Bolton Clinical Commissioning Group

Right of Access / Subject Access Requests Procedure

Policy Number	**IG013**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**July 2019**
Last Review Date	**June 2019**
Next Review Date	**June 2021**
Policy Author	**IG Team**
Version Number	**6.1**

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	Diane Sankey/Mike Robinson	Escalated to CCG Exec for Approval
1	October 2013	Executive Committee	Approved – review two years
2	January 2015	Diane Sankey	Minor amendments to job titles/depts./CSU Name
3	November 2016	IG Team	Minor amendments
4	July 2018	IG Team	Reviewed document in line with GDPR changes
4.1	August 2018	IG Board	Approved
5	September 2018	CCG Chief Officer	Approved
5.1	June 2019	IG Team	Further amendments in line with GDPR
6.0	June 2019	IG Board	Approved
6.1	July 2019	CCG Chief Officer	Approved

Analysis of Effect completed:	By: Mike Robinson	Date: 30 Sept 2013

Contents Page

1 Introduction

Objective

The objective of this procedure is to provide staff across Bolton Clinical Commissioning Group (henceforth referred to as "the CCG") with a clear guide on how to manage incoming Right of Access / Subject Access Records requests which could be for full or partial access to health records and non-health records.

Background

The Data Protection Act 1998, which became effective from the 1st March 2000, has been reviewed and updated under General Data Protection Regulations (GDPR) and the Data Protection Act 2018. As previous, this legislation 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 (Article 15 of the GDPR). These were referred to as Subject Access Requests.

Under GDPR Subject Access Requests are also known as the Right of Access to Information. This procedure will use the terminology 'Right of Access.'

Access to deceased patient's information is governed by the Access to Health Records Act 1990.

A record can be computerised (electronic) and / or manual form (paper files). It may include such documentation as hand written notes, letters to and from other professionals, reports, imaging records, printouts, photographs, DVD and sound recordings.

Right of Access requests 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. These are:

- Case files held by the Continuing Health Care / Funded Care Team
- HR Records and other related HR documents for CCG staff held by the CCG
- PALS (Patient Advice and Liaison Service) / Complaints / Incidents information held by the CCG
- Safeguarding Information held by the CCG Safeguarding Team
- Internal correspondence about a staff member.

The CCG do not process original health records but they may hold copies of these as part of a complaint / CHC folder. If requests for Health Records are made, the requester 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.

It is important that all staff bear in mind when compiling records that the content could be requested under the Data Protection Act 2018 / GDPR as a Right of Access Request, and ensure that records they create are written in a way that would be appropriate to disclose.

This procedure informs staff how requests for access to information about an individual are dealt with and how CCG 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.

This procedure is designed to provide a guide to best practice in handling requests but guidance should be sought from the Information Governance (IG) Team. Full implementation of this procedure will enable the organisation to:

- Comply with legal obligations under the Data Protection Act 2018 / 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 organisational activities in line with public policy requirements
- Enable individuals to verify information help about them is accurate

2 Definitions

General Data Protection Regulation 2016 (GDPR) - This is a European Union (EU) legislation that became directly applicable in member states (e.g. the UK) on the 25th May 2018. The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

The Data Protection Act 2018 – The updated Data Protection Act enacted on the 23rd May 2018, sits alongside GDPR and fills gaps regarding data processing where flexibility and derogations are permitted. It also states the legislation on processing for law enforcement purposes, the intelligence services, and outlines the functions of the Information Commissioner's Office (ICO) which is the UK's supervisory authority.

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

Personal Data - This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special Category Data - This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

For more information about special categories of data please refer to the ICO guide at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Personal Confidential Data - This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

One calendar month - This is calculated from the day a request is received (whether it is a working day or not) until the corresponding calendar date in the next month. For example - If a request is received a request on 31st March the time limit will start from the same day. As there is no equivalent date in April the date for compliance is the 30th April. If the 30th April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply with a request.

Processing – This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller - Under the Data Protection Act 2018 / GDPR, the CCG is a Data Controller. That is, the organisation (or person) that determines the purposes for which and the manner in which any personal data about individuals are processed. Data Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Data Processor – Processors act on behalf of, and only on the instructions of, the relevant controller.

Data Subject

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

Right of Access Request

Right of Access Request is the terminology used when a person requests access to their personal information that is held by any organisation. They may still be referred to as Subject Access Requests.

