Norfolk and Waveney
Integrated Care Board

Norfolk and Waveney ICB

SUBJECT ACCESS REQUEST AND 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:	**Subject Access Request and Information Rights Policy**
Ref Number:	**N/A**
Version:	**2**
Date of this version:	**October 2022**
Produced by:	This policy has been prepared by the IG Manager / Data Protection Officer.
What is it for?	This policy provides NHS Norfolk and Waveney Integrated Care Board (ICB) with a process to respond to a living individuals rights to access their personal data under the Data Protection Act 2018 and to enable certain individuals with a right of access to the health records of a deceased individual, to raise a request under the Access to Health Records Act 1990. This policy also provides guidance on other information rights as detailed under UK GDPR.
Evidence base:	• 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?	This policy applies to any request by a patient, their Power of Attorney, a beneficial of an interest in a deceased individual's Estate, or member of staff for access to their personal data held by NHS Norfolk and Waveney ICB. This policy does not apply to the release of information held by a GP Practice, care provider or local authority. Implementation of this policy is the responsibility of all staff who work for NHS Norfolk & Waveney ICB, including employees, contractors, interims, governing body members and member practice representatives.
Impact Assessment:	Equality Impact Assessment completed – no adverse impact Data Protection Impact Assessment not required.
Other relevant approved documents:	Local Policies: • IG Strategy and Framework • Data Protection & Confidentiality Policy • Freedom of Information Act Policy & Publication Scheme • Records Management Policy • Information Risk Management Policy • Data Protection by Design & Default / Data Protection Impact Assessment Policy • Data Quality Policy

References:	• 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 Audit & Risk Committee
Approved by:	Audit Committee
Date approved:	29 June 2022
Dissemination:	1 July 2022
Date disseminated:	NWICB Intranet
Review Date:	August 2023
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

Contents

1	**INTRODUCTION**		**6**
2	**PURPOSE**		**6**
3	**SCOPE**		**7**
4	**GENERAL PRINCIPLES OF INFORMATION & ACCESS RIGHTS**		**7**
	4.1	The Right to be Informed	**7**
	4.2	The Right of Access	**8**
	4.3	The Right of Rectification	**8**
	4.4	The Right to Erasure	**9**
	4.5	The Right to Restrict Processing	**9**
	4.6	The Right to Data Portability	**9**
	4.7	The Right to Object	**9**
	4.8	Rights Relating to Automated Decision Making & Profiling	**10**
5	**ROLES AND RESPONSIBILITIES**		**10**
6	**INFORMATION REQUESTS TO SUPPORT HUMAN RESOURCES**		**10**
7	**SUBJECT ACCESS REQUESTS (RIGHT OF ACCESS)**		**11**
8	**ACCESS TO HEALTH RECORDS REQUESTS**		**11**
9	**IDENTIFYING WHICH LEGISLATION APPLIES**		**12**
10	**MAKING A REQUEST FOR ACCESS TO PERSONAL DATA**		**13**
11	**RESPONDING TO A REQUEST**		**13**
12	**FEES**		**14**
13	**CHILDREN'S RECORDS**		**14**
14	**ADULTS WITHOUT CAPACITY**		**14**
15	**ACCESS TO THIRD PARTY RECORDS**		**15**
16	**REFUSAL**		**15**
17	**STAFF ACCESS TO RECORDS**		**15**
18	**POLICE (AND OTHER AGENCIES CONDUCTING CRIMINAL INVESTIGATIONS)**		**16**
19	**REQUESTS RELATING TO A PENDING LITIGATION CLAIM**		**16**
20	**COMPLAINTS & INTERNAL REVIEW**		**16**
21	**COMPLAINTS AND APPEALS**		**16**
22	**MONITORING AND REVIEW**		**17**
23	**EQUALITY IMPACT**		**17**

Appendix 1	**Access to Records Request Form**	**18**

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 (see 4.1)
- The right of access (formerly Subject Access rights) (see 4.2)
- The right to rectification (see 4.3)
- The right of erasure (see 4.4)
- The right to restrict processing (see 4.5)
- The right to data portability (see 4.6)
- The right to object (see 4.7)
- Rights in relation to automated decision making and profiling (see 4.8)

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 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.

1.4 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.

2. PURPOSE

2.1 The purpose of this policy is to provide guidance on the general principles of information rights and establish a process to manage all requests for the release of personal data from:

- Living individuals under the Data Protection Act (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 (AHRA)
- Legal representative on behalf of beneficiaries of a deceased individual under the AHRA

2.2 It defines the legislative requirements which govern the above types of requests and supports staff to identify which process to apply to each type of request.

