, including Medical and Dental employees, contractors, agents, elected members, charitable groups and partners. Other service providers of the CCG should abide by their duties and responsibilities under the DPA and GDPR, which should be set out in contracts, and also taking account of any requirements within associated legislation.

2.2 This policy applies to the handling of ***all*** Personal Data that is used within the CCG held on any media including Dictaphone, computer system, mobile device or manual records.

3. Roles and Responsibilities

3.1 Data Protection Officer

Under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. The role of Data Protection Officer is to facilitate the CCG's compliance with GDPR and will:

- Monitor CCG compliance with the DPA and GDPR
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to the DPA and GDPR and the protection of personal information
- Assist in implementing essential elements of the DPA and GDPR such as the principles of data processing, data subjects' rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches
- Maintaining a record of the CCG's processing of personal data (ROPA)

3.2 Caldicott Guardian

The Caldicott Guardian will have responsibility for ensuring the confidentiality of clinical records and authorisation of the sharing of patient information when consent has not been obtained. The Caldicott Guardian will have responsibility for approving all holdings, uses and disclosures of Personal Data used for clinical purposes with delegated roles and responsibilities clearly defined and appended to the job description.

3.3 Information Asset Owners

Information Asset Owners will be identified for all items of Personal Data kept and used by the CCG. The owners will normally be the most appropriate departmental managers and will be responsible for risk management of the information asset/s within their responsibility.

3.4 All Staff

All employees have a responsibility to ensure that they follow this Policy.

3.4.1 Employees must ensure that personal data is processed in a secure manner at all times to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage and to assure the integrity of the data using the technical and organisational measures provided by the CCG

3.4.2 In particular they will ensure that personal data is kept:-

- In a safe place where there would be no unauthorised access, and must not be left unattended in public/waiting areas
- In a locked filing cabinet or drawer where possible
- In an office with restricted access, or
- Where disk, memory stick, mobile device, dictaphone or other electronic storage system is used, appropriate security measures are applied in line with the organisations security policies.

3.4.3 Further guidance can be sought from the IT helpdesk and associated policies which can be found on the CCG's website.

3.4.4 Employees must:

- Check that any personal data they provide to the CCG or elsewhere is accurate and up to date
- Ensure data provided by and recorded for others (i.e. staff and patients) is accurate and up to date
- Inform the organisation of any changes to their personal data, e.g. change of address, change of name, photographic identity, etc.
- Check the accuracy of data, including sensitive data, which they may send out from time to time, in order to update existing personal data.
- Understand that they must be appropriately trained and supervised where necessary to handle data including requests for the disclosure or sharing of data.

3.4.5 Employees have the right to request a copy of their personal data held by the CCG.

3.4.6 Any breach of this Policy and Procedure may result in disciplinary action being taken as it is a breach of the Staff Code of Conduct on Confidentiality.

3.5 Where health records are used, the service lead for the service they provide will ensure health records are maintained according to national legislation and guidance.

3.6 Data will only be collected and processed to the extent that it is required to fulfil operational needs or to comply with any statutory or information governance standards.

3.7 The Data Protection Officer will provide support and advice to all employees on the application of this Policy in relation to clinical data/health records where necessary.

3.8 The nominated Human Resources lead must ensure that personnel data held by the organisation is protected from unauthorised or unlawful access, loss or disclosure. They will also act as the Information Asset Owner in relation to HR records and will collect and process appropriate data to the extent that it is required to fulfil operational needs or to comply with any statutory or information governance standards.

3.9 The nominated Human Resources lead will provide practical support and advice to all employees on the application of this Policy in relation to non-clinical data.

3.10 NHS Property Services shall be responsible for compliance with the DPA and GDPR and related legislation in relation to personal data obtained

through the use of CCTV.

3.11 Trade Unions/Employee Representatives may collect and maintain personal data in order to provide membership services and comply with certain statutory obligations (Special Category Data). All personal data will be treated with the utmost confidentiality and with appropriate levels of security.