3 Roles and Responsibilities

Chief Operating Officer

The Chief Operating Officer has ultimate responsibility for the implementation of the provisions of this Procedure. As the Accountable Officer, they are responsible for the management of the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

Data Protection Officer (DPO)

The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; advise on what training staff may require and conduct internal audits.

Caldicott Guardian

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

Right of Access Lead

The IG Manager will manage Right of Access Requests and is responsible for ensuring that Bolton CCG meets its legal responsibilities and complies with internal and external governance requirements in processing applications for personal records and that a record of all Right of Access Requests is maintained.

Employees

All staff have a duty to familiarise themselves with this procedure and comply with the processes, timescales and confidentiality requirement that support this procedure. They should be aware of how to access this procedure and to seek advice from their line manager or the Right of Access Request Lead or the Information Governance (IG) Team if required.

Information Governance Board

Information Governance (IG) Board is responsible for reviewing and approving this procedure and forwarding onto other relevant groups for information. The number of requests managed will be reported to the IG Board on a monthly basis.

4 Recognising a Right of Access Request

A Right of Access Request is a request made by an individual or an individual's representative (see Right of Access section) for information held by the CCG about that individual.

A request does not need to be made in writing and the requestor does not need to mention the Data Protection Act 2018 / GDPR legislation or state that they are making a 'Right of Access Request' for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, but their request should still be treated according to this policy.

The CCG have created a form called "Request for Access to Personal Information Form" which can be provided to a requestor, should the requestor ask to submit their request via a form. A copy of this can be found in the Appendix 1. Please note they do not have to complete this form.

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

- Email
- Fax
- Post
- Social Media
- Corporate Website

Requests made online must be treated like any other Right of Access request when they are received, however, the CCG will not provide personal information via social media channels.

Requests should be identified and forwarded immediately to the IG Manager (who is the Right of Access Lead), who will then co-ordinate the request and contact the Information Asset Owner to process the request.~~,~~

St Peters House,
Silverwell Street,
Bolton
BL1 1PP

Or

Email: bolccg.quality-team@nhs.net

5 Right of Access

Under the Data Protection Act 2018 and 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.

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, have parental responsibility, or are acting on behalf of a deceased person.

The table below outlines the request process which includes fee information, identity checks and when requests are made on behalf of another individual.

Right of Access – Article 15	
How can the request be made?	A request can be made verbally or in writing to any part of the organisation and it does not have to state it is a subject access request or refer to Article 15 of the GDPR as long as the individual is requesting access to their own personal data. If the request is made verbally (for example, via the telephone). The CCG recommend that such a request is confirmed in writing in order to check the validity of the request and the identity of the requestor (or their representative). (Recital 64 – GDPR). A written request also provides evidence to ensure that the CCG has all the relevant and necessary information to process the request accordingly. This can assist to prevent any delays / misunderstandings. If the request does not contain sufficient information or the requestor has asked for everything, you can ask them to narrow the scope down, for example a period of time or relating to a specific care episode (Recital 63 – GDPR). However, if the requestor is insistent with their full request this must be processed unless you can apply an exemption to this.
Confirm or deny processing	An individual has the right to obtain confirmation from the CCG as to whether or not the CCG are processing their personal data. If this is confirmed the requestor can make a request to access information should they wish to do so.
What is the timescale for complying with a request?	The timescale is one calendar month. This is calculated from the day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.
Can the timescale be extended?	This can be extended by a further two months if the request is complex or if a number of requests have been received from the individual.

	The individual must be informed within one month of receipt of their request with an explanation as to why the extension is necessary. It is good practice to have regular communications with the requestor to keep them updated.
Can a fee be charged?	No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged this fee must be justified.
Can ID be requested?	Yes if you require clarification of identity. This must be requested as soon as possible and sufficient information must be provided by the requestor to enable you to confirm the requestor's identity and also where a representative is submitting a request, the consent or legal justification for this. Please see Appendix 2 for information regarding appropriate documentation to verify identity. The period for responding to the request begins when you receive the additional information.
Can a third party make a request?	Yes, a request for information can be made via a third party. This could be a solicitor acting on behalf of a client or an individual who feels more comfortable allowing someone else to act for them. If a third party is making the request you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. A written authority, general power of attorney, or court order must be requested.
Requests where an individual lacks mental capacity	There are no specific provisions within GDPR but the Mental Capacity Act 2005 enables a third party to exercise the right of access on behalf of such an individual. You require proof that they can do this.
Requests for access to children's data	Where a child is competent, they are entitled to request access to their record. Children aged over 16 years are presumed to be competent. Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to request access to their information. However, children who are aged 12 or over are generally expected to have the competence to give or withhold their