2.3 This policy should be read in conjunction with NHS Norfolk & Waveney Integrated Care Board's (ICB) IG Strategy and Framework 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 This policy applies to any request raised by a patient, a parent or legal guardian, member of the public, member of staff and/or legal representative(s) in relation to personal data held by the ICB and used for its processing activities. This policy does not relate to information held by GP Practices and/or provider organisations.

3.2 Application of this policy applies to all staff (substantive, temporary and seconded to the ICB), contractors, members of the Board and clinical advisors.

3.3 This policy relates to personal data held in the following forms:

- Paper records, both current and archived regardless of the volume of records held
- Electronic records held within the ICB's IT network
- Personal data stored within an electronic system, such as a case management system, electronic staff record
- 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)
- Video recordings
- Audio recordings

3.4 This policy applies to all complaints files, personnel records, continuing healthcare files and all other documentation which makes reference to a living or deceased individual.

3.5 This policy does not cover requests for records generated by the Coroner's Court as a result of a Police enquiries. It also does not cover requests made by the Police. These types of requests should be referred to the Data Protection Officer.

3.6 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, as all requests for information which may result in a breach of the DPA, are exempt from disclosure under the Freedom of Information Act 2000.

3.7 This policy does not apply to requests for duplicate copies of information already provided by the ICB, or requests for anonymised information. These types of requests should be referred to the Data Protection Officer.

4. GENERAL PRINCIPLES OF INFORMATION & ACCESS RIGHTS

4.1 The Right to be Informed

The right to be informed encompasses the organisation's obligation to provide 'fair processing
information' and emphasises the need for transparency over how we use personal data. To meet our obligations, the ICB has two privacy notices – one for patient and service user information, and one for staff information – both of which 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**

This policy reflects the current legal and professional guidelines which underpin the processing and release of person identifiable data:

- UK General Data Protection Regulations (UK GDPR)
- Data Protection Act 2018 (DPA)
- Subject Access Code of Practice – Information Commissioner's Office

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).

All individuals have the right to obtain access to the information that the ICB holds about them. The ICB has published guidance on the intranet and public website for anyone wishing to invoke this right.

From the date of receiving the request, the organisation has one calendar month to provide the information. Therefore, it is imperative that requests are forwarded to the IG Team to process; nwICB.informationgovernance@nhs.net

The legislated timeframe may be extended to a maximum of three calendar months where the request is complex or numerous. If this is the case, the individual must be informed of this within the initial one-month compliance period, with an explanation as to why the extension is necessary and the likely response date.

The organisation must provide a copy of the information requested free of charge. The ICB is only permitted to charge a 'reasonable fee' where the request is manifestly unfounded or excessive (particularly if it is repetitive), or it relates to duplicate copies of information already provided. This fee must be based solely on the administrative cost of providing the information.

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 for the request to be processed.

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 2.4).

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 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 ensuring that the ICB only holds the minimum information necessary to justify its operational and statutory obligations. This will ensure that the ICB does not create unmanageable repositories of information which could have a negative impact on responding to an access request in a timely manner. Staff are also responsible for ensuring that information is stored in a structured and easily identifiable way in accordance with the Records Management Policy, so that it can be retrieved in a timely manner.

5.2 The IG Team has responsibility to ensure that requests for access to personal data under an access request are lawful and justifiable and the appropriate supporting documents have been provided.

5.3 The IG Team has operational responsibility for responding to all requests for access to personal data in respect of living and deceased individuals.

5.4 The Caldicott Guardian has executive responsibility for the release of personal data under a subject access request and the release of personal data relating to a deceased individual. As the Caldicott Guardian has a clinical background, they will be responsible for reviewing the final response, ensuring that the personal data has been appropriately and correctly redacted and authorise the release of the response.

5.5 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, refusals to release personal data and any associated complaints.

6. INFORMATION REQUESTS TO SUPPORT HUMAN RESOURCES

6.1 Requests for information can be made to the ICB in respect of HR matters such as

employment tribunals.

7. SUBJECT ACCESS REQUESTS (RIGHT OF ACCESS)

7.1 Subject Access 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

7.2 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.

7.3 It is imperative to review all information before it is released to the requester. The IG Team will therefore ensure that all references to a third party have been redacted (i.e., crossed through) 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.

7.4 To assist with the release of personal data, staff are responsible for 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).

7.5 Staff are also responsible for 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.

7.6 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. Please refer to the Freedom of Information Policy for further details regarding this.

