NHS
Bedfordshire, Luton and Milton Keynes
Integrated Care Board

Subject Access Requests
&
Access to Health Records Policy

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Bedfordshire, Luton & Milton Keynes Integrated Care Board website is the controlled copy
www.befordshirelutonandmiltonkeynes.icb.nhs.uk

Sustainable Development - Environmental

Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

Document Control	
Document Owner:	Senior Information Risk Owner
Document Author(s):	Information Governance Team
Directorate:	Medical Directorate
Approved By:	Operational Group
Date of Approval:	25-03-2024
Date of Next Review:	25-03-2026
Effective Date:	25-03-2024

Version Control			
Version	**Date**	**Reviewer(s)**	**Revision Description**
v1.0	01-07-2022	Head of Safe Practice & DPO	Added further information relating to children. Updated job role titles.
V2.0	25-03-2024		

Implementation Plan

Development and Consultation:	The following individuals were consulted and involved in the development of this document: ▪ Information Governance Team ▪ Information Governance Group
Dissemination:	Staff can access this document via the website and will be notified of new / revised versions via the staff briefing. This document will be included in the organisation's Publication Scheme in compliance with the Freedom of Information Act 2000.
Training:	The following training will be provided to make sure compliance with this document is understood. All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance. In addition to this, all staff are required to annually complete and pass the NHS Digital's Data Security Awareness Level 1 module on the Electronic Staff Record (ESR) e-Learning portal. ▪ Please also refer to the Training Needs Analysis (TNA) section of this policy.
Monitoring:	Monitoring and compliance of this document will be carried out as below: An assessment of compliance with assertions which make up the Data Security and Protection Toolkit, will be undertaken each year and audited by internal auditors. ▪ In addition the Information Governance Team will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice.
Review:	The Document Owner will ensure this document is reviewed in accordance with the review date on page 2.
Equality, Diversity and Privacy:	Appendix 1 - Equality Impact Assessment Appendix 2 - Data Protection Impact Assessment
Associated Documents:	The following documents must be read in conjunction with this document: • Information Governance Policy, Framework & Strategy • Data Protection Policy • Information Sharing Policy • Records Management & Lifecycle Policy • Social Media Policy • Integrated Risk Management Policy • Offsite Storage Procedures

	• Controlled Environment for Finance Procedures • Information & Cyber Security Incident Procedure • Working From Home Guidance • Staff IG Handbook
References:	The following articles were accessed and used to inform the development of this document: • Records Management Code of Practice for Health and Social Care (2021) • Information Commissioners Office – Children and the UK GDPR (What rights do children have? | ICO)

Table of Contents

1.0 Introduction

1.1 NHS Bedfordshire, Luton and Milton Keynes Integrated Care Board (ICB) aims to ensure robust governance through its formal written procedural documents, such as this document, which communicate standard organisational ways of working. These documents help clarify operational requirements and consistency within day-to-day practice. They can improve the quality of work, increase the successful achievement of objectives and support patient safety, quality and experience. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible.

1.2 The ICB must design and implement procedural documents that meet the diverse needs of our service and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010. The Equality Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to the individual protected characteristics is incorporated at Appendix 1.

1.3 A Data Protection Impact Assessment is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. The Data Protection Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to an individual's privacy is incorporated at Appendix 2.

1.4 The ICB has a duty to comply with the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018). They give individuals (data subjects) the right to request access to the information the ICB holds about them. This right is commonly known as a Subject Access Request (SAR).

1.5 The Access to Health Records Act 1990 (AHR Act 1990) grants rights to specified individuals to request information held by the ICB about a deceased individual.

1.6 The aim of this policy is to:

- Ensure that the ICB meets its obligations regarding 'subject access requests' under the terms of UKGDPR and DPA 2018
- Ensure that the ICB meets its obligations regarding 'access to health records requests' under the terms of the AHR Act 1990
- Set out clear guidelines for ICB staff to help make the access timely and within the legislation.

2.0 Scope

2.1 This policy **applies** all ICB staff members, including Ordinary Members of the Board of the ICB, and Practice Representatives, involved in the ICB's policy-making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third-party supplier) - here in after referred to as 'staff'.

