

---

# Subject Access Request Procedure

---

<b>Version:</b>	6.0
<b>Ratified by:</b>	NHS Bury Clinical Commissioning Group Information Governance Steering Group
<b>Date ratified:</b>	16 June 2022
<b>Name of originator /author (s):</b>	Information Governance Team
<b>Responsible Committee / individual:</b>	NHS Bury Clinical Commissioning Group Audit Committee
<b>Date issued:</b>	June 2022
<b>Review date:</b>	June 2023
<b>Target audience:</b>	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
<b>Equality Analysis Assessed:</b>	Yes

## Further information regarding this document

<b>Document name</b>	Subject Access Request Procedure CCG.GOV.022.5.0
<b>Category of Document in The Policy Schedule</b>	Governance
<b>Author(s) Contact(s) for further information about this document</b>	Information Governance Team
<b>This document should be read in conjunction with</b>	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Secure Transfers of Data Procedure.
<b>This document has been developed in consultation with</b>	NHS Bury CCG Information Governance Steering Group
<b>Published by</b>	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place Knowsley Street Bury BL9 0SN Tel: 0161 762 1500
<b>Copies of this document are available from</b>	CCG Corporate Office CCG website

## Version Control

<b>Version History:</b>		
<b>Version Number</b>	<b>Reviewing Committee / Officer</b>	<b>Date</b>
<b>1.0 = policy once reviewed</b>	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	10 <sup>th</sup> December 2014
<b>2.0 = policy once reviewed</b>	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	18 <sup>th</sup> November 2015
<b>2.1 = policy once reviewed</b>	GMSS IG Team	22 <sup>nd</sup> December 2017
<b>3.0 = policy once ratified</b>	NHS Bury Clinical Commissioning Group Information Governance Operational Group	30 <sup>th</sup> January 2018
<b>3.1 = policy once reviewed</b>	GMSS IG Team	25 <sup>th</sup> September 2018

<b>Version History:</b>		
<b>Version Number</b>	<b>Reviewing Committee / Officer</b>	<b>Date</b>
<b>4.0 = policy once ratified</b>	NHS Bury Clinical Commissioning Group Information Governance Operational Group	31 <sup>st</sup> October 2018
<b>4.1 = policy once reviewed</b>	IG Team	25 <sup>th</sup> May 2021
<b>5.0 = policy once ratified</b>	NHS Bury Clinical Commissioning Group Information Governance Steering Group	28 <sup>th</sup> May 2021
<b>5.1 = policy once reviewed</b>	IG Team	May 2022
<b>6.0 = policy once ratified</b>	NHS Bury Clinical Commissioning Group Information Governance Steering Group	16 June 2022

---

# Subject Access Request Procedure

---

## Table of Contents

1.	Introduction .....	5
2.	Definitions .....	6
3.	Roles and Responsibilities .....	6
4.	Recognising a Subject Access Request .....	7
5.	Rights of Access .....	8
6.	Exemptions .....	8
7.	Requests from Parties other than the Subject .....	10
8.	Subject Access Request Process.....	13
9.	Fees.....	15
10.	Accessibility .....	15
11.	Timescales for Disclosure .....	15
12.	Escalation / Complaints Procedure.....	16
13.	Training and Awareness.....	16
14.	Dissemination and Implementation .....	17
15.	Further Information.....	17
16.	Other relevant documents .....	17
	Appendix 1 - Request for Access to Personal Information Form .....	18
	Appendix 2 - Acceptable ID documents for Subject Access Requests .....	21
	Appendix 3 - Agreement to Disclosure of Records Form .....	23
	Appendix 4 Subject Access Request Process Flow Map .....	24