	consent to the release of information from their health records. When assessing a child's competence, it is important to explain the issues in a way that is suitable for their age. It is important to seek the advice from the Caldicott Guardian, medical professionals and the Data Protection Officer (DPO) in such cases. Where, in the view of the appropriate health professional, a child lacks competency to understand the nature of the right to request access, the holder of the record is entitled to refuse to comply with the right of access request. Where a child is considered capable of making decisions about access to his or her medical record, the consent of the child must be sought before a parent or other third party can request access.
Actions required if a request is refused.	If it is decided to refuse or reject a right of access request, the individual must be informed without undue delay and within one month of receipt of the request. The individual must be informed of the reason for refusal and their right to make a complaint to the Information Commissioners Office (ICO). They can also if required enforce this right through a judicial remedy.

Recital 59 and 63 of the GDPR states that organisations 'provide means for requests to be made electronically, especially where personal data are processed by electronic means'. *A right of access request facility (online form) that allows individuals to make their request in an electronic format to the CCG (if they wish to do so) is available via the CCG website.*

It must be noted that an application form is not compulsory and it must not be used to extend the time limit for processing.

Article 15 also states than an individual must also be provided with information about data processing activities within the CCG when responding to a Right of Access request. This information is outlined in the CCG's Privacy Notice. **Therefore, a copy of the privacy notice must be provided with the information requested back to the individual requesting it.** This includes information about data processing activities by the CCG as required by GDPR.

If an individual makes a request electronically, the information is to be provided in a commonly used electronic format, unless the individual specifically requests otherwise. For example, if an individual requests that information is provided to them in hard copy and posted out to them, the CCG must honour this request.

GDPR also recommends that where possible, provision for remote access to a secure self-service system to provide an individual with direct access to his or her information (Recital 63). For the CCG, this doesn't apply at the moment as records are not stored in such a way. However for a GP practice, patient online access to the medical records offers this solution.

6 Exemptions

Disclosure might cause harm / Third Party Information

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 condition applies:

- If, in the opinion of the healthcare professional in charge of the patient's care, 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)

Those who make the disclosure decision (e.g. healthcare professionals) must carefully consider, and be prepared to justify, any decisions to disclose or withhold information. The CCG Caldicott Guardian / Data Protection Officer (DPO) must be advised and make the final decision if there appears to be any grounds for withholding information.

Disclosure decisions must be documented (on the Right of Access Logbook). This is important when disclosure is prevented in order to justify the decisions to withhold information.

If information has been withheld, the CCG is free to advise applicants of the grounds on which 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 / Safeguarding Concerns

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 / DPO, before releasing any information.

Third Party Disclosure

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 (taking into account the duty of confidentiality owed to the other individual, any steps taken to seek his/her consent, whether he/she is capable of giving consent and whether consent has been expressly refused)

Repeat of Earlier Request / Manifestly Unfounded

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Information / records relating to the deceased

Applications relating to the deceased are not covered under the Data Protection Act 2018 or GDPR and are made under the Access to Health Records Act 1990.

Records made after 1st November 1991 can be made available to a patient representative, executor or administrator via the Access to Health Records Act 1990. Any person with a claim arising from the death of a patient has a right of access to information specifically relating to the claim.

The person making the request must explain why they need access to the records and too which part of the record supports their claim.

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 and DPO.

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 a particular individual to

know the details of their illness or their care, then no access should be granted to that individual.

In addition, 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.

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”.

Dealing with Joint Records

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.

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 made by Parties other than the Data Subject

Requests for Access to Records Made by a Patient Representative

Any person can authorise a representative to request access to information held about them on their behalf. This must be completed in writing, with confirmation of the representative’s identity and relationship to the patient.

Representatives able to provide evidence that they are acting under a Power of Attorney or a Court of Protection Order will be granted the right of request access to information held about an individual.

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 - 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 or where there is legal justification to disclose the information. Examples of requests from other agencies are listed below:

Solicitors

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 Orders

A Court may order disclosure information (e.g. under the Civil Procedure Rules, the Data Protection Act 2018). 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 in an attempt to override the Court's decision.