2.2 This policy does not cover other rights of the data subject under UKGDPR – i.e.

- The Right to Be Informed
- Right to Rectification
- Right to be forgotten
- Right to Restriction
- The Right to Object to Processing
- Automated Decision Making including Profiling
- Portability

Please refer to the ICB Data Protection Policy.

2.3 For requests for information under the Freedom of Information (FOI) Act 2000, please refer to the ICB's FOI Policy

3.0 Definitions

This section provides the public and our staff members with an explanation of terms used within this policy.

3.1 Concept of Confidentiality

3.1.1 A duty of confidentiality arises when a person discloses information to another person under conditions where it is realistic to expect that the information provided will be treated in confidence.

3.1.2 Disclosure of this information can either be authorised or unauthorised where only limited staff members have the authority to disclose information.

3.1.3 A breach of confidentiality is the unauthorised disclosure of information provided in confidence.

3.2 Confidential Information

3.2.1 Confidential information can be anything that relates to patients, staff or any other commercially sensitive information (such as contracts and tenders) held in any form (such as paper, electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on mobile devices such as laptops, tablets, smartphones, BlackBerrys) or even passed by word of mouth.

3.3 Data Controller

3.3.1 A data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.4 Data Processor

3.4.1 A data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.5 Personal Data

3.5.1 This means data which relate to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples of this type of data could include;

- Person's name, address, full postcode, date of birth.
- Email address and telephone numbers.
- Pictures, photographs, videos, audio-tapes or other images of patients.
- NHS number or local unique identifiers, these are considered identifiable if the organisation holds the means to re-identify the person from this unique identifier.
- Any other data, or linked data, that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.6 Special Category Data

3.6.1 Data held about an individual which contains both personal and sensitive information. Under the UKGDPR the following types of information are deemed as special category:

- Race,
- Ethnic origin,
- Religious or other beliefs,
- Political opinions,
- Trade union membership,
- Genetics,
- Biometrics (where used for ID purposes),
- Physical or mental health,
- Sexual life, and
- Criminal proceedings or convictions.

3.7 Processing

3.7.1 Processing means obtaining, recording, holding the information or data or carrying out an operation on the information or data. An operation could include organising, adapting or altering the data. It also includes retrieving, consulting, linking to other data sources or using the information or data.

3.7.2 Disclosing the information or data by transmission or dissemination indicates processing as does alignment, combination, blocking, erasure and destruction. Viewing data on a computer screen is considered to be processing under the Data Protection Act 2018 and the UKGDPR.

4.0 Policy Statement

4.1 The right of access by data subjects are provided under Article 15 of UKGDPR and Schedule 2, 3 and 4 of the DPA 2018.

4.2 Individuals (data subjects) have the right to:

- Have access to a copy of the information an organisation holds about them, subject to certain safeguards.
- Be provided with a copy of the information held.
- Have the information explained if it is illegible or unintelligible.
- Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

4.3 Applicants (requesters) do not have to give a reason for requesting access to the information; their motive is irrelevant.

4.4 Subject access requests can be made by:

- The data subject (individual) themselves.
- Individuals who have parental responsibility for a child.
- In certain situations, a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent.
- A representative nominated by the individual to act on their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority.

4.5 The Access to Health Records Act 1990 grants rights to certain individuals to request information about a deceased individual. These are:

- The individual's personal representative (this will be the executor of the will or the administrator of the estate)
- Any person who may have a claim arising out of the individual's death

4.6 Although the ICB does not hold Health Records it may hold information that falls under this act.

4.7 Access to Health Records requests (AHR) must be processed in much the same way as a SAR, but there are some differences which MUST be considered, these are:

- time allowed, which is 40 calendar days, not one calendar month
- we must ask the requester why they are requesting the information and what they are going to do with it
- only provide what is required to meet the purpose of the request

4.8 The ICB MUST identify:

- If it is known whether the deceased patient did not wish for their records to be disclosed or the records contain information that the deceased patient expected to remain confidential, and
- As with a SAR, if the release of the information would be likely to cause serious harm to the physical or mental health of any individual

4.9 The ICB must give the same level of confidentiality to information about the deceased as for information about living individuals. The Department of Health and General Medical Council (GMC) agree that there is an ethical obligation in requiring that confidential obligations continue to apply, subject to certain mandatory disclosures.