## 1. Introduction

- 1.1 The Data Protection Act 2018 / General Data Protection Regulation (UK GDPR), gives every living person (or their authorised representative) the right to apply for access to information held about them by an organisation irrespective of when it was compiled. Access to deceased patient's information is governed by the Access to Health Records Act 1990.
- 1.2 This procedure is designed to inform staff how requests for access to information about an individual are dealt with and how to respond to such requests. It explains the process by which patients, members of the public, staff, legal representatives and 3rd parties can request the information.
- 1.3 This procedure is designed to provide best practice in handling requests for information about an individual. Full implementation of this policy will enable NHS Bury Clinical Commissioning Group (hereafter referred to as the CCG) to:
  - Comply with legal obligations under the Data Protection Act 2018 / UK GDPR;
  - Increase levels of trust and confidence by being open with individuals about the information that is held about them;
  - Provide better 'customer care';
  - Improve transparency of CCG activities in line with public policy requirements;
  - Enable individuals to verify that information held about them is accurate.
- 1.4 Subject Access Requests (SARs) relating to the CCG will normally be for access to view and /or to request copies of the following types of records which the CCG process:
  - Case files held by the Continuing Health Care/Complex Care Team;
  - HR Records and other related HR documents for CCG staff held by the CCG or Greater Manchester Shared Services (GMSS) on behalf of the CCG;
  - Complaints / Incidents information held by the CCG;
  - Safeguarding Information held by the CCG Safeguarding Team (subject to limitations dependant on the circumstances of the SAR);
  - Other internal correspondence relating to a staff member under the Data Protection Act 2018 / UK GDPR as a subject access request.
- 1.5 A record can be computerised / electronic (including emails) and / or manual form (paper files). It may include such documentation as handwritten notes, letters to and from other professionals, reports, imaging records, printouts, photographs, DVD and sound recordings.
- 1.6 The CCG does not process original health records, but they may hold copies of these as part of a complaint or CHC folder. If requests for health records are made, the data subject will be asked to contact the Data Controller which will be either the GP Practice and / or a secondary care provider such as an NHS Trust.
- 1.7 It is important that all staff bear in mind when compiling records that the content could be requested under the Data Protection Act 2018 / UK GDPR as a subject access

request and ensure that records they create are written in a way that would be appropriate to disclose.

- 1.8 In line with legislation the CCG shall respond to SARs as soon as possible and no later than 30 days after verification of data subject. In exceptional circumstances, an extension of 60 days may be applied, on the basis of approval by the DPO and notification to the data subject within 30 days of verification. There is also no fee involved in the process (except in certain limited circumstances).

## 2. Definitions

2.1 The following definitions apply in this policy:

- **Information Commissioner**

2.2 The Information Commissioner's Office (ICO) is the UK's independent authority set up to promote access to official information and to protect personal information.

- **Data Controller**

2.3 Under the Data Protection Act 2018 / UK GDPR, the CCG is a data controller. That is, the organisation (or person) that determines the purposes for which, and the way, any personal data about individuals is processed.

- **Data Subject**

2.4 According to the Data Protection Act 2018 / UK GDPR, the data subject is a living individual (not an organisation) who is the subject of the personal data.

- **Subject Access Request**

2.5 Subject Access Request is the terminology used when a person requests access to their personal information that is held by any organisation.

## 3. Roles and Responsibilities

3.1 The following roles and responsibilities are applicable in this policy:

- **Chief Officer**

3.2 The Chief Officer has overall ultimate responsibility for implementation of the provisions of this policy and procedure.

- **Caldicott Guardian**

3.3 The Caldicott Guardian of the CCG is responsible for ensuring that the organisation is compliant with the confidentiality requirements of the Data Protection Act 2018 / UK GDPR.

- **Data Protection Officer (DPO)**

3.4 The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the UK GDPR and other data protection laws. They are required to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition, they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc). Responsibility for management of subject

access requests also lies with the DPO. They will ensure that the CCG meets its legal responsibilities and complies with internal and external governance requirements in processing applications for personal records.

- **Information Governance Support Officer**

The IG Support Officer will provide administrative support to the DPO, together forming the IG Team. This will include maintaining records of SARs, DPIAs, DSAs etc, overseeing the IG mailbox and servicing the Information Governance Steering Group.

- **The Information Governance Steering Group**

3.6 The Information Governance Steering Group is responsible for reviewing and approving this procedure and forwarding on to other relevant groups for information. The number of SARs managed will be reported to the IG Steering Group on a monthly basis.

- **Employees**

3.7 All employees, whether permanent, temporary or contract, will be made aware of this procedure and are required to adhere to the principles set out. They should be aware of how to access this procedure and to seek advice from their line manager or the IG team if required.

#### 4. **Recognising a Subject Access Request**

4.1 A Subject Access Request (SAR) is any request made by an individual or an individual's representative (see Rights of Access section) for information held by the CCG about that individual.