3.12 Contractors/Support Services/Consultants/Partners or other Servants or Agents with the CCG must ensure that:-

- They and all of their employees who have access to personal data held or processed for or on behalf of the CCG are aware of this Policy and are fully trained in and are aware of their duties and responsibilities under the DPA and GDPR. Any breach of any provision of the DPA and GDPR will be deemed as being a breach of any contract between the CCG and that individual, company, partner or organisation.
- Data Protection audits required by the CCG are permitted upon request.
- The CCG is indemnified against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

4 Registration and Notification to the Information Commissioner

4.1 Under the DPA and GDPR it is no longer a requirement to notify the Information Commissioners Office (ICO) in relation to the CCG's use of personal information.

4.2 It is however expected that in order to demonstrate compliance with GDPR, organisations will need to keep a record of its processing activities.

4.3 The CCG's current registration with the ICO describes in general terms, the personal data being processed by the CCG and includes:

- Staff Administration
- Accounts and Records
- Health Administration and Services
- Research
- Crime Prevention and Prosecution of Offenders
- Public Health
- Administration of Membership Records.

4.4 The Data Protection Officer is responsible for maintaining a record of the CCG's processing of personal data.

5 Informing people of personal data NHS Rotherham CCG keeps about them

5.1 Data Subjects have a right to be made aware that the CCG holds their personal data, for what purposes it will be processed, to which third parties it could be disclosed and for what purpose under GDPR data subjects must also be informed of the retention periods for their data and information on how to complain about the use of their personal data.

5.2 All Data Subjects about whom the organisation holds, processes or discloses personal data will be informed of this in a Privacy Notice which will be published on the CCG's website. Staff will be informed using the guidance provided in the CCG's Code of Conduct on Confidentiality.

6 Record Keeping and Storage of Personal Data

6.1 NHS Rotherham CCG supports Data Subjects having open access to their personal data. Personal data will therefore be recorded with a view to the Data Subject having access.

- Personal data will be accessible and understandable to Data Subjects
- Personal data will be kept to a minimum sufficient for the purposes for which it was collected
- Personal data will only be held for the minimum period necessary for processing unless required to be kept for longer
- Third party information will not be disclosed without proper permissions being obtained
- Personal data, including archives, will be capable of being retrieved within the specified time-scales
- Personal health or social care data will not be disclosed to the Data Subject where[3]:
    a. The health and social care data is processed by a court
    b. A third party would suffer serious harm as a result of disclosure
    c. Serious harm to the physical or mental state of the Data Subject would result from the disclosure
    d. Information was provided on the strict understanding that it would not be disclosed to the Data Subject

Exemption a. only applies if the health or social care data is:

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the data to be withheld from the individual it relates to.

For further information see section 9.2 Withholding Data

7 NHS Rotherham CCG's Use of Personal Data

7.1 The CCGs use of personal data will not be outside of the scope of its current registered purposes.

7.2 Where personal data is to be used for educational purposes the explicit written prior consent of the Data Subject will be obtained and recorded. This requirement includes student access to case notes for case study purposes.

7.3 All research will be approved by the relevant ethical committee including the method for obtaining patient consent if personal data is to be used as in the research.

7.4 The CCG complies with the national data opt-out policy and the CCG has put procedures in place to review uses or disclosures of confidential patient information against the national data opt-out operational policy guidance.
Personal data used for Secondary Uses such as research, educational purposes or for performance monitoring purposes will be anonymised in

[3] Exemptions to the DPA 2018 are detailed in Schedules 2-4 of the DPA 2018.

context as stipulated within the Data Sharing Framework Contract and Data Sharing Agreements with NHS Digital.

8 Disclosure of Personal Data to Third Parties

The organisations disclosure of personal data will not be outside of the scope of its current registered purposes.

8.1 Routine Disclosures

- Personal data will not be disclosed to third parties without a legal basis and appropriate Information Sharing Agreements.
- Even authorised disclosures will be restricted to the minimum required for the purpose.
- Personal data will only be sent to third parties outside of the CCG who will handle the information in accordance with the Data Protection Act and GDPR.
- All third party companies requiring legitimate access to CCG systems will handle information in accordance with the Data Protection Act and GDPR.
- Disclosure of personal data relating to the commissioning process will be in accordance with the Code of Practice on Confidential Information.

