



Norfolk and Waveney
Integrated Care Board

Norfolk and Waveney ICB

INFORMATION RIGHTS POLICY

Document Control Sheet

This document can only be considered valid when viewed via the ICB'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.

Name of document:	Information Rights Policy <i>Previously known as Subject Access Request and Information Rights Policy</i>
Ref Number:	N/A
Version:	3.0
Date of this version:	July 2024
Produced by:	This policy has been prepared by the IG Support Officers on behalf of IG Manager / Data Protection Officer.
What is it for?	This policy informs the general public on their information rights under UK GDPR and confirms how the organisation handles information rights requests. It also provides guidance to staff on their responsibilities.
Evidence base:	<ul style="list-style-type: none"> • UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • Access to Health Records Act 1990 • Freedom of Information Act 2000 • Human Right Act 1998 • Regulation of Investigatory Powers Act (& Lawful Business Practice Regulations 2000) • Public Interest Disclosure Act 1998 • Re Use of Public Sector Information Regulations 2005
Who is it aimed at and which settings?	Implementation of this policy is the responsibility of all staff who work for NHS Norfolk & Waveney ICB, including employees, contractors, interims, and Board members. It is also aimed at the general public for information and guidance.
Impact Assessment:	Equality Impact Assessment completed – no adverse impact. Data Protection Impact Assessment not required.
Other relevant approved documents:	Local Policies: <ul style="list-style-type: none"> • IG Strategy and Framework • Data Protection & Confidentiality Policy • Freedom of Information Act Policy & Publication Scheme • Records Management Policy • Information Risk Management Policy • Data Quality Policy
References:	<ul style="list-style-type: none"> • UK General Data Protection Regulations • National Data Guardian's Data Security Standards • Information Commissioner's guidance on Subject Access Requests • Access to Health Records Act 1990
Training and competencies	This policy is underpinned by the Data Security and Awareness national e-learning package which is mandatory for all staff
Monitoring and Evaluation	This policy will be monitored and reviewed for effectiveness by the IG Manager / Data Protection Officer.

Consultation:	This is an external document that does not require further involvement or engagement at this time, as it has been written in accordance with the UK's current data protection legislation.
Reviewed by:	IG Working Group
Approved by:	Audit and Risk Committee
Date approved:	16 th July 2024
Dissemination:	Staff Intranet
Date disseminated:	5 th August 2024
Review Date:	April 2026
Contact for Review:	nwicb.informationgovernance@nhs.net

Version Control

Revision History	Summary of Changes	Author(s)	Version No.
May 2022	Creation of a policy for the new Norfolk & Waveney Integrated Care Board	IG Manager	V0.1
July 2022	Amendments to information rights sections.	IG Manager	V0.2
June 2022	Policy approved by SIRO and Deputy Caldicott Guardian on behalf of IG Working Group	IG Manager	V1
October 2022	Template change.	IG Manager	V2
Nov 2023 – April 2024	Review and change name to Information Rights Policy from Subject Access Request Information Rights Policy. Revision of flow and clarity of wording	IG Manager/IG Support Officer	V2.1
July 2024	Final Version	IG Support Offer	V3.0

Contents

1	<u>INTRODUCTION</u>	6
2	<u>PURPOSE</u>	6
3	<u>SCOPE</u>	7
4	<u>GENERAL PRINCIPLES OF INFORMATION RIGHTS</u>	7
5	<u>ROLES AND RESPONSIBILITIES</u>	10
6	<u>PROCESSING OF INFORMATION REQUESTS</u>	11
7	<u>RIGHT OF ACCESS (SUBJECT ACCESS REQUESTS)</u>	12
8	<u>ACCESS TO HEALTH RECORDS REQUESTS</u>	13
9	<u>MAKING A REQUEST FOR ACCESS TO PERSONAL DATA</u>	14
10	<u>FEES</u>	15
11	<u>CHILDREN'S RECORDS</u>	15
12	<u>ADULTS WITHOUT CAPACITY</u>	16
13	<u>ACCESS TO THIRD PARTY RECORDS</u>	16
14	<u>REFUSAL</u>	16
15	<u>OTHER TYPES OF INFORMATION REQUESTS</u>	17
16	<u>COMPLAINTS AND APPEALS</u>	17
17	<u>MONITORING AND REVIEW</u>	17
18	<u>EQUALITY IMPACT</u>	18
Appendix A	<u>PROCESS FLOWCHART FOR RIGHT OF ACCESS REQUESTS</u>	19
Appendix B	<u>ACCESS TO RECORDS REQUEST FORM</u>	20

1. INTRODUCTION

1.1 In summary, the UK General Data Protection Regulations (UK GDPR) provides the following rights for individuals:

- The right to be informed.
- The right of access (formerly Subject Access rights).
- The right to rectification.
- The right of erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

The following provisions apply to all of the above information rights:

- Requests can be made verbally or in writing.
- Requests must be acted upon without undue delay and responded to within one month (or three months if complex).
- The identity of the requesting individual needs to be confirmed before any personal data is disclosed.