4.2 All SARs must be made in writing, however the data subject does not need to mention the Data Protection Act 2018 / UK GDPR legislation or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, when they are seeking access to personal records held about them, but their request should still be treated according to this policy.

4.3 A SAR can be made via any of, but not exclusively, the following methods:

- Email to [BUCCG.corporateoffice@nhs.net](mailto:BUCCG.corporateoffice@nhs.net);
- Fax;
- Post to Bury CCG Information Governance Subject Access Requests, 1 Knowsley Place, Knowsley Street, Bury, BL9 0SN;
- Social Media;
- Corporate Website via <https://www.buryccg.nhs.uk/we-are-here-to-help/publications-scheme-2/freedom-of-information/subject-access-request-sar/>.

4.4 Where the SAR request does not contain all the necessary information for it to be processed, a 'Request for Access to Personal Information', as set out at Appendix 1, should be provided to a data subject for them to submit a subject access request, however there is no legal requirement for this form to be completed where information is provided by other means.

- 4.5 SARs made online will and must be treated like any other SAR when they are received, however the CCG will not provide personal information or a response via social media channels.
- 4.6 Where a SAR is received into a department other than the corporate office, the request should be forwarded immediately to the Information Governance Team who will then co-ordinate the request and contact the Information Asset Owner to process the request.

## 5. Rights of Access

- 5.1 Under the Data Protection Act 2018 / UK GDPR, any living person who is the subject of personal information held and processed by the CCG, has a right of access to that information. This is a legal right, subject to given exemptions below. They also have the right to an explanation of any terms they may not understand (such as technical language or terminology) and the right to ask that any inaccurate information is corrected, and to request a copy of those corrections.
- 5.2 Subject access provides a right for the individual to see their own personal data as well as to request copies of these.
- 5.3 An individual does not have the right to access information recorded about someone else unless they are an authorised representative or have parental responsibility or are acting on behalf of a deceased person.
- 5.4 The CCG is not required to respond to requests for information unless it is provided with enough details to enable the location of information to be identified, and to satisfy itself as to the identity of the individual making the request.

## 6. Exemptions

- 6.1 The following exemptions apply in respect to this policy:
- **Disclosure might cause harm / Third Party Information**
- 6.2 Under the Data Protection (Subject Access Modification) Health Order 2000, the CCG has the right to deny patients access to all or part of their health records if one of the following conditions applies:
- If, in the opinion of the healthcare professional / Head of Service, access would disclose information likely to cause serious harm to the physical or mental health or condition of the patient or any other person (for example, a child in a child protection case);
  - If giving access would disclose information which identifies a third party (unless the individual concerned has given consent).
- 6.3 Those who make the disclosure decision (e.g. healthcare professionals / Head of Service) must carefully consider, and be prepared to justify, any decisions to disclose or withhold information. The Caldicott Guardian must be consulted.

An agreement to disclosure of records form is completed and authorised accordingly for further actions as required.

- 6.4 If information has been withheld, the CCG is free to advise applicants of the grounds on which the information has been withheld – but they are not obliged to do so. For example, the CCG may not wish to volunteer the fact that information has been withheld if they believe that such a disclosure would cause undue distress, or if it might jeopardise a child protection investigation.
- **Child Protection Concerns**
- 6.5 There may be situations in which access to all or part of a child’s health records can be refused – for example, where there are ongoing child protection issues, or where releasing information may put a child or young person at risk of harm. In these cases, advice must be sought from the appropriate managers and child protection professionals, as well as the Caldicott Guardian, before releasing any information.
- **Third party disclosure**
- 6.6 Where records contain information that relates to an identifiable third party, that information may not be released unless:
- The third party is a health professional who has compiled or contributed to a health record, or who has been involved in the care of the individual;
  - The third party, who is not a health professional, gives their written consent to the disclosure of that information;
  - It is reasonable to dispense with the third party’s consent (considering the duty of confidentiality owed to the other individual, any steps taken to seek their consent, whether they are capable of giving consent and whether consent has been expressly refused).
- **Repeat of Earlier Request/Manifestly Unfounded**
- 6.7 Where requests are manifestly unfounded or excessive, because they are repetitive, consideration will be given to:
- charging a reasonable fee considering the administrative costs of providing the information; or
  - refusing to respond.
- 6.8 Where the decision is taken by the IG Team to refuse to respond to a request, an explanation must be provided to the individual, explaining the reason for the decision and informing them of their right to complain to the supervisory authority (Information Commissioner’s Office) and to a judicial remedy without undue delay and at the latest within one month.
- **Information relating to the deceased**
- 6.9 Applications for access to health records of the deceased are made under the Access to Health Records Act 1990.
- 6.10 Health records relating to deceased people do not carry a common law duty of confidentiality. Please note that the CCG would not process these. However, it is the policy of the Department of Health and the General Medical Council (GMC) that records relating to the deceased people should be treated with the same level of confidentiality as those relating to living people. For example, if the record contains a note made at the patient’s request that they did not want an individual to know the details of their illness or their care, then no access should be granted to that individual. The CCG will apply this policy to information requested under Access to Health Records Act 1990.