8.2 Disclosures to the Police

- Requests for information from the police will be handled by an appropriate Senior Officer.
- Information will only be disclosed where it can be proved to be a requirement to comply with the relevant legislation.
- All requests should be made in writing and recorded.

8.3 Disclosures in the Public Interest

The organisation will disclose information in the public interest where:

- A Data Subject discloses information that incriminates them in a serious crime.
- A patient's health affects their ability to drive or hold a firearms license.

8.4 Transferring Data Abroad

Personal data will not be transferred outside of the United Kingdom unless that country or territory "ensures adequate level of protection" for the rights and freedoms of Data Subjects.

Transfers of data may be granted:

- Where the data subject has given **explicit consent**
- It is necessary to perform or make a contract
- By reason of substantial public interest
- Is part of personal data on a Public Register
- Is on terms approved by the Information Commissioner

All transfers will be authorised by the organisations Caldicott Guardian.

9 Subject Access Requests

9.1 The process for responding to Subject Access requests is outlined in **Appendix 1.**

9.1.2 Upon a valid request from the Data Subject, CCG is obliged to supply:-

- A description of the data
- The purpose for which data is being held
- The source of the data
- The person(s) to whom the data will be or may be disclosed
- Where possible the envisaged period for which the personal data will be stored, or the criteria used to determine that period
- The fact that the data subject has a right to request rectification or erasure of personal data, or restriction of processing
- Information on the right to lodge a complaint with the ICO
- The existence of any automated decision-making.

9.1.3 The CCG is unable to charge a fee for responding to Subject Access Requests. A reasonable fee may be charged under DPA and GDPR however for any further copies of the information or when a request is manifestly unfounded or excessive, but any fee must be based on administrative costs only and the reason for the cost.

9.1.4 Due to the type of information the CCG may hold about individuals and its sensitivity (particularly special category data) proof of identity will be required to ensure that data is provided to the correct individual.

The only exception to this is where and existing employee who is known makes a subject access request for their information to their line manager. Completion of subject access request documentation and submission to the Governance Officer however is still required.

<u>Required proof of identity documentation</u>

9.1.5 Two original pieces of documentation, for example a recent utility bill or bank statement showing the individual's name and current address, will be required. In some cases additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of the information held. Where the request is to be sent via the post, this will only be sent to the registered address for the individual. If another address is stipulated, this will be investigated further to determine the legitimacy of the request.

9.1.6 The CCG will supply everything requested that is held at the time the application was made within one month of the request being received. Under GDPR it is possible to extend this timescale by a further two months where requests are complex. However if this is the case the CCG must inform the individual within one month of the request and explain why the extension is necessary. NHS best practice recommends disclosure within 21 days.

9.2 Withholding Data

9.2.1 The decision to withhold data following the making of a legitimate subject access request is a complex one based on a number of legal exemptions[4] which require consideration including the balancing of rights of individuals and public interest. Therefore each request needs to be considered on a case by case basis.

Decision making and involvment

9.2.2 Each decision to withhold information would need the following decision making involvement

- The decision to withhold health and/or social care information must involve the CCG's Caldicott Guardian.
- All decisions to withhold information must have involved the CCGs Data Protection Officer (DPO).
- The Chief Officer (Accountable Officer) can decide to withhold data that is contrary to the advice of the Caldicott or DPO however this needs to be reported to the Governing Body and state the reason(s) why.