5.0 Roles and Responsibilities

The following have specific responsibilities in relation to this policy. For full details about staff with key roles and responsibilities for Information Governance (IG) in the ICB, please see the IG Policy, Framework & Strategy which should be read in conjunction with this policy. Roles and responsibilities in relation to this policy are detailed below.

5.1 Caldicott Guardian

5.1.1 Acting as the "conscience" of the organisation, the Caldicott Guardian actively supports work to enable information sharing where is it appropriate to share and advises on options for lawful and ethical processing of information.

5.1.2 The Caldicott Guardian also has a strategic role, which involves representing and championing privacy and information sharing requirements at senior management level.

5.1.3 In addition they are responsible for approving release of information requested as part of the subject access and access to health records process.

5.2 IG Team

5.2.1 The IG Team is responsible for ensuring they process subject access and access to health records requests appropriately and within the 'Time Allowed'.

5.3 Data Protection Officer (DPO) & Head of Safe Practice

5.3.1 The DPO is responsible for ensuring the ICB complies with the requirements of UKGDPR, DPA 2018 and AHR Act 1990. The DPO also acts as a contact point for data subjects and the supervisory authority (ICO).

5.4 All Staff

5.4.1 All staff are responsible for ensuring they comply with this policy by forwarding requests to the IG Team immediately and for (as detailed in this policy), assisting

requesters and providing (when asked by the IG Team) requested information in a timely manner.

6.0 Processes and Procedures

6.1 Receiving Requests

6.1.1 The IG Team is required to manage and process all requests received by the ICB. ICB staff who receive requests MUST immediately forward any requests they receive to the ICBs IG team blmkicb.ig@nhs.net

6.1.2 A request could be from the data subject or from a third party acting on their behalf e.g., a solicitor or an accident claims firm and could arrive by:

- post (including hand delivered to one of the ICBs locations)
- by email to any member of ICB staff

6.1.3 Under UKGDPR requesters are permitted to request information verbally.

6.1.4 If a member of ICB staff receives a verbal request they must explain to the requester that it would be useful if they could confirm their request in writing by completing the ICBs SAR & AHR form which is available on the public website www.bedfordshirelutonandmiltonkeynes.icb.nhs.uk as this will assist us in ensuring we have the correct information to process their request.

6.1.5 They will need to forward their request, together with the relevant ID to the IG Team as instructed on the form.

6.1.6 If the requester is unable or unwilling to print the form you must take their contact details and forward them to the IG Team blmkicb.ig@nhs.net who will contact them.

6.2 Deadline/Time Allowed

6.2.1 The ICB must process the request and provide the information as soon as practicable and at least within one calendar month from the date of the initial request to process the SAR. This is why it is important for any requests to be forwarded to the IG Team immediately.

6.2.2 Only in specific circumstances when the request is excessive (i.e., requester has made more than one request) or its particularly complex the ICB can extend the one calendar month time allowed (for up to a further two calendar months). However, the requester must be informed of the reasons for the extension within one calendar month from date the request was received.

6.2.3 The one calendar month clock for processing the request starts on the day the ID information is received by the ICB.

6.2.4 Remember if it as an AHR, the time allowed is 40 calendar days.

6.3 Consent and Identification

The IG Team is responsible for ensuring the appropriate consent is provided and checked prior to confirming if the ICB holds information about the data subject or not.

If the request is not from the data subject, evidence of consent may be required. This will depend on who the request is from.

- **Children**

  Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident, they can understand their rights, you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

  A child may exercise this right on their own behalf as long as they are competent to do so. In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

  If you have already decided that a child is competent to provide their own consent, then it will usually be reasonable to assume they are also competent to exercise their own data protection rights.

  If a child is competent then, just like an adult, they may authorise someone else to act on their behalf. This could be a parent, another adult, or a representative such as a child advocacy service, charity or solicitor.

When may a parent exercise these rights on behalf of their child?

Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent or guardian.

You should therefore only allow parents to exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of the child.

How does this work in practice?

An adult with parental responsibility may seek to exercise any of the child's rights on their behalf.
If you are satisfied that the child is not competent, and that the person who has approached you holds parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf. The exception to this is if, in the specific circumstances of the case, you have evidence that this is not in the best interests of the child.

If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or again if it is evident that this is in the best interests of the child.

What matters is whether the child can understand and deal with the implications of exercising their rights. So, for example, does the child understand what it means to request a copy of their data and how to interpret the information they receive as a result of doing so? When considering borderline cases, you should consider, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to exercise the child's rights. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

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'.