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 sufficient 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.

All Court Orders or documents appertaining to or alluding to be a Court Order should be forwarded immediately to CCG Right of Access Lead and where necessary advice will be sought from the Caldicott Guardian / DPO.

Requests made by the Police

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 of 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.

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.

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).

Any request by the police for access to information held about an individual must be accompanied by the relevant consent and official letter / form signed by Chief Superintendent of the requesting police force or equivalent.

The Right of Access Lead should be notified of any access requests by the police.

Department of Work and Pensions
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.

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
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.

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 and every research subject or proposal.

If it is sufficient 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 - 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'.

Those with parental responsibility have a statutory right to apply for access to their children's health records, although if the child is capable of giving consent, he or she must consent to the access.

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.

Parental responsibility endures if the child is in care or custody. It is lost, however, if the child is adopted.

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 brought to an end by a Court
- Marrying the mother
- Obtaining a court order
- Obtaining a residence order

In practice, parental responsibilities would include:

- Safeguarding a child's health, development and welfare
- Financially supporting the child
- Maintaining direct and regular contact with the child

Parental responsibility can also be acquired

- Through an appointment as the child's guardian
- By way of a residence order from the Court
- By anyone having an Adoption Order made in their favour

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".

A Local Authority can acquire parental responsibility by:

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

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.

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.

For online services only and where consent applies, under GDPR (in the UK) the age of consent for children is 13 and over.

For more detail regarding parental responsibility please refer to the BMA Guidance: https://www.bma.org.uk/advice/employment/ethics/children-and-young-people/parental-responsibility

For more detail re the Children's Act 1989 please refer to:
http://www.legislation.gov.uk/ukpga/1989/41/section/2

Individuals living abroad - 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 Right of Access Process

Appendix 3 provides a map of the process for dealing with Right of Access Requests.

Where the request is for information held by a service that is managed by the CCG, for example Continuing Healthcare, the following procedure should be followed:

- **Receipt of Request** - Requests for information held about an individual should be logged on the CCG's Incident Management System, these will be directed to the Right of Access Lead. The request will be acknowledged and logged on the Right of Access logbook.

  The 1 calendar month timeframe commences from the date the request is received.

- **Confirmation of identity / further clarification** – The Right of Access Lead needs to be satisfied they know the identity of the requestor and should not request a lot more information if the identity of the person is known to them. If there are any doubts about the identity of the person making the request more information can be requested. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.

  Where ID is required ideally the requestor should provide 2 forms; a photo ID e.g. passport / driver's license and a utility bill. See Appendix 2 for 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. If further information or ID is required from the requestor in order to process the request the timeframe can be stopped until the information is received. The time will re-commence once sufficient information has been received. The Right of Access logbook must be maintained and kept updated to evidence this.

- **Member of staff ID checks** – The Right of Access Lead needs to check the identity of anyone making a request to ensure information is only given to the person entitled to it. In the first instance, if in any doubt checks will be made with the staff member's line manager. If this can be confirmed then they do not need to present two forms of ID.

- **Forms** – The requestor may be asked to complete a form to better enable the CCG to locate the relevant information. The Right of Access Lead will forward the relevant form to the requestor, 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 calendar month response timeframe.

- **Confirmation** – Once the relevant ID has been received, the Right of Access Lead will confirm this to the requestor and notify them that their request will be responded to within a 1 calendar month. The period begins from the date that the ID is received / ID confirmed. The requestor will be informed if there will be any deviation from the 1 calendar month timeframe, however, such deviation should be an exception and be escalated to the Caldicott Guardian / DPO prior to informing the requestor.

- **Collating** – The Right of Access Lead will contact the relevant departments and Information Asset Owners (IAOs) and ask if any information about the requestor, or other individual if the requestor 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 Right of Access Lead 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 / redaction / and or if consent is required from any third party. The team will be expected to complete a Right of Access Disclosure Proforma (Appendix 4) to confirm what information has or has not been disclosed.

  If the request relates to patient data the request must be copied to the CCG Caldicott Guardian and DPO.

- **Refusing a request** – The Right of Access lead will draft a letter to respond back informing the data subject that the CCG have grounds of refusing a request. Under GDPR grounds for refusing to process a Right of Access Request are; if the request is manifestly unfounded or excessive.

- **Response** – 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.