Decision making considerations

9.2.3 Further considerations may include:

- whether to seek legal advice; and
- the legal timescales to respond to the request

To assist in consideration of withholding information the CCG will consider:

j) the data subject agrees to the withholding.
k) if the data identifies a third party
l) if the health or social care data is being processed by a court
m) if a third party would suffer serious harm as a result of disclosure
n) if there could be serious harm to the physical or mental state of the data subject would result from the disclosure
o) if the information was provided on the strict understanding that it would not be disclosed to the data subject
p) if information relates to negotiations e.g. employment negotiations
q) if the request is manifestly unfounded
r) if the request is excessive

Other exemptions considerations could include the areas of:

- Crime, law and public protection
- Regulation, parliament and the judiciary
- Journalism, research and archiving
- Finance, management and negotiations
- References and exams

Exemption c. only applies if the health or social care data is:

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the data to be withheld from the individual it relates to.

[4] Exemptions to the DPA 2018 are detailed in Schedules 2-4 of the DPA 2018.

Information to be provided to the Data Subject

9.2.3 If partial data (redacted) or whole data is withheld then unless under exceptional legal circumstances the Data Subject will need to be informed of:

- The reason why the data has been withheld.
- Their right to make a complaint to the ICO; and
- Their ability to seek to enforce this right through a judicial remedy

The requestor must be informed of this as soon as possible and at the latest within one month.

Further guidance can be found on the ICO's Guide to the General Data Protection Regulation (GDPR)[5]

9.3 Deceased Patients

9.3.1 If the patient is deceased then neither the Data Protection Act nor GDPR applies. The Access to Health Records Act 1990 allows access to be provided for the patient's personal representative and any person who may have a claim arising out of the patient's death.

9.3.2 If the patient is deceased and where satisfactory evidence of entitlement is supplied, the CCG will therefore allow disclosure to:

- The deceased patients personal representative
- Any individual having a claim arising from the patient's death.

9.3.3 The CCG will withhold personal data*:*

- If the record contains a note that the patient did not wish the applicant to have access to the record, unless the application is in respect of a claim arising from the patient's death.
- Where it has been decided that giving access would disclose information likely to cause serious harm to the physical or mental health of any individual.

9.4 A Person's right of Access to Amend Their Personal Data

9.4.1 Data Subjects have rights to ensure that their personal data held is accurate and to prevent any processing likely to cause damage or distress.

9.4.2 Where the Data Subject requests an amendment to the personal data the CCG will:

- Amend the personal data with the appropriate file notes, where the health professional or appropriate CCG officer agrees with the amendment, or
- File the request and response within the individuals record where the health professional or appropriate CCG officer does not agree with the amendment.

10 Opting Out

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

10.1 Employees must read carefully any documentation which implies their consent to the processing of personal data, for example, the completion of a booking form for a conference which states that information may be used for other specific purposes.

10.2 On occasions where an employee may be asked to participate in any photographic or other publicity campaign on behalf of NHS Rotherham CCG consent will be assumed at the time unless the employee explicitly opts out.

10.3 Employees have the right to opt out of Direct Marketing and in deciding to do so should ensure that the relevant tick box is completed to withdraw personal details from any database.

10.4 The CCG will ensure that employees are kept informed of the methods used to arrive at any automated decisions (e.g. job applications) thereby giving the choice of opting out of the process.

11 Dissemination and Implementation of the Policy

11.1 The policy can be located from the CCG website. It will be re-launched following any review/update via the following communications plan:

11.2 An electronic version of the policy document will be circulated by the Complaints and Governance Officer to all staff and will ensure the policy is published on the CCG's website following ratification by the Governing Body.

11.3 Departmental leads must ensure that new policy documents are communicated to all relevant staff and that arrangements for training and support are identified. A record of how this communication has taken place should be available for audit purposes.

11.4 Departmental leads will ensure old paper versions are removed from the department.

11.5 Notification of the approval of the policy and its whereabouts will be printed in relevant communication materials.

12 Monitoring and Reviewing

12.1 The CCG will maintain a register of all Information Assets containing patient identifiable data and will map all information flows relating to these and review annually.

12.2 Performance in dealing with Subject Access requests will be monitored by the IG Group and reported annually to the Board.

12.3 The CCG will put in place procedures for systematically reviewing its arrangements for administering and managing Access requests. These procedures will include systems for auditing compliance with the relevant Acts.