- 6.11 Records made after 1st November 1991 can be made available to a patient representative, executor or administrator. Any person with a claim arising from the death of a patient has a right of access to information specifically relating to the claim.
- 6.12 The person making the request must explain why they need access to the records and which part of the record supports their claim.
- 6.13 The request should normally be made to the last known record holder, unless there are extenuating circumstances, such as concerns over the treatment the deceased person received. In such cases, advice must be sought from the Caldicott Guardian.
- 6.14 The record holder has the right to deny or restrict access if it felt that disclosure would cause serious harm to the physical or mental health of any other person or would identify a third person.
- 6.15 If access to deceased patient records is requested this would only apply to the Continuing Health Care Team / Safeguarding Teams or any other service in the CCG providing “direct patient care”.
- 6.16 Requests for deceased patients GP records must be transferred to the Primary Care Support Service (<http://www.pcass.nhs.uk/>).

- **Dealing with Joint Records**

- 6.17 Where joint records are held, the relevant organisations must be informed of the access request and agree who will lead the disclosure process. However, requests for joint records should not have to be made to both organisations. Either organisation can provide the information requested provided the applicant is informed that the information is jointly held.
- 6.18 The term ‘joint records’ does not include records that contain information provided by one organisation to the other. While the information held by each organisation might be similar, they cannot be considered as joint records. In such cases a separate application must be made to each authority.

## **7. Requests from Parties other than the Subject**

- 7.1 The following can make requests in line with this policy:

- **Requests for Access to Records Made by a Patient Representative.**

- 7.2 Any person can authorise a representative to access information held about them on their behalf. This must be done in writing, with confirmation of the representative’s identity and relationship to the patient.
- 7.3 Representatives able to provide evidence that they are acting under a Power of Attorney or a Court of Protection Order will be granted access to information held about an individual.
- 7.4 Where an individual who is physically or mentally disabled and unable to provide written consent for a representative to seek access on their behalf, the CCG will give

the individual as much assistance as possible, in order to ascertain whether consent has been granted by other means to the representative.

- **Request for access by other organisations**

- 7.5 Various external organisations and agencies may request information held about an individual. In almost all cases, staff must not share any information unless they have consent from the individual. Advice should be sought from the IG Team. Examples of requests from other agencies are listed below:
- **Solicitors**
- 7.6 Solicitors may apply to see information held about their client, but informed, explicit and signed consent must first have been obtained from the individual before a copy of the information is released. The solicitor should be given access only to the information and explanation that would otherwise have been made available to the individual, subject to the restrictions stated above.
- **Court Order/Police**
- 7.7 A Court may order disclosure information (e.g. under the Civil Procedure Rules, the Data Protection Act 2018) and, unlike a request from a solicitor, a Court Order should be obeyed unless there is a robust justification to challenge it, in which case the CCG may challenge the order through the Court. The Court's decision is law unless the CCG decides to appeal the order and take the case to a higher Court to override the Court's decision.
- 7.8 Courts and Coroners are entitled to request original records. If they do, copies of the record must be retained by the CCG. Coroners normally give enough notice for copies to be made but have the power to seize records at short notice, which may leave little or no time to take copies.
- 7.9 All Court Orders, or documents appertaining to or alluding to be a Court Order, should be notified to the DPO and Caldicott Guardian.
- 7.10 Article 11 of the Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the prevention or detection of crime and the apprehension or prosecution of offenders. Any request by the Police for access to information held about an individual must be accompanied by the relevant consent form from the Chief Superintendent of the requesting Police Force.
- 7.11 The Crime and Disorder Act 1998 also allows (but does not require) the CCG to disclose information to the Police, local authority, probation service, or health authority for the purposes of preventing crime and disorder. For the CCG to consider releasing any information without consent, the access request must relate to a serious crime in line with the Crime and Disorder Act 1998 (for example, murder or rape), otherwise the Police should be asked to obtain a Court Order or written approved signed consent (see above regarding Court Orders).
- 7.12 All such requests from the Police should be in writing and forwarded immediately to the DPO and notified to the Caldicott Guardian.
- **Department of Work and Pensions**
- 7.13 Article 11 of the Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the assessment or collection of any tax or duty. Any