1.2 Unless otherwise stated in this policy, individuals who would like to invoke any of the above rights under UK GDPR should submit their request to the Information Governance (IG) Team at nwicb.informationgovernance@nhs.net.

1.3 Individuals have the right to appoint a representative to make a request on their behalf. A third party can also act on behalf of an individual and invoke any of these rights where the individual lacks capacity. Appropriate legislation and authority to act will apply.

1.4 The Access to Health Records Act 1990 gives the right of access where the patient has died to a personal representative and/or any person who may have a claim arising out of the individual's estate. Requests made under the Access to Health Records Act 1990 must be responded to within 40 days.

1.5 An individual has the right to complain to the ICB and the Information Commissioners Office if they are unhappy with the response to a request.

2. PURPOSE

2.1 The purpose of this policy is to outline how the organisation handles information rights and resulting requests. It provides guidance in managing requests for the release of personal data. Requests can be received from anyone. For example:

- Living individuals under the Data Protection Act 2018 (DPA)
- Power of Attorneys for living individuals under the DPA
- Legal representatives on behalf of living individuals under the DPA
- Beneficiaries of a deceased individual's Estate under the Access to Health Records Act 1990 (AHRA)
- Legal representative on behalf of beneficiaries of a deceased individual under the AHRA
- Police

- Coroners Court
 - Medical Examiner
 - Court of Protection
 - Courts and Tribunals
- 2.2 This policy should be read in conjunction with the ICB's, Record management Policy, IG Strategy and Framework, Data Protection & Confidentiality Policy, and supporting policies, as well as the ICB's Privacy Notices, which describe how the ICB addresses data protection, confidentiality, information security and records management.

3. SCOPE

- 3.1 Application of this policy applies to all staff (substantive, temporary and seconded to the ICB), contractors, members of the Board and clinical advisors.
- 3.2 This policy applies to any request raised in relation to personal data held, owned, or managed by the ICB that is outside normal working practices. This policy does not relate to information held by GP Practices and/or provider organisations.
- 3.3 This policy relates to personal data which refers to a living or deceased individual held by the ICB in any format such as (this is not an exhaustive list):
- Paper records, both current and archived.
 - Electronic records held by the ICB.
 - Personal data stored within an electronic system, such as a case management system, electronic staff record etc.
 - Information contained within emails, MS Teams Chat, WhatsApp, and SMS messages (this includes information on ICB issued or personal devices if the dominant purpose for the communication was related to conduct of duties within the ICB).
 - Information held via video or audio in support of business practices, in line with the ICB records management policy.
- 3.4 This policy only relates to the release of person identifiable data under the DPA and/or AHRA. It does not relate to the release of information under the Freedom of Information Act 2000.

4. GENERAL PRINCIPLES OF INFORMATION & ACCESS RIGHTS

4.1 The Right to be Informed

The ICB has an obligation to provide 'fair processing information' and be open and transparent over how we use personal data. To meet our obligations, the ICB has two privacy notices – one for the public [Your information - Norfolk & Waveney Integrated Care System \(ICS \(\[improvinglivesnw.org.uk\]\(https://www.improvinglivesnw.org.uk\)\)\)](#), and one for staff. Both of these explain:

- What a privacy notice is and why it has been issued.
- Who we are, what we do and how to contact us.
- What information we collect, how and why.
- How the information is stored and used, and why this is important.
- How we keep information safe and maintain confidentiality.

- Where and why information may be shared with others.
- An individual's right to withhold or withdraw sharing consent.
- How to gain access to the information that we hold.
- How to raise concerns, queries, or complaints.

4.2 [The Right of Access](#)

Under UK GDPR and DPA, the right of access, commonly referred to as subject access, gives all individuals the right to obtain a copy of their personal data, as well as other supplementary information. Current legislation assists individuals to understand how and why organisations are using data about them, and check that it is being used lawfully i.e., in accordance with their information rights.

The DPA however, only relates to living individuals. There is additional legislation in place to underpin the release of health records relating to deceased individuals, to ensure that their right of confidentiality does not cease following death. This is called the Access to Health Records Act 1990 (AHRA).

A Right of Access, also referred to as a Subject Access Request, is most often used by individuals who want to see a copy of the information an organisation holds about them. However subject access goes further than this and an individual is entitled to:

- Be informed whether their person data is being processed, held, or stored.
- Request a copy of the data held about them, in a format of their choice.
- Request details of the purposes for processing of their personal data and who it is being shared with.
- Request details of the source sharing their personal data with the organisation.

4.3 [The Right of Rectification](#)

Individuals are entitled to have their personal information corrected (rectified) if it is inaccurate or incomplete. The corrections must be actioned by the ICB within one calendar month of receiving the request. This timeframe may be extended to a maximum of three calendar months where the request is complex.