8. ACCESS TO HEALTH RECORDS REQUESTS

8.1 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”.

8.2 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 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. 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.

9. IDENTIFYING WHICH LEGISLATION APPLIES

9.1 The ICB receives requests for the release of person identifiable data from a variety of sources, however, the majority of requests received are made to support an appeal against a Continuing Healthcare decision and/or process. Whilst we have a duty to respond to all requests, we have an overriding duty to ensure that personal data is only released in accordance with the DPA and AHRA. Staff are therefore required to understand which category the request for the release of personal data falls under:

- A. Does the request relate to a living individual? If Yes, it must be managed as a Subject Access request

- B. Does the request relate to a deceased individual? If Yes, it must be managed as an Access to Health Records request.

10. MAKING A REQUEST FOR ACCESS TO PERSONAL DATA

10.1 The data subject should be encouraged to use the Access to Records Request Form (Appendix A) to ensure that the ICB has sufficient information and verification of identity before processing a request, as we are legally obliged to ensure that requests are handling appropriately.

10.2 Personal Representatives, Powers of Attorney, parents, legal guardians and legal representatives acting on behalf of a patient or the Estate of a deceased individual should also be encouraged to complete the Access to Records Request Form (Appendix A). This will ensure that the ICB has sufficient information to process the request and avoid any potential delays.

11. RESPONDING TO A REQUEST

11.1 All requests for the release of the person identifiable data, whether relating to a living or deceased individual should be managed by the IG Team. If a member of staff receives a request for access to personal records / data, it must be forwarded to the IG Team to instigate the appropriate process as per Appendix B.

11.2 The DPA/GDPR or AHRA do not specify how to make a valid request. Therefore, to enable the ICB to manage their obligations effectively, requestors should be encouraged to make requests as per Appendix A.

11.3 All requests for access to personal records will be managed in accordance with Appendix B of this policy to ensure that the ICB adheres to the statutory timeframe and maintains a log of all requests received, in accordance with the guidance issued by the Information Commissioner's Office (ICO).

11.4 The ICB will provide a response to the request within one calendar month in line with DPA. However, the timeline will not start, unless:

- any required fee has been paid, if applicable. (Refer section 13)
- the identity of the requestor has been verified and the legitimacy of the request has been confirmed.
- sufficient details have been supplied to locate the information.

11.5 If the one calendar month time limit is insufficient to meet the full needs of the request, the applicant should be informed as soon as this is identified, and in any case before the initial deadline date of one calendar month. An extension to the deadline may be applied of up to two calendar months, and this should be communicated in writing to the applicant. It may also be appropriate to consider a staggered approach to supplying the information, i.e., sending as and when identified rather than waiting until all information is fully collated.

11.6 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.

11.7 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 destroyed under confidential conditions if no longer required.

12. FEES

12.1 In most cases the ICB cannot charge a fee to comply with a request for access to personal data under DPA or AHRA.

12.2 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

12.3 The ICB's fees will be based on the administrative costs of complying with the request such as consumables, paper and postage.

12.4 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.

12.5 Where a fee remains appropriate, no work on the request will commence until the fee has been received.

13. CHILDREN'S RECORDS

13.1 For the purposes of disclosure of records, a child is a person who has not attained their 16th birthday at the time of the request. If the applicant is 16 or over their request should be treated a request from an adult in accordance with this policy. The parents or legal guardians of the applicant over 16 years are not entitled to see the records without the consent of the young person. The only exception to this is when the over 16 year old lacks capacity and the parent / legal guardian holds a Lasting Power of Attorney.

13.2 If the application is from a child that is under 16, the ICB may need to obtain parental authority to release the information, on the basis that the applicant is not authorised to make such a request under GDPR / DPA legislation. This will be achieved using the Access to Records Request Form (Appendix A).

13.3 However, the ICB will look sympathetically on a request from a child aged 12 -16 who is judged to be "Gillick Competent". Such a request will be managed by the Data Protection Officer and Caldicott Guardian.

14. ADULTS WITHOUT CAPACITY

14.1 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.

14.2 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.

14.3 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 request.

15. ACCESS TO THIRD PARTY RECORDS

15.1 On occasion, the ICB will receive requests for information that is owned by a Third Party as a Data Controller.

15.2 In these instances, we will advise the data subject that we are unable to release this information but provide the relevant contact details to enable the data subject to raise a further request direct with the relevant Data Controller.

15.3 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.

16. REFUSAL

16.1 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 13 above).

16.2 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.

16.3 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.