  The response is sent back to the requestor in the format requested.

  The Right of Access Lead will check how the requestor would like the information, for example if they prefer the transfer to be done electronically the lead should ensure they send it via this format.

  If email is used, the information must be sent by NHS Mail. If NHSMail is not an option then the [Secure] method should be used which sends an encrypted email to a non-NHSMail account. Please refer to the Secure Transfers of Data Procedure which is located on the CCG's website for more information.

  If the method chosen is post, it should be sealed securely, marked private and confidential addressee only and sent by 'signed for' delivery.

- **Logging & Closure** – After the response has been sent to the requestor the request will be considered closed and the log will be updated accordingly by the CCG Right of Access Lead via the Safeguard system and logbook. All sent emails in personal folders are to be saved in a file on the network drive.

- **Monitoring and Reporting** – The CCG Right of Access will routinely monitor the requests and the CCG's IG Board will receive regular reports regarding the number of requests received and any issues relating to them, such as difficulty obtaining information, internal reviews and complaints.

9 Fees

Under the new Data Protection Act 2018 / 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

Every effort will be made to provide the requestor 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.

The Data Protection Act 2018 / GDPR require 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.

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

11 Timescales

The CCG will respond to requests for access to information held about an individual within 1 calendar month.

This is calculated from the day a request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

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

12 The Right to Lodge a Complaint

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 should be informed of the options available to them to take further action.

These options include meeting with the CCG, escalating the matter to the CCG's Data Protection Officer / IG Team on the following details:

Mike Robinson (CCG Associate Director of Governance and Safety / CCG DPO)
Email: Michael.robinson1@nhs.net

If the matter is not resolved, the requestor can then escalate the matter to the Information Commissioner's Office (ICO) at the details below, and may also seek independent legal advice.

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

Website - https://ico.org.uk/make-a-complaint/ for more information relating to making a complaint

Telephone: 0303 123 1133

13 Training and Awareness

Specific training will be provided to staff who are identified as holding information that could be subject to a Right of Access Request. Please refer to the CCG Data Security Training Needs Analysis for further detail.

14 Dissemination and Implementation

Dissemination

This procedure will be published on the CCG's website and awareness will be raised via staff newsletters.

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.

The IG Team will support staff in the process.

15 Further Information

Further information or advice on the content or application of this procedure is available from:

- bolccg.quality-team@nhs.net
- Information Governance Team
- The Information Commissioner's Office (see section 13 for full details)

16 Other relevant documents

This procedure should be read in conjunction with the following Bolton CCG Policies:

- IG001 Information Governance Policy
- IG002 Confidentiality and Data Protection Policy
- IG005 Records Management Policy
- IG012 Secure Transfer of Information Guidance
- IG019 Individual Rights Procedure

Further Information / Useful Links

- Information Commissioners Office (ICO)
  https://ico.org.uk/

- Information Governance Alliance (IGA)
  https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

- British Medical Association (BMA) – GDPR Guidance
  https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr

- The Data Protection Act 2018 (DPA 2018)
  https://www.gov.uk/government/collections/data-protection-act-2018

- The General Data Protection Regulation 2016 (GDPR)
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Appendix 1

Request for Access to Personal Information Form

Under the Data Protection Act 2018 / GDPR, you have the right to request to any personal information we may hold about you as an organisation. This is known as a 'Right of Access' Request (formerly called a Subject Access Request).

To help us be clear about your request please complete this form and send back to:

Post:

Right of Access Request
St Peters House
Silverwell Street
Bolton
BL1 1PP

Or

Email: bolccg.quality-team@nhs.net - please ensure your write 'Right of 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. 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 to process you request, we may be unable to process your request.

……

……

……

……

……

……..

……..

7. The information requested is about me?

Yes ☐ No

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.

Please tick on the attached form which 2 forms of identity have been enclosed.

If you require information to go to a representative then please give the name and address of the representative.

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

……

……

……

……

8. If you require a representative to access information on your behalf then please complete the below

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:

……

……

……

……

9. I confirm that I am the representative

Signed:……..

Print Name: ……

Date: ……..

We will make every effort to process your Right of Access Request as quickly as possible within the month time limit.

However if you have any queries whilst your request is being processed, please do not hesitate to contact the Right of Access Lead at the CCG.