Any processing of the information which requires correction should be restricted until the corrections are completed.

In all cases the applicant must be directed to the IG Team who will consider whether rectification is appropriate, taking in to account the nature of the personal information, what it will be used for and the impact of any change.

4.4 [The Right to Erasure](#)

The right to erasure is also known as 'the right to be forgotten' and enables an individual to request the deletion or removal of personal data. However, this right will only apply under specific circumstances (further details are available [here](#) on the ICO website). There are also additional requirements when the request for erasure relates to a child's personal data. Further guidance should be sought from the IG Team as required.

The ICB must respond to a request for erasure without undue delay and at the latest within one month, confirming whether the data in question has been erased or whether the request has been refused.

4.5 [The Right to Restrict Processing](#)

Individuals are entitled to stop or prevent the processing of their personal data. Where this occurs, the ICB is permitted to continue storing the data – unless the individual also invokes their right to erasure (see 4.4).

The ICB must comply with a request for restriction without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requestor's identity or a fee where applicable.

Where processing is restricted, the ICB will retain just enough information to ensure that this restriction is respected in the future. Should this type of request be received, further guidance should be sought from the IG Team.

4.6 [The Right to Data Portability](#)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. However, this right will only apply when the, the data is given with consent and processing is carried out by automated means, and therefore is unlikely to apply to the information held by the ICB. Should this type of request be received, further guidance should be sought from the IG Team.

The ICB must comply with a request for data portability without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requestor's identity or a fee where applicable.

4.7 [The Right to Object](#)

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority.
- Direct marketing (including profiling); and
- Processing for the purposes of scientific/historical research/statistics.

The individual must have an objection on "grounds relating to his or her particular situation", and the ICB must cease the processing unless compelling legitimate grounds for the processing can be demonstrated, which override the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise, or defence of legal claims.

The right to object is explained within the ICB's privacy notices, and individuals should be made aware of this right "at the point of first communication". This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information". This right is particularly relevant to research carried out by (or in conjunction with) the organisation. Should this type of request be received, further guidance should be sought from the IG Team.

The ICB must comply with an objection without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requestor's identity or a fee where applicable.

4.8 Rights Relating to Automated Decision Making & Profiling

UK GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Individuals have the right not to be subjected to a decision when it is based on automated processing, and it produces a legal effect or a similarly significant effect on the individual.

It is unlikely that this situation will occur due the ways in which information regarding patients, service users and staff is processed by the ICB. However, should there be a query relating to this area, guidance should be sought from the IG Team.

5. ROLES AND RESPONSIBILITIES

5.1 All staff are responsible for:-

- Familiarising themselves with this policy.
- Recognising a request for personal information and immediately raising any individual rights requests, received verbally or in writing, to the IG Team (the right of access, rectification, erasure, restriction of processing, right to object etc.)
- Prioritising a request for information from the IG Team.
 - Requests by the IG Team for relevant searches must be responded to within the deadline given. If this is not possible, you must contact the IG Team as soon as possible to discuss.
 - Searches must be conducted as directed by the IG Team in line with the scope of the request.
 - All information identified must be shared with the IG Team in its raw, unredacted / uncensored form. It is unacceptable for any member of staff to knowingly withhold information with the intention of preventing its release. If it is identified that this has occurred, action may be taken in line with the ICB's Disciplinary Policy.
- Ensuring any processing undertaken is accurately represented within the ICB's Privacy notices. (the right to be informed) [Your information - Norfolk & Waveney Integrated Care System \(ICS \(improvinglivesnw.org.uk\)\)](#)
- Ensuring they provide information about the purpose for which the ICB is collecting and processing their information and who it may be shared with etc. For example, staff who collect information directly from individuals via surveys, engagement activity etc. (right to be informed)
- Ensuring that only the minimum information necessary to satisfy the original purpose for the data collection is held by the ICB (UK GDPR Principle B – Purpose Limitation).
- Accurately and timely record keeping in line with the Data Quality Policy (right to erasure and rectification)
- Ensuring they comply with the ICB AI policies and complete a risk assessment prior to processing secure information. For example, staff who use and set up artificial intelligence support packages (rights in relation to automated decision making)

- Understanding individuals' rights as set up in the Privacy Notice, these are your rights as well as service users. [Privacy Notice - Your Rights - Norfolk & Waveney Integrated Care System \(ICS \(improvinglivesnw.org.uk\)\)](https://www.improvinglivesnw.org.uk/Privacy-Notice-Your-Rights-Norfolk-Waveney-Integrated-Care-System-ICS)
- Ensuring that information is held in a safe and structured way, in accordance with the Records Management Policy, to ensure that it can be retrieved quickly when an access request is received.
- Staff must not look up or amend their own record as it could be seen as abuse of privilege – this includes health/medical and employment records. All access must be governed via the processes outlined in this policy, and staff are required to follow the same procedure as any other requestor.
- Staff should only access the records of their family, friends, and other people they know (such as colleagues) when there is a legitimate professional reason to do so, in line with the job description and contract of employment. If this situation occurs, the member of staff should inform an appropriate senior manager who will assess the impact and risks and may allocate another member of staff to the relevant task(s).