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

17. STAFF ACCESS TO RECORDS

17.1 Staff should not look up or amend their own record as it could be construed 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 for them to do so, in

line with their job description and contract of employment. If this situation occurs, the member of staff should inform an appropriately senior manager who will then assess the impact and risks and may allocate another member of staff to the relevant tasks.

18. POLICE (AND OTHER AGENCIES CONDUCTING CRIMINAL INVESTIGATIONS)

18.1 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. The police will need to submit their request, to the IG Team, in writing, detailing what data they require for what purpose and with a crime reference number.

19. REQUESTS RELATING TO A PENDING LITIGATION CLAIM

19.1 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)

20. COMPLAINTS & INTERNAL REVIEW

20.1 Applicants can ask the ICB for an internal review if they are not content with the information being released. This is the first review stage for applicants.

20.2 If a complaint is received from a dissatisfied applicant, the recipient must contact the IG Team who will confirm to the applicant that the request for review has been received and indicate to them when they should expect a response.

20.3 The IG Manager/Data Protection Officer will carry out the internal review unless they were involved in the processing of the original request (either as provider of information provider or in the decision-making process) in which case an alternative member of staff within the IG Team will perform the internal review.

20.4 The internal review must be a fair and impartial review of the decisions made during the original consideration of whether to release information. All internal reviews must consider the information released against the information requested and make a full review of the papers associated with the original application.

20.5 The internal reviewer will discuss the decisions made with the staff member, or members, who dealt with the original application to build a full picture as to how decisions were made.

20.6 The applicant must be fully informed of the outcome of the internal review. To assist in any further investigations by the Information Commissioner, full records of the review must be kept.

21. COMPLAINTS AND APPEALS

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

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

21.2 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
Online: Contact us | ICO

22. MONITORING AND REVIEW

22.1 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.

22.2 The Audit 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.

23. EQUALITY IMPACT

23.1 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: Access to Records Request Form

The Access to Health Records Act 1990 and Data Protection Act 2018 give patients/clients/staff or their representatives a right of access, subject to certain exemptions, to their health records. NHS Norfolk and Waveney Integrated Care Board (ICB) respects the rights of individuals to request copies of personal data, where there is a legitimate basis for the request.
Personal data collected from you by this form, is required to enable your request to be processed, this personal data will only be used in connection with the processing of the Request for Access to Records.
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 – Illegible forms will delay the time taken to respond to requests.										
1.	**Details of the Data Subject (i.e. the subject of the personal data requested)** (Please complete one form per person)									
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
If further details are available please include in a separate covering note.										

2.	**Details of Records to be Accessed**
In order to locate the records you require please provide as much information as possible. Please list the department or services you have 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** / /	

3.	**Details of applicant** (Complete if different to patients/clients/staff members details)
Full Name:	
Company (if Applicable):	
Address:	
Email address:	
Contact telephone number:	
Is the request related to a living individual (data subject)?	**Yes ☐ No ☐**
Are you the Parent / Legal Guardian of the living individual (data subject)	**Yes ☐ No ☐** If Yes, please provide a copy of the data subject's **Birth Certificate** or **evidence that you are the legal guardian**.
Are you Power of Attorney for the living individual (data subject)	**Yes ☐ No ☐** If Yes, please provide a copy of the **Power of Attorney**. This is required in order to proceed with a request under the General Data Protection Regulations / Data Protection 2018
Are you the Legal Representative of the living individual (data subject)	**Yes ☐ No ☐** 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 Regulations / Data Protection 2018
Is the request related to a deceased individual?	**Yes ☐ No ☐**
Do you have a claim arising from the deceased individual's Estate:	**Yes ☐ No ☐** 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 ☐ No ☐** If Yes, please provide a copy of the **Grant of Probate**. 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 (data subject)	**Yes ☐ No ☐** 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**

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.

Signature of patient/client/staff member **:**_____**Date:** / /

5.	**Correspondence Address**
Address for receipt of final response including personal data. Please note only one response will be provided. A charge will be levied for additional copies	**Postcode:** **Tel:**

6.	**Declaration (to be completed by the Applicant)**

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).

Please select one box:

☐ I am the patient/client/staff member (data subject)

☐ I am the parent/guardian of the data subject

☐ I am the Power of Attorney for the data subject

☐ I am the Personal Representative of the data subject

☐ I am the Legal Representative of the data subject

☐ 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).

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 (i.e. Driving Licence).
- 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 removed; 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.

Print Name	
Signed (Applicant)	
Date	

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

Email: nwicb.informationgovernance@nhs.net