12.4 The CCG will maintain a register of Data Protection breaches and will ensure that any learning points that arise from such breaches are used to improve related policies, standards, procedures and guidance.

12.5 This policy will be reviewed at least every 2 years to ensure that it remains up to date, effective and takes account of emerging good practice. Where new legal directions come into force, the policy will be reviewed in line with the commencement date of that legislation.

12.6 The CCG will commission audits as necessary regarding the process, compliance and if the policy is embedded within every day organisational activity.

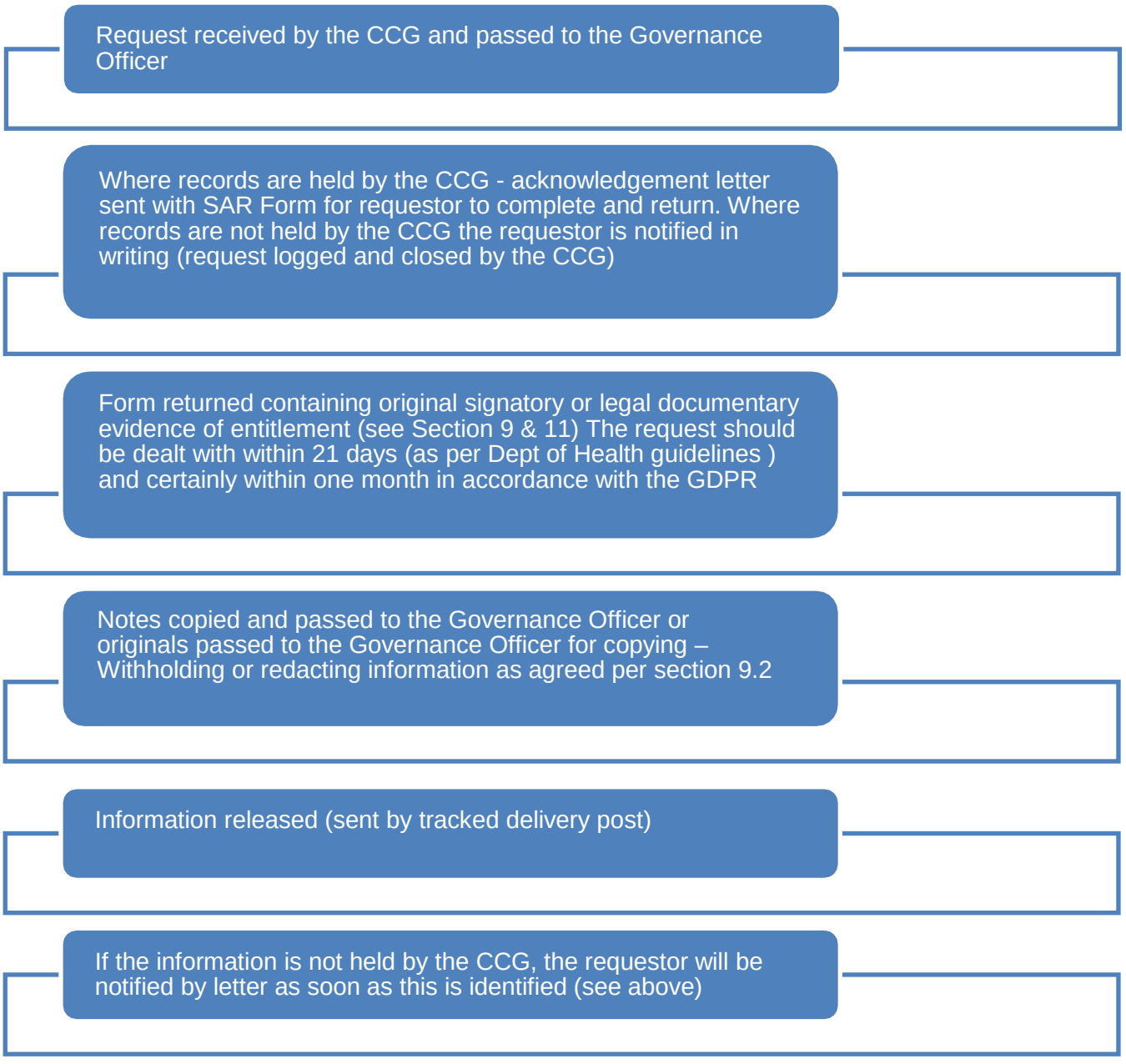
Appendix 1

Procedure for responding to Data Subject Access Requests

All Data Subject Access Requests (SARs) and Access to Health Records (AHR) requests should be directed to the Governance Officer immediately. The Governance Officer will process subject access requests on behalf of the CCG.