5.2 The IG Team is responsible for: -

- Ensuring that requests for access to personal data are lawful, fair, and justifiable and the appropriate supporting documents have been provided.
- Responding to all requests for access to personal data in respect of living and deceased individuals, within the appropriate timeframes. Personal data is only released in accordance with the DPA and AHRA.
- Responsible for redacting third party, sensitive or undisclosable information from the content provided.
- Providing advice and guidance to staff on this policy, and any sharing or processing.
- If the organisation has actioned a request for rectification, erasure or restriction of processing and already disclosed the personal data in question to any third parties, the ICB must inform them about the action taken, unless it is impossible or involves disproportionate effort to do so. The IG Team will discuss this with the relevant team to ensure the appropriate action is taken.

5.3 The Caldicott Guardian has executive responsibility for the ICB's response to information requests. The Caldicott Guardian has a clinical background, they will be responsible for reviewing the final response, ensuring that any personal data has been appropriately and correctly redacted, in line with Caldicott Principles and authorise release of the response.

5.4 The Data Protection Officer (DPO) is responsible for ensuring that the ICB acts lawfully in accordance with the DPA and AHRA. Therefore, the DPO will be responsible for managing all complex requests, ID approval, refusals to release personal data and any associated complaints.

6. [PROCESSING OF INFORMATION REQUESTS](#)

6.1 A request can be received verbally or in writing, from the individual or their representative,

such as lawyer, family member, Power of attorney, Court appointed Deputy etc. If a request is received by the organisation, it must be sent to the IG Team nwibc.informationgovernance@nhs.net immediately.

6.2 All requests for information outside normal practices must be passed to the IG Team.

The IG Team will process the request as outlined in [Appendix A](#) and:

- Log the request.
 - Determine if the request is:-
 - ☐ related to a living individual – governed under UK GDPR.
 - ☐ related to a deceased individual – governed under the Access to Health Records Act 1990.
 - Determine if there is a legal basis to proceed and whether further information is required from the requester.
 - Contact the requester to: -
 - ☐ acknowledge receipt of the request.
 - ☐ ask for ID or authority to act if required.
 - ☐ ask for clarity or refinement of the request.
 - ☐ keep them informed if there are any anticipated delays in the process.
 - ☐ offer advice and guidance where required.
 - Contact ICB colleagues asking for information in relation to the request.
 - Collate and review the information and redact/remove information not related to the data subject.
 - Seek approval and sign off from the Caldicott Guardian to the final response.
 - Send final response to the requester via secure Egress encrypted email.
 - Maintain a log of all requests received, in accordance with the guidance issued by the Information Commissioner's Office (ICO) and monitor compliance against the statutory timeframes.
- 6.3 It may also be appropriate for the ICB to consider a phased approach to responding to a request where large volumes of information are involved. For example, sending information in stages as and when records are ready for release rather than waiting until all the information is fully collated.
- 6.4 If the organisation takes the decision not to action a request made by an applicant in relation to the rights outlined above, this must be clearly communicated to the applicant in writing along with a full explanation and reasons for the decision. The applicant must also be given the right to make a complaint via the organisation's formal procedures and be made aware of their right to complain to the Information Commissioner's Office.

7. [RIGHT OF ACCESS \(SUBJECT ACCESS REQUEST\)](#)

7.1 The ICB has one calendar month to respond to the request (commencing on the day of

receipt of the request). However, the timeline will not start, unless:

- any required fee has been paid, if applicable. (Refer section 9)
- the identity of the requestor has been verified e.g.; proof of identity has been provided.
- the legitimacy of the request has been confirmed e.g., evidence of authority to act from a third party making a request.
- The scope of the request is clear to allow for the retrieval of information.

7.2 The response timeframe can be extended by two further months if the case is complex. The ICB will keep the requestor informed if this is to happen.

7.3 An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them, or they are acting on behalf of someone). Therefore, it is important to establish whether the information requested falls within the definition of personal data.

7.4 All information is reviewed before it is released to the requester. The IG Team will ensure that all references to third parties have been redacted to protect the confidentiality of everyone bar the requester, where it is appropriate to do so. It is important to balance the redaction process against avoiding changing the context and meaning of the information provided to the requester. The IG Team will therefore take all appropriate steps to ensure that information is not overly redacted in order to provide as open and transparent response as possible.

7.5 If the request relates to information about the ICB (for example, policies, statistics, and finances) rather than the personal information of an individual, then this would be handled under the Freedom of Information Act 2000. All FOI requests should be notified to the FOI Team via email - agem.nwicb.foiservice@nhs.net.