request by the Department of Work and Pensions for access to any information held about an individual must be accompanied by the relevant form.

- 7.14 The individual should be asked (if possible) for their informed, explicit and signed consent to disclose the information, unless this would prejudice the enquiry or court case.
- **Research Organisations**
- 7.15 Although research is considered an important factor in improving healthcare, the Information Commissioner does not consider it an essential element in the provision of healthcare.
- 7.16 If personal identifiable or pseudonymised information is required, informed, explicit and signed consent must be obtained. Service users are generally aware and supportive of research, but it is not reasonable to assume that they are aware of, or likely to consent to each research subject or proposal.
- 7.17 If it is enough for the purposes of the research to use anonymised data, consent is not required, but patients should be informed by posters and/or leaflets how their information may be shared.
- **Parental Responsibility**
- 7.18 Parental responsibility is defined in the Children Act 1989 as ‘all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his/her property’.
- 7.19 Parents, or those with parental responsibility, will generally have the right to apply for access to information held about a child, although disclosure may be refused if the child is deemed competent as per the ‘Gillick competencies’ and refuses to give consent.
- 7.20 Married parents both have parental responsibility unless a Court Order has removed that status from any party. A separated or divorced parent who no longer lives with the child has parental responsibility unless a Court has removed that status from either party.
- 7.21 Parental responsibility endures if the child is in care or custody. It is lost, however, if the child is adopted.
- 7.22 If the parents are not married, only the mother automatically has parental responsibility. The father may acquire it in the following ways:
- Registering the birth, along with the mother, as the child’s father (for children born after 1st December 2003);
  - Formal agreement with the mother (Section 4 of the Children Act 1989) – agreement can then only be ended by a Court;
  - Marrying the mother;
  - Obtaining a court order; or
  - Obtaining a residence order.
- 7.24 Parental responsibility can also be acquired:
- Through an appointment as the child’s guardian;

- By way of a residence order from the Court; or
- By anyone having an Adoption Order made in their favour.

7.25 Through Section 2(9) Children Act 1989 – “A person who has parental responsibility for a child may not surrender or transfer any part of that responsibility to another but may arrange for some or all of it to be met by one or more persons acting on his behalf”.

7.26 A Local Authority can acquire parental responsibility by:

- Emergency protection (local authority); or
- Interim or Full Care orders (local authority).

7.27 In this case the parents do not lose parental responsibility, but the local authority can limit the extent to which a person exercises their parental responsibility.

7.28 Where, in the view of a health professional, the child is not capable of understanding the application for access to records, the CCG is entitled to deny access as being against their best interests.

7.29 Legally, young people aged 16 and 17 are regarded to be adults for the purposes of consent to treatment and the right to confidentiality. As such, if a person of this age wishes any information about them to be treated as confidential this wish should be respected and they have the right to deny parental access to information held about them.

- **Individuals living abroad**

7.30 A request for access to information held about an individual made from outside the UK will be treated in the same way as a request made from within the UK. People living outside of the UK have the same rights of access to information an organisation holds about them as UK residents do.

## **8. Subject Access Request Process**

8.1 The IG Team will follow the procedure below and as set out at Appendix 4 in respect of processing the SAR and will liaise with the relevant Information Asset Owners / Manager and Heads of Service to ensure all SARs are processed in line with legislative timeframes.

