


Information Requests Policy

DOCUMENT CONTROL

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the website.

 Do you really need to print this document?

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

Document Owner:	Chief Officer	
Document Author(s):	Tania Palmariellodiviney	
Version:	V1.0	
Approved By:	Operational Executive Team	
Date of Approval:	14 August 2023	
Date of Review:	2 years from the date of approval	
Link to Strategic Objective(s):	Increase healthy, life expectancy, and reduce inequality	<input type="checkbox"/>
	Improve access to health and care services	<input checked="" type="checkbox"/>
	Increase the numbers of citizens taking steps to improve their wellbeing	<input type="checkbox"/>
	Achieve a balance financial position annually	<input type="checkbox"/>
	Give every child the best start in life	<input type="checkbox"/>



CHANGE HISTORY

Version	Date	Reviewer(s)	Revision Description
0.1	March 2023	Tania Palmarielloviney/ DPO	Draft – replaces 'Access to Information Policy'
1.0	August 2023	N/A	Final – approved by Executive Team



CONTENT

Section No.		Page No.
1	Introduction – Purpose, Scope and Definitions	3
2	Purpose	3
3	Scope	3
4	Definitions	3
5	Roles and Responsibilities – Implementation and Monitoring	5
6	Implementation	6
7	Monitoring	6
8	Freedom of Information Requests (FOIs)	7
9	Environmental Information Regulation (EIR)	8
10	Freedom of Information Requests – flow chart	9
11	Subject Access Requests (SARs)	10
12	Subject Access Request – flow chart	14
13	Other Information Rights Requests	15
14	Information of Deceased Patients	17
15.	Fees	19
Appendices	Appendix 1 – Response times and Extensions	20
	Appendix 2 – Exemptions and Fees	21
	Appendix 3 – Main Differences between FOI and EIR	22
	Appendix 4 – Other third-party requires under UK GDPR and AHRA	23
	Appendix 5 – Acceptable verification and ID	24
	Appendix 6 – Children’s Medical Information – Handling Parental Requests	25
	Appendix 7 – Equality Impact Assessment and Health Inequality Impact Assessment	26



1. INTRODUCTION

- 1.1 NHS Hertfordshire and West Essex Integrated Care Board (HWE ICB) is committed to ensuring full compliance with all Data Protection (DP) and Information Governance (IG) related laws, legislation and guidance, which plays a vital part in the provision of a consistently high level of health and care service delivery.
- 1.2 Information requests in relation to this document are any requests for information under UK GDPR, Data Protection Act 2018 (DPA 2018), Access to Health Records Act 1990, Freedom of Information Act (FOIA), Environmental Information Regulations (EIR) and other requests for information that the ICB may be obliged to provide access to under UK law.

2. PURPOSE

- 2.1 The purpose of this policy and the procedures outlined within, is to:
- (a) Define the steps that must be taken when receiving information requests
 - (b) Set a clear and consistent standard for managing information requests
 - (c) Ensure legal compliance in relation to information requests

3. SCOPE

- 3.1 This policy applies to:
- (a) All ICB staff members, including the Board and Practice Representatives, involved in the ICB's policy-making processes, whether permanent, temporary or contracted-in (either as an individual or through a third-party supplier).

4. DEFINITIONS

- 4.1 The following keys apply in the context of this policy:

Term	Definition
FOIA	Freedom of Information Act 2000
FOI	Freedom of Information
UK GDPR	United Kingdom General Data Protection Regulation
DPA 2018	Data Protection Act 2018
EIR	Environmental Information Regulation 2004
AHRA	Access to Health Records Act 1990
ICB	Integrated Care Board
HWE	Hertfordshire and West Essex
DP	Data Protection
IG	Information Governance
DPO	Data Protection Officer
SAR	Subject Access Request



