NHS
Lincolnshire
Integrated Care Board

Subject Access Request Policy

ICB document reference:	**ICB IG 003**
Name of originator/author:	NHS AGEM CSU
Date of approval:	March 2024
Name of responsible Committee:	Executive Committee/Audit & Risk Committee
Responsible Director/ICB Officer:	Julie Ellis-Fenwick, Head of Corporate Governance
Category:	Information Governance
EIA undertaken:	
Date issued:	March 2024
Review date:	March 2027
Target audience:	All staff
Distributed via:	Email, Website, Intranet and Board Portal

Document Control Sheet

Document Title	Subject Access Request Policy
Version	0.7
Status	Draft
Authors	NHS AGEM CSU
Date	21/02/2024

Document history			
Version	**Date**	**Author**	**Comments**
0.1	25/11/20	NHS AGEM CSU/Optum Health Systems Support: Information Governance Teams	Updated document based on predecessor Lincolnshire ICB documentation & taking account of the Data Protection Act 2018 and GDPR.
0.2	01/12/20	NHS AGEM CSU/Optum Health Systems Support: Information Governance Teams	Updated to reflect ICB policy approval process and IG lead
0.3	21/12/20	NHS AGEM CSU/Optum Health Systems Support: Information Governance Teams	Updated to reflect governance/approval arrangements
0.4	10/02/21	NHS AGEM CSU	Minor wording amendments
0.5	04/10/21	NHS AGEM CSU	Slight wording amendment. Still fit for purpose.
0.6	27/06/2022	NHS AGEM CSU	Policy review and rebrand for the transition of the CCG to an ICB
0.7	21/02/2024	NHS AGEM CSU	Minor changes.

Contents

Subject Access Request Policy

Introduction

1. Data protection legislation sets out that data subjects should in general have the right of access to their own personal data. This policy sets out how NHS Lincolnshire Integrated Care Board (ICB) seeks to enable data subjects to exercise their right of access in accordance with the requirements in the Data Protection Act 2018.

Aims of the policy

2. This policy aims to:

   3.1 outline the ICB commitment to responding to all subject access requests (SARs) in an open and transparent way

   3.2 outline the ICB commitment to ensuring that all personal data is processed fairly and lawfully and in accordance with data subjects' rights

   3.3 clarify the responsibility of everyone working for the ICB, or on our behalf to comply with this policy when dealing with SARs

   3.4 Identify the approach that the ICB will routinely take when responding to SARs, including setting out in general terms any exemptions likely to be relied upon when responding to requests

Scope

3. This policy applies to all SARs received by NHS Lincolnshire ICB.

Roles and Responsibilities

4. The Data Protection Officer will monitor compliance with this policy.

   The Information Governance team within NHS Arden & Greater East Midlands Commissioning Support Unit is responsible for managing all responses to SARs within statutory deadlines. The team can be contacted at agem.lincs.ig@nhs.net

5. NHS Lincolnshire ICB staff are responsible for:

   5.1. Being able to identify SARs

   5.2. Referring SARs immediately to the Information Governance team at agem.lincs.ig@nhs.net

   5.3. Co-operating with and assisting the Information Governance Team to coordinate responses to SARs.

6. NHS Lincolnshire ICB will provide staff with appropriate training so that they are able to comply with their responsibilities under this policy.

Policy review

7. The ICB will review this policy every 3 years, or more frequently in the event of any legislative or regulatory changes.

Policy statements

Details of how to make a request

8. The ICB publishes information about how people can access the information held about them through its privacy notice on its website.

Confirmation of identity

9. The Information Governance team will normally ask applicants to provide written confirmation of their SAR via email or letter, although it is recognised that SARs do not have to be made in writing. Where verbal requests are received the requester will receive confirmation of the request details to ensure clear understanding of the request by the ICB. For applicants from Continuing Health Care and Personal Health Budget Services decisions regarding seeking identity information should be made on a case by case basis, as it may not be reasonable to ask data subjects or their representatives for this information if it is already held by the ICB.

10. The Information Governance team will usually progress a SAR once the following information has been provided.

    10.1. full name of requester

    10.2. previous name(s) (if applicable)

    10.3. address and/or email address

    10.4. date of birth

    10.5. authorisation to communicate with a third party (if applicable).

11. Depending on the circumstances, the Information Governance team may ask the applicant, or their representative, for further proof of identity or authority to act.

12. Where the Information Governance team is otherwise satisfied as to the identity of the person making the request, and the ICB agrees, it may elect to waive the requirement for the applicant to provide proof of identity.

Clarifying the request

13. Where there is a large amount of information relating to the applicant, the Information Governance team may ask the applicant to clarify the specific information the requester is looking for. The team should send clarifying correspondence to the requester as soon as possible following receipt of the request.

Timescale for compliance

14. The Information Governance team must log the date that the request was received, and the applicant's identity confirmed.

15. The team must aim to deal with all requests promptly and to respond within one month. Where this is not possible the team must within one month tell the applicant:

    15.1. that they are extending the response time for up to two months and the reasons why, or

    15.2. why they have decided not to respond to the request and how to contact the Information Commissioner's Office to seek support and advice or seek a judicial remedy

    15.3. Both the above decisions must be made following discussion and agreement within the ICB

16. The Information Governance team will monitor the time taken to comply with requests and report to the ICB Director of Finance and Contracting.