8.2 Where the CCG does not hold the information directly, for example where the information is held by a service that is commissioned by the CCG from Greater Manchester Shared Services (GMSS), for example HR, the IG Team will liaise with the service providers IG Lead.

- **Receipt of Request**

8.3 Requests for information held about an individual should be directed to the CCG IG Team. The IG Support Officer will acknowledge the request and log it on the relevant Subject Access Request register. They will then notify the data subject of the next steps

- **Confirmation of identity / further clarification**

8.4 The IG Team need to be satisfied they know the identity of the data subject and should not request more information if the identity of the person is known to them. Where ID is required the data subject must provide 2 forms of ID; a photo ID e.g. passport / driver's license and a utility bill. Appendix 2 sets out a full list of ID that may be provided. ID can be photocopied and posted to the CCG or it can be scanned and emailed to the CCG.

8.5 Where the request relates to a staff member, in the first instance the IG Support Officer will check with a staff member's line manager that the staff member who makes the request is who they say they are. If this can be confirmed, then they do not need to collate two forms of ID. The IG Support Officer will also check if there are any other circumstances which they need to be aware of pertaining to the request.

- **Forms**

8.6 The request for information must include enough detail to locate the relevant information. The data subject may therefore be asked to complete a form to better enable the CCG to locate the relevant information. The IG Support Officer will forward the relevant form to the data subject, see Appendix 1, however while the CCG may ask for a form to be completed in order to assist with internal processes, this cannot be insisted upon and failure to complete a form cannot stall the 1 month response timeframe.

- **Confirmation**

8.7 Once the relevant ID has been received and details relating to the information requested is advised, the IG Support Officer will confirm this to the data subject and notify them that their request will be responded to within one month. The period begins from the date that the ID is received. The data subject will be informed if there will be any deviation from the one month timeframe, however, such deviation should be an exception and be escalated to the DPO and Caldicott Guardian prior to informing the data subject.

- **Collating**

8.8 The IG Support Officer will contact the relevant departments and ask if any information about the data subject, or other individual if the data subject is a third party, is held by them. This may involve an initial meeting with the department to go through the request if required. The department will be provided with a deadline to respond back to the IG Team either with the information requested or to state they do not hold any. A further meeting may need to be arranged to review and check the information. This review checks if any of the information is subject to an exemption and / or if consent is required from any third party. The department will be required to complete the Agreement to Disclosure of Records Form (Appendix 3) to ensure they have provided all the information requested and return this to the IG Support Officer with the information to be disclosed.

8.9 The information must be collated, reviewed and returned to the IG Lead by the given deadline to ensure the one month timeframe is not breached.

- **Refusing a request**

8.10 Where a decision has been made to refuse the Subject Access Request, the DPO will prepare a letter to inform the data subject of this decision and the basis for this. Under

UK GDPR, grounds for refusing to process a Subject Access Request are if the request is manifestly unfounded or excessive.

- **Response**

8.11 The finalised response will be collated together with the information retrieved from the department(s) or a statement that the CCG does not hold the information requested. A written response will be sent back to the data subject. The IG Support Officer will check how the data subject would like the information, for example if they prefer the transfer to be done electronically then the IG Support Officer should ensure they send it via this format.

- **Logging and Closure**

8.12 After the response has been sent to the data subject the SAR will be considered closed and the log will be updated accordingly by the IG Support Officer.

- **Monitoring and Reporting**

8.13 The DPO will routinely monitor the requests received and compliance with statutory timeframes, providing monthly updates to the CCG's Information Governance Steering Group which will also reflect any issues relating to processing SARs such as difficulty obtaining information, internal reviews and complaints.

## **9. Fees**

9.1 Under the Data Protection Act 2018 / UK GDPR, information must normally be provided free of charge. A fee may be made if the request is 'manifestly unfounded or excessive.' There may be a reasonable charge for further copies.

## **10. Accessibility**

10.1 Every effort will be made to provide the data subject with information in an accessible format. Requests for information in large print, translated or audio format will be considered on a case by case basis, and may not necessarily be met. However, the CCG will help individuals to understand information where possible.

10.2 The Data Protection Act 2018 / UK GDPR requires that information is provided in an 'intelligible form'. The CCG is not required to translate information or decipher poorly handwritten notes, but best practice would be to help individuals where there are barriers to understanding the information.