7.6 If it is evident that an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, the response can be sent directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

7.7 The ICB will retain Subject Access Request records for a minimum of three years, unless the information is disputed and the retention period shall be extended to 6 years, as required by the Records Management Code of Practice 2021. Thereafter, records will be reviewed and securely destroyed if no longer required to be retained.

8. ACCESS TO HEALTH RECORDS REQUESTS

8.1 These requests will be processed by the IG Team.

8.2 The AHRA provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under Section 3(1)(f) of the Act as “the patient’s Personal Representative and any person who may have a claim arising out of the patient’s death”.

- A “Personal Representative” is defined as an Executive or Administrator of a deceased individual’s Estate. As such, a personal representative does not need to explain why they are making a request, but they must provide documented evidence that they are

the personal representative before any identifiable information is released. This should be in the form of a Will, Grant of Probate or Letters of Administration.

- 8.3 If a Personal Representative has legal representation, a copy of the Grant of Probate, letter of authority for the legal representative to act on their behalf and a signed consent form to release the information to the third party must be obtained before any identifiable information is released.
- 8.4 In the absence of a Personal Representative, the ICB must be satisfied that the person requesting the release of personal data relating to the deceased individual could have a claim arising out of the deceased individual's Estate, particularly if the individual passes away intestate (without a Will), and their relationship to the deceased individual. Individuals who are not personal representatives must provide a reason for the request, including why they believe they have a claim arising out of the Estate.
- 8.5 It is important to note that relatives, friends, and carers do not have an automatic right of access to a deceased individual's health records. The request must be justifiable and proportionate.
- 8.6 Requests made under AHRA can be complex, and therefore should be managed by the IG Team in conjunction with the Information Asset Owner for the records in question. This will enable the IG Team to identify if there is a legal basis for the release of information, or if disclosure outweighs the duty of confidentiality to the deceased and any other individual referenced in the information.
- 8.7 The IG Team will consider any preferences expressed by the deceased prior to their death, the distress or detriment that any living individual might suffer following the disclosure and any loss of privacy or negative impact on the reputation of the deceased. The views of the surviving family and the length of time after death are also important considerations, as the obligation of confidentiality to the deceased is likely to erode over time.
- 8.8 The IG Team will also consider the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information extracted from the records. For example, if the point of interest is eligibility for a particular period of care, then disclosure, where appropriate, should be limited to the pertinent details.
- 8.9 Requests made for information relating to a deceased individual should be answered within 40 days (commencing on the day of receipt of the request). However, as the nature of these requests can be complex, it is important to ensure that the request is valid which may delay completion of the request in a timely manner. In addition, refer to 7.2 for aspects which may delay the processing of the request.

9. MAKING A REQUEST FOR ACCESS TO PERSONAL DATA

- 9.1 If an individual wishes to know what information the ICB holds about them, they can make a request by contacting any member of the ICB staff, in verbal or written format. Ideally the IG team request that the individual contacts us directly by either:
 - Completing the form in [Appendix B](#) and send it via email to the ICB IG Team – nwicb.informationgovernance@nhs.net
 - Send a request via post to IG Team, Norfolk and Waveney Integrated Care Board,

Floor 8 County Hall, Martineau Lane, Norwich, NR1 2DH.

- Send an email or letter outlining where you feel we may hold information, the relevant timeframes, and the type of format the information may be held in.
 - If you make a request verbally, be clear on the request being made so staff members can identify that it needs to be forwarded to the IG team.
 - If you do not receive an acknowledgement letter or email response from the ICB within a week of making the request, please contact the IG Team.
- 9.2 The ICB may contact you to request further details, to clarify the extent of the request or for proof of ID if required. If you are requesting information on behalf of another individual you will be asked for Consent to act on behalf of the other individual, such as Power of Attorney, Letter or Authority or their last will and testimony.
- 9.3 The ICB IG team's preferred method of communication is email. Any confidential information will be sent using Egress, the encryption software used by the ICB. You will need to set up a password to access the information provided to you. Guidance on how to do this can be found here [Accessing Encrypted Emails Guide](#)
- 9.4 The ICB will provide a response within the required timeframes (sections 6 & 7).

10. [FEES](#)

- 10.1 In most cases the ICB will not charge a fee to comply with a request for access to personal data under DPA or AHRA.
- 10.2 However, a reasonable fee for the administrative costs of complying with a request can be levied if:
- The request is manifestly unfounded or excessive; or
 - An individual requests further copies of the data following a completed subject access request.
- 10.3 The ICB's fees will be based on the administrative costs of complying with the request such as consumables, paper, and postage.
- 10.4 Where a fee is appropriate, the IG Team will contact the requester promptly to inform them and provide the opportunity for the requester to revise their request to avoid a fee.
- 10.5 Where a fee remains appropriate, no work on the request will commence until the fee has been received.