Appendix 2 - ID Checklist

Acceptable ID documents for Right of Access Requests

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

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

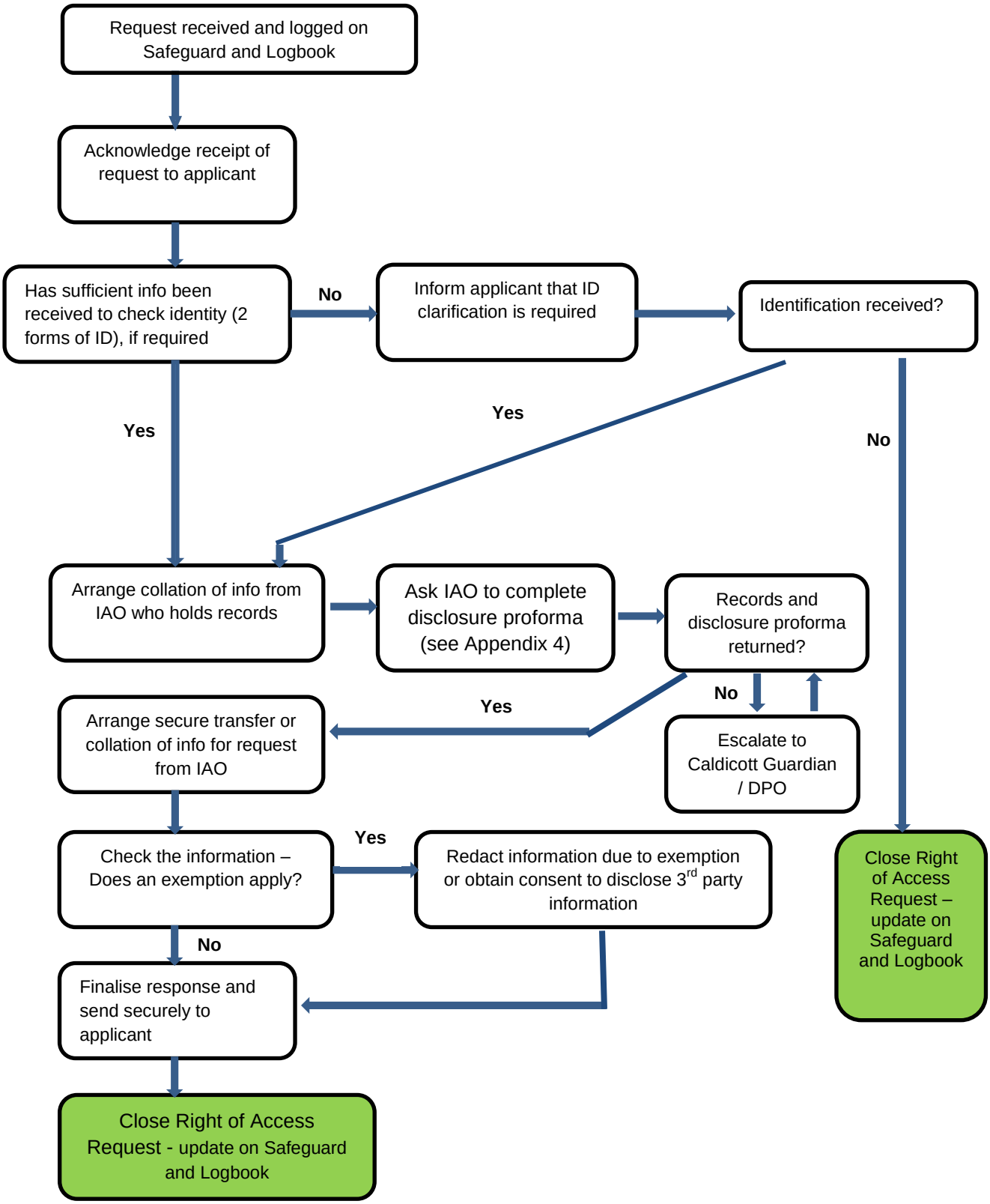
Please tick against the documents you have provided.

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*****
Any documents not listed above are not acceptable forms of photographic identification e.g. organisational ID card.	
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	
	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 – Right of Access Request Process Flow map



Appendix 4 – Right of Access Request Disclosure Proforma

1. Applicant's Full Name

   ……

2. Applicant's Date of Birth

   ……

3. Applicant's Current Address

   ……

   ……

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

Staff Name: ……..

Post held: ……

Signature: ……

Date: ……..