10.3 If information is coded, and it is not possible for people outside of the organisation to understand the coded information, the CCG is required to provide access to the code.

## **11. Timescales for Disclosure**

11.1 The CCG will respond to requests for access to information held about an individual within one month.

- 11.2 If the application does not include enough information to identify the person making the request, or to locate the information, that information should be sought promptly, and the one month period begins when it is supplied.

## **12. Escalation / Complaints Procedure**

- 12.1 If an individual or their representative is not satisfied with the outcome of their request, for example, if they feel information has been withheld or recorded incorrectly, or that they have not been allowed sufficient time to view the information, they will be informed of the options available to them in the final response sent to the data subject to enable them to take further action.
- 12.2 In the first instance, the individual should be encouraged to attend an informal meeting with a view to addressing and resolving the issues locally with the relevant service lead and DPO, however other options include escalating the matter to the CCG's Caldicott Guardian, escalating the matter to the Information Commissioner's Office, and seeking independent legal advice.
- 12.5 If the matter is not resolved, an individual can escalate their concerns to the Information Commissioners Office (ICO) using the following contact details

The Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
Tel: 01625 545 745  
E-mail: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

- 12.6 In all cases, wherever possible, local resolution should be sought, however, the individual has the right to pursue any of these channels at any time and may wish to pursue several actions simultaneously.

## **13. Training and Awareness**

- 13.1 All staff will be made aware of the Subject Access Request procedure and the requirements of the CCG to respond within the statutory timeframe.
- 13.2 Specific training, as set out in the approved Training Needs Analysis, will be provided to staff who are identified as holding information that could be subject to a Subject Access Request. This includes the following:
- Safeguarding
  - Continuing Healthcare
  - Incidents / Complaints (Patient Services Team)

## **14. Dissemination and Implementation**

- 14.1 **Dissemination** - The procedure will be disseminated to all departments, accessed through the internal shared drive and published on the CCG website.
- 14.2 **Implementation** - All CCG staff will be made aware of this procedure through generic and specific training programmes and guidance materials, which will be regularly reviewed and updated.

## **15. Further Information**

- 15.1 Further information or advice on the content or application of this policy is available from:
- The IG Team - [BUCCG.ig@nhs.net](mailto:BUCCG.ig@nhs.net)
  - The Caldicott Guardian for Bury CCG - [w.blandamer@bury.gov.uk](mailto:w.blandamer@bury.gov.uk)

## **16 Other relevant documents**

- 16.1 This procedure should be read in conjunction with the following Bury CCG Policies:
- Information Governance Framework;
  - Data Protection and Confidentiality Policy;
  - Records Management Policy;
  - Secure Transfers of Data Procedure; and
  - Individual Rights Procedure.

## Appendix 1 - Request for Access to Personal Information Form

Under the Data Protection Act 2018 / UK GDPR, you have the right to request to any personal information we, as an organisation, may hold about you. This is known as a Subject Access Request. (A Subject is an individual who is the subject of personal data).

Please complete this form and return it to:

**Post:** NHS Bury CCG, Information Governance – Subject Access Request, 1 Knowsley Place, Knowsley Street, Bury, BL9 0SN

**Email:** [BUCCG.ig@nhs.net](mailto:BUCCG.ig@nhs.net) - Please ensure you write "Subject Access Request" in the subject field of the email.

1.	Applicant's Full Name	.....
2.	Applicant's Date of Birth	.....
3.	Applicant's Current Address	..... ..... .....
4.	Applicant's Previous Address (if applicable)	..... ..... .....
5.	Applicant's Telephone Number:	
	Home Telephone No:.....	
	Mobile Telephone No:.....	

6. The information requested is about me.

Yes  No

If **Yes**, please go to Question 8

7. The Applicant (whose data is being requested) must give permission for the information to be released to their representative.

I give my permission for..... to request access to my personal information as described in question 8 (below) of this form.

Signature of Data Subject.....

Print Name:.....

Name of representative and address where information is to be sent:

.....  
.....  
.....  
.....

8. To help us search for the information you require, please tell us the about the information you require with as much detail as possible. For example, copies of personnel file between (date) and (date). If we do not receive enough information, we may be unable to process your request.

.....  
.....  
.....  
.....  
.....  
.....  
.....

9. I confirm that I am the Data Subject

Signed: .....