All information relating to any request is recorded on the tracking log from date of receipt of request and upon finalisation. This information is password protected for security purposes.

The following procedure should take place when a Data Subject Access Request is received from anyone for whom we hold records, or their representative.



Appendix 2

SUBJECT ACCESS REQUEST FORM GUIDANCE NOTES

1. **Personal Details**: Please complete your personal details as requested. Please tell us if you have been previously known by any other name. If you are requesting historical information, please provide as many details as possible, e.g. previous addresses (use a separate sheet if necessary).

2. **Details of the Data you require**: You should give as much assistance as you can about particular areas to search so that we can give you what you require without delay. You should also give any relevant reference numbers that might be useful. These details are required to assist in locating the data so that you can be given a copy of everything.

3. **Proof of Identification**: Proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, for example, a recent utility bill, bank statement (photocopies are not acceptable) showing your name and address. In some cases, additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of the information held.

4. **Keep your documents secure**: Always send important documents by recorded delivery or other special post as necessary. The CCG cannot be held liable for items lost in the post.

5. **If you have any questions** relating to identification requirements or any other aspect of a subject access request, please contact the Data Protection Officer.

Information Governance
Oak House
Moorhead Way
Bramley
ROTHERHAM
S66 1YY

Appendix 3

Subject Access Request - Response Template

a) Why are we holding your information?

b) What information are we holding (list all information being held & the source if not collected from the data subject)?

c) Has any of your information been shared with any third parties (a person or group besides the two primarily involved)?

d) The length of time we will be keeping your records?

Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016 sets out what people working with or in NHS organisations in England need to do to manage records correctly

https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

You have the right to request your information be corrected/deleted (if incorrect) from your GP and you have the right to object to your information being processed.
You have the right to complain if you are not happy with our response; please find details below for reporting your complaint to the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510

https://ico.org.uk/for-the-public/raising-concerns/

Appendix 4

NHS
Rotherham
Clinical Commissioning Group

Equality Impact Assessment

Title of policy or service:	Data Protection and Access to Health Records Policy	
Name and role of officer/s completing the assessment:	Andrew Clayton – Head of Health Informatics	
Date of assessment:	21.02.20	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	*(select one option - see page 4 for guidance)*

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	The Data Protection and Access to Health Records Policy documents the CCGs responsibilities in respect of the Data Protection Act 2018 (to be superseded by a Data Protection Act 2018 alongside the requirements of the General Data Protection Regulation (GDPR), including the rights afforded to individuals by the Act. It specifically includes the right of access to personal information held by the CCG and extends to include the Access to Health Records Act 1990 which details how deceased person's records may be accessed. This policy has been reviewed against the new requirements of GDPR.

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is either justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.					
	What key impact have you identified?			**For impact identified (either positive and or negative) give details below:**	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		
Race	☐	☒	☐		
Religion or belief	☐	☒	☐		
Sexual orientation	☐	☒	☐		
Gender reassignment	☐	☒	☐		
Pregnancy and maternity	☐	☒	☐		
Marriage and civil partnership (only eliminating discrimination)	☐	☒	☐		
Other relevant groups	☐	☒	☐		
HR Policies only: Part or Fixed term staff	☐	☒	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	Andrew Clayton, Head of Health Informatics	**Date of next Review:**	February 2022

Once completed, this form **must** be emailed to Alison Hague, Corporate Services Manager for sign off: Alison.hague@rotherhamccg.nhs.uk

Alison Hague signature:	