11. [CHILDREN'S RECORDS](#)

- 11.1 Where a child requests their own information, the ICB must assess whether the child is competent to exercise their own rights. Whilst there is no specific age identified in England for this, a child aged 12 or over could be of sufficient age and maturity to exercise their rights, unless the contrary is shown. If a child is deemed competent, just like an adult, they may authorise someone else to act on their behalf. This could be a parent, another adult

or representative. The parents or legal guardians of the child exercising their rights (if deemed competent) may not be entitled to see the records without the consent of the young person. The only exception to this is when the child lacks capacity and the parent / legal guardian holds a Lasting Power of Attorney.

- 11.2 If the ICB is satisfied that the child is not competent to exercise their rights and the individual making the request on their behalf holds parental responsibility for the child, then it would normally be considered appropriate for the holder of parental responsibility to exercise the child's rights on their behalf.

12. ADULTS WITHOUT CAPACITY

- 12.1 UK GDPR/DPA legislation makes no special provision regarding requests for personal information from adults who lack mental capacity and are unable to manage their own affairs.
- 12.2 Mental disorder does not equate to mental incapability and many individuals who suffer from a mental disorder have sufficient capacity to enable them to deal with their own affairs. However, the potential for physical harm or mental distress must be considered, and so these types of requests will be managed by the Data Protection Officer, Caldicott Guardian and clinical member of staff engaged in the individual's care.
- 12.3 Patients with learning disabilities, depending on their individual circumstances may have enough capacity to understand the process, albeit with support. Again, the Data Protection Officer, Caldicott Guardian and clinical member of staff engaged in the individual's care will manage these types of requests.

13. ACCESS TO THIRD PARTY RECORDS

- 13.1 On occasion, the ICB will receive requests for information that is owned by a Third Party as a Data Controller.
- 13.2 In these instances, the ICB will advise the data subject that it is unable to release this information but will provide the relevant contact details to enable the data subject to raise a further request direct with the relevant Data Controller.
- 13.3 This will ensure that the data subject receives the correct most up to date information, and all considerations have been given by the appropriate party in respect of confidentiality and information rights.

14. REFUSAL

- 14.1 In certain cases, the ICB can refuse to comply with a request if it feels that it is manifestly unfounded or excessive, particularly if the requester refuses to modify the request, does not confirm their identity if they are not already known to the ICB or refuses to pay a fee (in accordance with Section 12 above).
- 14.2 Some information, particularly relating to safeguarding concerns, could cause significant physical and mental distress/harm to the data subject and/or a third party if read and therefore, if there is no justifiable or legal reason to release the information, these types of requests will be rejected or partially addressed.

14.3 These decisions will be taken by the ICB's Data Protection Officer and the Caldicott Guardian, who can make a clinical decision on the potential for the information to cause significant harm.

14.4 Any decision to refuse disclosure will be centrally recorded by the IG Team.

15. OTHER TYPES OF INFORMATION REQUESTS

15.1 The police and other agencies have an important and general power of common law to prevent and detect crime and the Crime and Disorder Act 1998 introduces a number of measures to control crime and disorder. Requests must be submitted to the IG Team in writing detailing what data is required and for what purpose. Where relevant, a crime reference number should also be provided.

15.2 Where it is considered that a claim against the ICB may arise, or one has been notified, (pre-action disclosure), it may be the first indication that an incident has occurred. Any such requests that indicate that there is a potential claim against the organisation should be notified immediately to Corporate Affairs (nwicb.corporateaffairs@nhs.net)

15.3 Requests for information can be made to the ICB in respect of HR matters such as employment tribunals. Requests such as these should be discussed with the IG Team at the earliest opportunity as there will be specific timeframes within which the ICB has to respond.

16. COMPLAINTS AND APPEALS

16.1 The applicant has the right to appeal against the ICB's decision to refuse access to personal data or make a complaint about the way a request has been managed. Such complaints should be made to NHS Norfolk and Waveney ICB:

Data Protection Officer
NHS Norfolk & Waveney Integrated Care Board
Eighth Floor
Norfolk County Hall
Martineau Lane
Norwich
NR1 2DH

Email: nwicb.informationgovernance@nhs.net

16.2 After local resolution has been exhausted, if the requester remains unsatisfied with the ICB's response, they are able to escalate their concerns to the following regulatory body:

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

Telephone number: 0303 123 1113 Email: casework@ico.gsi.gov.uk

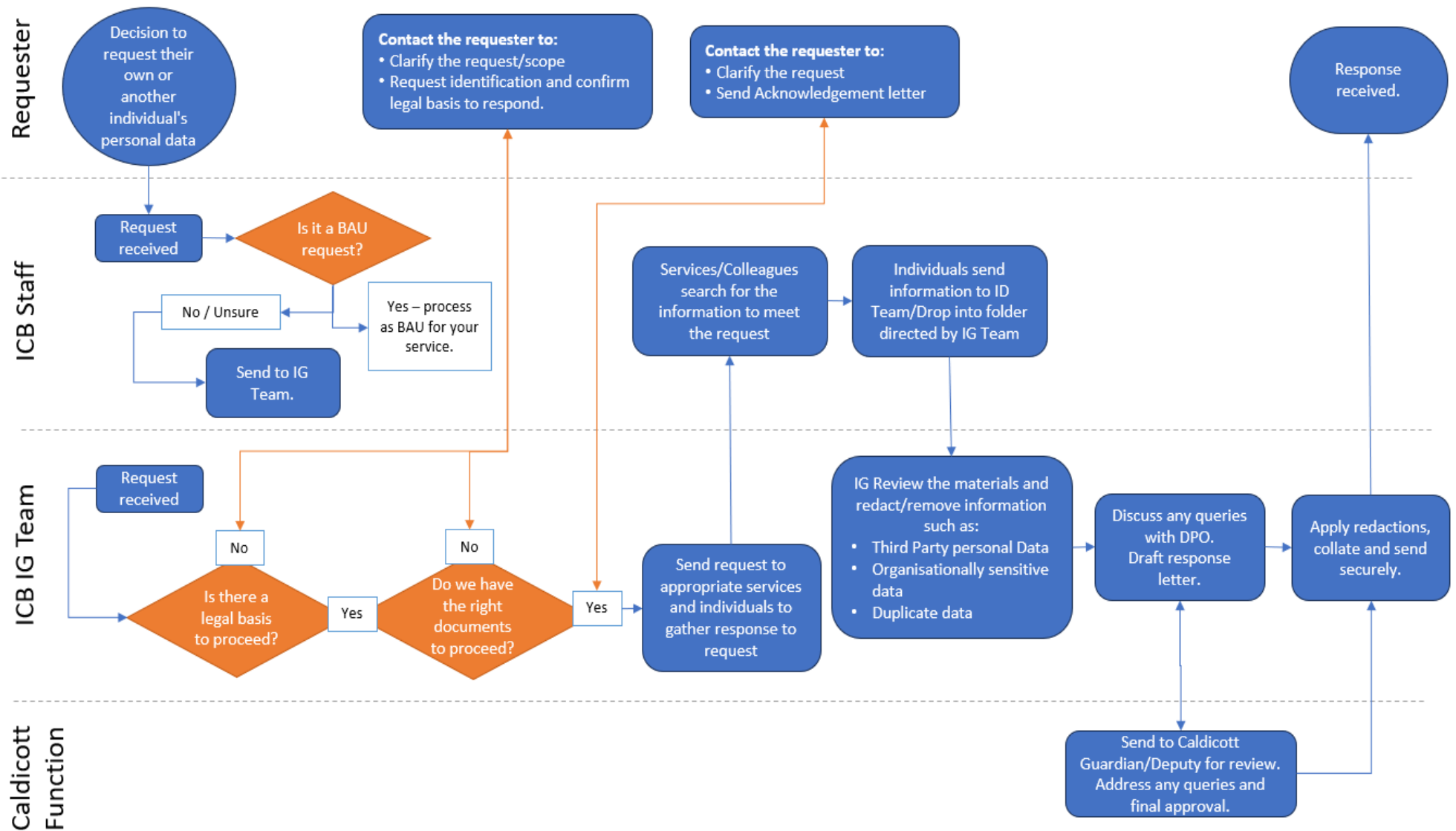
17. MONITORING AND REVIEW

- 17.1 The IG Working Group will be responsible for monitoring the effectiveness of this policy and ensuring that all access to personal records requests are handled in accordance with this policy.
- 17.2 The Audit & Risk Committee will be responsible for monitoring the effectiveness of this policy as part of the ICB's process for internal control, by reviewing the ICB's performance against statutory response times and the volume and outcome of any complaints relating to access to personal records.

18. EQUALITY IMPACT ASSESSMENT

- 18.1 In applying this policy, the ICB will have due regard to the need to eliminate unlawful direct and indirect discrimination, promote equal opportunity and provide for good relations between diverse groups. The ICB will have due regard to the following protected characteristics under the Equality Act 2010; age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; gender; and sexual orientation.

APPENDIX A: PROCESS FLOWCHART FOR RIGHT OF ACCESS REQUESTS



APPENDIX B: ACCESS TO RECORDS REQUEST FORM

The Access to Health Records Act 1990, Data Protection Act 2018 and UK GDPR gives patients/clients/staff or their representatives a right of access, subject to certain exemptions, to their health records.

Personal data collected from this form is required to enable your request to be processed. This personal data will only be used for the processing of your request.

Charges Payable: In accordance with legislation **no fee** will be charged for your request, unless the request is manifestly unfounded, excessive, or repetitive. If necessary, before any further action is taken, we will contact you with details of our “reasonable administrative charges” in order to comply with your request or provide an opportunity for you to modify your request.