Print Name:.....

Date:.....

I enclose a photocopy of 2 of the following items as proof of identity (one to be a photographic copy).

Please indicate on the attached Appendix 2, Acceptable ID Documents for Subject Access Requests which 2 forms of identity have been enclosed.

10. I confirm that I am the representative

Signed:.....

Print Name: .....

Date: .....

We will make every effort to process your Subject Access Request as quickly as possible within the one month time limit. This time limit begins after the verification of the data subject.

However, if you have any queries whilst your request is being processed, please do not hesitate to contact the CCG IG Team at Bury CCG using the contact details above.

## Appendix 2 - Acceptable ID documents for Subject Access Requests

To make a Subject Access Request for yourself, you will be asked to provide two forms of ID documentation, one being proof of identity and one to confirm your address, before any information will be released.

All forms of acceptable documentation are listed in the tables below. Please note, ONE document from each of the tables below should be provided (please send copies not originals):

**Please tick against the documents you have provided.**

PROOF OF IDENTITY	
Acceptable Photo Personal Identity Documents	
	Current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passports
	Passports of non-EU nationals containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK *
	Current UK (or EU/other nationalities) Photo-card Driving Licence (providing that the person checking is confident that non-UK Photo-card Driving Licences are genuine)
	A national ID card and/or other valid documentation relating to immigration status and permission to work*
<i>Any documents not listed above are not acceptable forms of photographic identification e.g. organisational ID card.</i>	
Acceptable Non-Photo Personal Identity Documents	
	Full UK Birth Certificate – issued within 6 weeks of birth
	Current Full Driving Licence (old version); (Provisional Driving Licences are not acceptable)
	Residence permit issued by Home Office to EU Nationals on inspection of own-country passport
	Adoption Certificate
	Marriage/Civil Partnership certificate
	Divorce or annulment papers
	Police registration document
	Certificate of employment in HM Forces
	Current benefit book or card or original notification letter from the Department of Work and Pension (DWP) confirming legal right to benefit
	Most recent HM Revenue and Customs (previously Inland Revenue) tax notification
	Current firearms certificate
	Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
	GV3 form issued to people who want to travel in the UK without valid travel documents
	Home Office letter IS KOS EX or KOS EX2
	Building industry sub-contractors certificate issued by HM Revenues and Customs (previously Inland Revenue)

CONFIRMATION OF ADDRESS	
To confirm the address, the following documents are acceptable:	
	Recent utility bill or certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible*
	Local authority tax bill (valid for current year) *
	Current UK photo-card driving licence (if not already presented as a personal ID document)
	Current Full UK driving licence (old version) (if not already presented as a personal ID document)
	Bank, building society or credit union statement or passbook containing current address
	Most recent mortgage statement from a recognised lender*
	Current local council rent card or tenancy agreement
	Current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit
	Confirmation from an electoral register search that a person of that name lives at the claimed address*
	Court Order*

***\* The date on these documents should be within the last 6 months (unless there is a good reason for it not to be e.g. clear evidence that the person was not living in the UK for 6 months or more) and they must contain the name and address of the applicant***

## Appendix 3 - Agreement to Disclosure of Records Form

This form is for internal use only.

A fully completed form and documents to be released in response to the SAR must be sent to the CCG IG Team . **Documents must not be released directly to the applicant**

1.	Applicant's Full Name
2.	Applicant's Date of Birth
3.	Applicant's Current Address

<b>AUTHORISER'S DECLARATION – Please tick relevant box or boxes</b>	
1. I agree to the attached records being released to the above-named person or the person's named representative	<input type="checkbox"/>
2. Part or whole of the records have been withheld on the grounds that:	<input type="checkbox"/>
a. Disclosure is likely to cause serious harm to the physical or mental health of the person or of another individual	<input type="checkbox"/>
b. Access would disclose information relating to, or provided by, a third party who has not consented to their information being disclosed	<input type="checkbox"/>
c. The record contains information the person expressly stated must not be released	<input type="checkbox"/>
d. The person is under 16 and I do not think he / she fully understands what an application to see their records means	<input type="checkbox"/>
Staff Name: .....	
Post held: .....	
Signature: .....	
Date: .....	

# Appendix 4 Subject Access Request Process Flow Map