Multiple requests and additional copies

17. If multiple or subsequent SARs are deemed unfounded or excessive, in particular because of their repetitive character, the ICB may consider:

    17.1. Charging a reasonable fee, or

    17.2. Refuse to act on the request.

18. In deciding whether multiple requests are excessive or made at unreasonable intervals, the Information Governance team will take into account:

    18.1. The nature of the data, including whether it is particularly sensitive

    18.2. The purposes of the processing, including whether it is likely to cause a detriment to the applicant

    18.3. The frequency with which the data is altered, including whether the data is likely to have changed or been altered since the previous request

    18.4. The time that has elapsed since the previous request

    18.5. The volume of information involved

    18.6. Any reasons given by the applicant for wanting the same information again

    18.7. Whether the information would be disclosable through other routes

    Decisions on this will be made following discussion and agreement with the ICB

19. The Information Governance team will keep a record of the decision made and respond to any requests by the applicant for a review of their decision.

Searching for personal data

20. The Information Governance team will ask the relevant ICB services to undertake a reasonable and proportionate search for the personal data requested.

21. A record of the search parameters and strategy used must be clearly recorded in every case, as advised by the ICB

Amending data that is the subject of a request

22. It is a criminal offence for staff to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure to a person who has made a SAR unless:

    22.1. The data would have been amended in any event; and/or

    22.2. It is reasonably believed that the individual is not entitled to receive the requested information

23. Accordingly, where any normal or routine amendment or deletion of data is proposed following receipt of a SAR, this should be discussed in the first instance with the Information Governance team.

24. The ICB will aim to provide data held at the time the SAR was received. However, in some cases routine use of the data may result in it being amended while the request is being dealt with. The ICB may therefore supply the information held as at the date of the response, even if this is different to that held when the request was received.

Review of the information

25. Once the relevant information has been located, the Information Governance team, in conjunction with an agreed ICB service lead, will review the data prior to disclosure and will determine whether any exemptions apply.

26. The subject access right is to information, i.e. personal data, and not to documentation. Accordingly, the team may extract the requesters personal data from documentation or redact information which is not the requesters personal data when preparing a response. Where appropriate, the team may provide relevant contextual information to assist the applicant, as advised by the ICB

27. For complex requests the ICB nominated lead and the appropriate ICB service lead will review the information prior to disclosure. In the most sensitive cases, further escalation and review may be necessary.

Exemptions

28. The ICB may be exempt from complying, in full or in part, with a SAR if:

28.1. the information sought is mixed data and there is not the consent of the other data subject to release the information, and it is not reasonable in the circumstances to disclose the data

28.2. the disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders

28.3. the disclosure would prejudice the ICB regulatory functions, or the functions of another regulator

28.4. the information contains legally privileged personal data

28.5. disclosure would be likely to prejudice the ICB negotiations with the data subject.

29. Some personal data that the ICB holds will be 'mixed' data relating to the requester and a third party. For example, records obtained during a Continuing Health Care services assessment may contain data belonging both to the author of the statement and the data subject. The Information Governance team, together with the relevant services lead will assess whether it is appropriate to seek consent in these cases before deciding whether to apply an exemption.

Response

30. Where the ICB holds data about a data subject, the response will contain the following information:

31.1 the purpose of the processing

31.2 the categories of the personal data concerned

31.3 the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations

31.4 where possible, the expected period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

31.5 the data subject's right to have inaccurate personal data rectified or erased and to request restriction or object to the processing of personal data

31.6 the right to lodge a complaint with a supervisory authority

31.7 where the personal data is not collected from the data subject, any available information as to their source

31.8 in cases of automated decision-making, including profiling, information about the reasons for the decision-making or profiling, as

well as the expected consequences of such processing for the data subject

31.9 in the case of transfer of the data subject's personal data to a third country or an international organisation, the appropriate safeguards that we arranged in relation to the transfer

31.10 an explanation of whether and why any exemptions have been applied to the personal data we hold.

Sending the response

32 The Information Governance team will usually respond to SARs by email.

The team will take appropriate security measures to protect the response from unauthorised disclosure.

Audit and record keeping

33. The Information Governance team will maintain records of:

33.1. the requests received by the ICB

33.2. the 'raw' products of any searches undertaken, and the strategy used

33.3. a master copy of the information containing all the personal data we hold about the applicant, along with a record of any exemptions applied

33.4. any correspondence with the applicant, including the final response

33.5. any advice received or records prepared during handling the request.

Complaints

34. The ICB will, where appropriate, voluntarily review responses that applicants are not happy with, to resolve any complaint or dispute in a proportionate manner.

35. Complaints about responses should be referred to the Information Governance team in the first instance.

36. Additionally, individuals have a right to request that the Information Commissioner assess compliance of circumstances with the requirements of data protection legislation, and/or to start legal action to enforce their subject access rights.

Glossary

Data Protection Act 2018	The Data Protection Act 2018 governs the processing of Personal Data. The legislation requires that personal data including special categories of personal data, which are regarded as more sensitive, must be processed by Data Controllers in accordance with the Act, which incorporates the data protection principles set out in the General Data Protection Regulations.
Data Controller	A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. The ICB is a Data Controller for the purposes of data protection legislation
Data Processor	Any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller.
Data Subject	Any living individual who is the subject of Personal Data.
Personal Data	Personal Data' means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The above definition includes any expression of opinion about the individual and any indication of the intentions of the Data Controller (i.e. us) or any other person in respect of the individual.
Special Categories of Personal Data (formerly "sensitive personal data")	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information about the commission of offences or criminal proceedings is also regarded as sensitive under data protection legislation and the ICB handles such information commensurately.
Processing	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.