PLEASE COMPLETE IN BLOCK CAPITALS OR TYPE

1.	Details of the Data Subject (i.e., the individual for whom this request is being made)
Surname:	
Date of Birth:	
Forename(s):	
Current Address:	
Any former names (If Applicable):	
Full Postcode:	
Telephone Number:	
Previous Address (If Applicable):	
NHS Number (If known/relevant):	
Full Postcode:	

2.	Details of Records to be Accessed
In order to locate the records requested, please provide as much information as possible. List the department or services accessed that you require records from: i.e. Complaints, Continuing Healthcare or Human Resources etc. (Continue on a separate sheet if required).	
Records dated from	Department or services accessed
/ / to / /	
/ / to / /	
/ / to / /	
/ / to / /	
/ / to / /	

3a.	Details of applicant (complete if different to the Data Subject)
Full Name:	
Company (if Applicable):	

Email address:	
Contact telephone number:	
3b	
Is the request related to a living individual?	Yes <input type="checkbox"/> No <input type="checkbox"/> if no go to section 3c
Are you the Parent / Legal Guardian of the living individual?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a copy of the data subject's Birth Certificate or evidence that you are the legal guardian.
Do you hold Power of Attorney or a Deputyship under the Court of Protection for the living individual?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a copy of the Power of Attorney or Court of Protection Order. This is required in order to proceed with a request under the General Data Protection Regulation / Data Protection 2018
Are you the Legal Representative of the living individual?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a copy of your Letter of Appointment and a signed and dated Consent Form to release the data subject's personal data to you. This is required in order to proceed with a request under the General Data Protection Regulation / Data Protection 2018
3c	
Is the request related to a deceased individual?	Yes <input type="checkbox"/> No <input type="checkbox"/> if no go to section 4
Do you have a claim arising from the deceased individual's Estate?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide the reason for your request (continue on a separate sheet if necessary):
Are you the Personal Representative of the deceased's Estate?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a copy of the Grant of Probate or Will of the deceased. This is required in order to proceed with a request under the Access to Health Records Act 1990
Are you the Legal Representative of the Personal Representative?	Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a copy of your Letter of Appointment, Grant of Probate and ensure Section 4 of this form is completed. This is required in order to proceed with a request under the Access to Health Records Act 1990

4.	Authorisation to release personal data to a Legal Representative (complete if the requester is not the Data Subject)
<p>I (Print name)_____hereby authorise the Norfolk and Waveney ICB to release the personal data requested within this application form to the above applicant (Section 3) who I have authorised to act on my behalf.</p> <p>Signature of patient/client/staff member : _____ Date: / /</p>	

5.	Correspondence/Email Address
<p>Address or email address for receipt of final response including personal data.</p> <p><i>Please note only one response will be provided. A charge will be levied for additional hard copies</i></p>	

6.	Declaration (to be completed by the Applicant)
<p>I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record(s) referred to above, under the terms of the Access to Health Records Act (1990) or the Data Protection Act (2018).</p>	
<p>Please select one box:</p> <p><input type="checkbox"/> I am the patient/client/staff member (data subject).</p> <p><input type="checkbox"/> I am the parent/guardian of the data subject.</p> <p><input type="checkbox"/> I hold Power of Attorney or Deputyship for the data subject.</p> <p><input type="checkbox"/> I am the Personal Representative of the data subject.</p> <p><input type="checkbox"/> I am the Legal Representative of the data subject.</p> <p><input type="checkbox"/> I have a claim arising from the patient/client's death and wish to access information relevant to my claim (covering letter with further details to be supplied).</p>	
Print Name	
Signed (Applicant)	
Date	

Please Note:

- If you are making an application on the behalf of somebody else, we require evidence of your authority to do so.
- It may be necessary to provide evidence of your identity (e.g. Driving Licence, Passport).
- If there is any doubt about the applicant's identity or entitlement, information will not be released until further evidence is provided. You will be informed if this is the case.
- Under the terms of the Data Protection Act 2018, requests will be responded to within **one calendar month** from receipt of the request. Where the request cannot be satisfied in this timeframe, we will ensure that the applicant is kept appraised. Requests will be satisfied within two calendar months.
- Under the Access to Health Records Act 1990, requests will be responded to within **40 days**. Where the request cannot be satisfied in this timeframe, we will ensure that the applicant is kept appraised. Requests will be satisfied within three calendar months.
- Under the terms of Section 7 of the Data Protection Act 2018, information disclosed under a Subject Access Request may have information redacted; this is to ensure that the confidentiality of any third party is maintained, unless their consent has been obtained or there is an overriding legal justification for disclosure.

Please complete and send this document to:

NHS Norfolk and Waveney Integrated Care Board
Information Governance Team
Eighth Floor
Norfolk County Hall
Martineau Lane
Norwich
NR1 2DH

Alternatively, send it via email to: nwicb.informationgovernance@nhs.net