Married, separated and divorced parents both have parental responsibility even if they no longer live with the child, unless a Court Order has removed that status from any party.

Parental responsibility can also be acquired:

- Through 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 order - (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 ICB is entitled to deny access as being against their best interests.

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**

  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.

- **Power of Attorney, Court Appointed Deputy, Protection Order**

  If someone does not have mental capacity to manage their own affairs then someone granted with Power of Attorney (only applicable when the individual is alive), their Court Appointed Deputy or Protection Order (again, only applicable when the data subject is alive), may make the request on their behalf and will not be required to evidence the data subjects consent.

- **Mental Capacity**

  Where an individual is unable to give consent due to physical and/or mental capacity the IG Team will do all it can to assist in demonstrating that the request without consent is appropriate and lawful e.g., by speaking to the individuals GP, other care provider etc.

- **Representative**

  When a request is received from somebody who is not the data subject and they do not have any legal right to act on their behalf without their consent e.g., Solicitors, Accident/Injury Claim Firms, Union Reps, Professional Registration Body e.g., NMC etc., then evidence of the data subjects consent MUST be provided together with details of what the data subject is consenting to. The ICB will only release information which the data subject has consented to.

- **Court Order & Coroners**

  Unlike a request from a solicitor, a Court Order does not need the data subject's consent and should be obeyed unless there is a robust justification to challenge it, in which case the ICB may challenge the order through the Court. The Court's decision is law, unless the ICB 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 records must be retained by the ICB. 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 **MUST** be forwarded immediately to the ICB's IG Team.

- **Department of Work and Pensions**

  Chapter 3 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 which MUST be forwarded to the IG Team.

- **Police**

  All requests from the Police should be in writing and forwarded immediately to the Information Governance team.

  Chapter 3 of the Data Protection Act 2018 allows (but does not require) personal data to be requested and provided to assist in the prevention or detection of crime and the apprehension of and prosecution of offenders.

  The Police are required to obtain the data subjects signed consent unless this would prejudice the enquiry or court case. Any request from the Police must be on an official Police request form (formerly known as a Section 29), detailing what information is being requested and consent of the individual or details of why it would not be appropriate to obtain the data subjects consent.

  Requests without consent must be counter signed by the Chief Superintendent or above.

  Chapter 3 of the Data Protection Act 2018 also allows (but does not require) personal information to be requested and provided to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder, without the data subject's consent.

  For the ICB 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).

- **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 information is required, informed, 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/ pseudonymised data, consent is not required, but patients should be informed by posters and/or leaflets how their information may be shared.

  Such requests must be in writing and forwarded immediately to the IG Team for consideration.

6.4 Proof of Identity (ID)

6.4.1 Depending on who the request is from the requester may need to provide proof of their identity (ID). The requester may provide this with their request, if they don't the IG Team will request it from the requester. The ID required will depend on who the request is from - see table below.

Request From	ID Required
Data Subject	A copy of: ● Their passport or driving licence or something with their signature on And ● A utility bill or financial statement that has their name and address on (they can black out/redact any financial information)
Solicitor e.g., Injury/Accident Claim	No ID required, but a consent form signed by the data subject with details of what information they are consenting to the release of MUST be provided.
Parent or Guardian of a child under the age of 16	A copy of: ● The child's Birth Certificate or Adoption Certificate or proof of the requesters custody of or responsibility for the child And ● The requesters passport or driving licence or something with their signature on And ● A utility bill or financial statement that has the requesters name and address on (they can black out/redact financial information)
Power of Attorney or holder of a Court Order of Protection	A copy of: ● The signed Power of Attorney document or Court Order of Protection And

	• The data subjects passport or driving licence or an official document with their photograph on And • The requesters passport or driving licence or an official document with their photograph on And • A utility bill or financial statement that has the requesters name and address on (they can black out/redact financial information)
Executor of Estate or Administrator of Will	• An official document or letter which lists the requester as the Executor of the Estate or Administrator of the Will And • The requesters passport or driving licence And • A utility bill or financial statement that has the requesters name and address on (they can black out/redact financial information)

6.5 Obtaining the Requested Information

6.5.1 The request may be for <u>everything</u> the ICB holds including handwritten notes, letters, reports, photographs, audio and visual recordings or may be for specific information/documents e.g., a report about the data subjects care, minutes of meetings held about the data subject. If the request is from or about a member of staff they may be requesting their personnel file.

6.5.2 When a request is received the IG Team will contact relevant departments to establish if they hold the requested.

6.5.3 Where the data subject is a member of ICB staff, in the interest of confidentiality, they may wish to send information to the requester directly or provide it to the IG Team in a sealed envelope. An approach will need to be agreed with the IG Team.

6.6 Checking the Information for Removal or Redaction

6.6.1 UKGDPR, the Data Protection Act 2018 and the Access to Health Records Act 1990 make provisions for withholding information in certain circumstances, which the IG Team will consider when processing requests.

6.6.2 The IG Team will check to ensure that all of the information provided by the relevant department falls under the scope of the request and identify if any of the information needs to be redacted. Redaction is a legal requirement covered by the Schedule 4 of the Data Protection Act 2018. However, it is illegal to withhold or delete information just because it may reflect badly on the ICB or a member of staff.

6.6.3 Redaction is the process of permanently deleting visible information (such as text and images) from a document. This may involve the removal of individual words, sentences or paragraphs or the removal of whole pages.

6.6.4 The IG Team will apply redactions on a case by case basis and will often depend on content and who the request is from.

6.6.5 The following are examples of the type of information that may be considered for redaction:

- Identifiable information about other individuals, as this is their data and not that of the data subject e.g., patient's mother is an ex-sex worker. The requester's right of access must be weighed against the other data subject's right to privacy.
- Any information that may cause psychological harm or distress to the data subject or another individual e.g., the record states that the data subject is adopted and there is no evidence to confirm that the patient is already aware of this or all local hospitals have been informed of our concerns in case one of the children attends their A&E.
- Information relating to an ongoing investigation e.g., HR, Safeguarding, NHS Fraud or other criminal investigation.
- Information on the ICB's upcoming plans which single individuals should not be made aware of as this would put them at an advantage over others.

6.6.6 In some cases it may be appropriate for the IG Team to inform third party organisations or other departments in the ICB e.g., Safeguarding, who have provided information which is contained in the record when deciding if it would be appropriate to redact it or not. However, whilst their opinion will be taken into account, the removal or redaction or not, the final decision will sit with the ICBs Data Protection Officer and Caldicott Guardian.

6.7 Approval for Release

Once the record has been checked and redactions and removals made (where relevant) the Head of Safe Practice as the DPO is responsible for checking that the ICBs legal obligations have been met in the processing of the request. The information to be released will then be shared with the ICBs Caldicott Guardian asking for their approval to release the information.

Appendix 1 - Equality Impact Assessment Initial Screening

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	Subject Access Request
Date of assessment:	14/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Protected characteristic and inclusion health groups. Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination: https://www.equalityhumanrights.com/en/equality-act/protected-characteristics	Could the policy create a disadvantage for some groups in application or access? (Give brief summary)	If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified? If not, please detail additional actions that could help. If this is not possible, please explain why
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
Gender reassignment The process of transitioning from one gender to another.	No	
Marriage and civil partnership Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.	No	
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-	No	

work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.		
Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	No	
Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
Sex A man or a woman.	No	
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.	No	
Carers Individuals within the ICB which may have carer responsibilities.	No	
Please summarise the improvements which this policy offers compared to the previous version or position.		
Review of legislation - UKGDPR		
Has potential disadvantage for some groups been identified which require mitigation?		
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)		

Appendix 2 - Data Protection Impact Assessment Initial Screening

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via blmkicb.ig@nhs.net

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

Name of Policy:	Subject Access Request
Date of assessment:	14/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

1.	**Will the policy result in the processing of personal identifiable information / data?** This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	Yes
2.	**Will the policy result in the processing of sensitive information / data?** This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	Yes
3.	**Will the policy involve the sharing of identifiers which are unique to an individual or household?** e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	Yes
4.	**Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information?** **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	No
5.	**Will the policy result in organisations or people having access to information they do not currently have access to?**	Yes
6.	**Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?**	No
7.	**Does the policy result in the use of technology which might be perceived as being privacy intruding?** e.g., biometrics, facial recognition, CCTV, audio recording etc.	Yes
8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	Yes
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	No