5. ROLES AND RESPONSIBILITIES

5.1 The following definitions apply in the context of this policy:

Role	Responsibilities
Chief Executive	The Chief Executive has overall responsibility for information governance within the ICB. The Chief Executive is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
Board Members	The ICB is ultimately responsible for decisions made regarding Access to Information requests. Board members of the ICB are responsible for ensuring that information held by them and their teams is up to date and accessible and for ensuring a timely response is made to enquiries under the FOIA.
DPO	The Data Protection Officer reports directly to the (most senior level of management), in matters relating to data protection assurance and compliance. The DPO operates independently.
Head of IG & Risk	The role of the Head of Information Governance and Risk is to be responsible for strategic and operational management of the Corporate Risk Management and Information Governance Functions, and leads in the development, interpretation and implementation and monitoring of the Risk Management and Information Governance Frameworks, in support of the achievement of the Organisations Strategic and Corporate Objectives.
Governance Manager Information Governance	The Governance Manager (IG) is responsible for the ICB's Publication Scheme, FOI Policy and processing of FOIs, Environmental Regulations, Information Rights and Access to Health Records requests. This includes day to day responsibility for the FOI Act, the General Data Protection Regulation, Data Protection Act and Access to Health Records Act and for ensuring that deadlines are met.
Senior Information Risk Owner (SIRO)	The role of Senior Information Risk Owner (SIRO) in the ICB has been assigned to the Chief Finance Officer (CFO). The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the ICB Governing Body and Quality and Governance Committee. This includes oversight of information security incident reporting and response arrangements. The Senior Information Risk Owner will act as the ICB's appropriate 'qualified person' in relation to the application of Section 36 of the FOIA (an exemption in relation to the prejudice to the effective conduct of public affairs).
Caldicott Guardian	The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing. For the ICB, this has been assigned to the Director of Quality and Nursing. Acting as the 'conscience' of the



	organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.
Information Asset Owner (IAO)	Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.
Information Asset Administrator (IAA)	Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.
Chief of Staff	The Chief Executive has delegated operational responsibility for information governance to the Chief of Staff.

6. IMPLEMENTATION

- 6.1 This policy will be made available via the HWE ICB intranet. It will be implemented by the Head of Information Governance and Risk and its implementation will be monitored by the ICB DPO.
- 6.2 The Chief of staff is responsible for ensuring that appropriate information request training is made available to staff, depending on their role and that training aligns with this policy. Refresher training must be completed by all staff yearly or as and when legislation or guidance is amended.
- 6.3 Failure to adhere to this policy and to comply with training requirements may result in disciplinary action.

7. MONITORING

- 7.1 Compliance of this policy will be monitored by the ICB DPO, who will report back to the ICB Board, via regular audits. Any nonconformities will be reviewed, actioned and any organisational learning shared appropriately.
- 7.2 The ICB DPO is responsible for reviewing the policy annually and as and when legislation or official guidance may change.



8. FREEDOM OF INFORMATION (FOI) REQUESTS

8.1 Receiving a request

8.1.1 A FOI request can be recognised by the information requested. If it is not relating to personal information of an individual, the information is likely to fall under the Freedom of Information Act 2000 (or Environmental Information Regulations 2004 (EIR); see end of this section).

8.1.2 A valid request under FOI must meet the specific criteria. It must:

- (a) be in writing (requests for environmental information can be verbal and fall under EIR)
- (b) provide the name of the requester and a contact address (email or postal address)
- (c) describe the information which is requested

8.1.3 A request does not have to explicitly cite 'FOI' or 'EIR'.

8.1.4 The following should not be interpreted as a valid FOI request:

- (a) requests not requesting recorded information (asking for opinions, press statements, making a complaint, etc.)
- (b) requests from an individual for information about themselves. This should be treated as a Data Protection Subject Access Request
- (c) routine or business as usual requests which you would respond to as a matter of course.

8.2 Response time

8.2.1 It is a legal requirement to respond to a request within 20 working days, starting from the next working day after the request is received by any member of ICB staff (not the FOI Officer).

8.2.2 Where further information is necessary, this should be requested without undue delay and the response time starts the following day from when the information has been received (*Appendix 1: Response time and extensions*).

8.3 Managing a request

8.3.1 Requested information must be disclosed unless a legally valid exemption or other exclusion applies and regardless of the outcome, a response must be sent. (*Appendix 2: Exemptions*).

8.3.2 All FOI requests must be forwarded to the FOI team without undue delay, using the following email address: hweicbhv.foi@nhs.net . Once the request has been received, the ICB FOI team will send an acknowledgement email/letter to the requestor, using the ICB's template.

8.3.3 The department who holds the information is ultimately responsible for dealing with an FOI request and the person receiving the request is ultimately responsible for informing the FOI team if they do not hold the information. In this case, the FOI team will locate the appropriate team to deal with the request.



- 8.3.4 It is everyone's responsibility to identify a FOI request and follow the procedures as set out in this policy.
- 8.3.5 The person/team dealing with the request must have their own notification process in place to ensure that a request is responded to within the legal timeframe – this process would include a central email address where requests such as this are sent to or a nominated lead to coordinate a response from within the team.
- 8.3.6 In straight forward cases, the information should be gathered and sent to the FOI team for Director sign-off, with the ICBs formal response being securely sent to the requestor, using the ICB's response template.
- 8.3.7 When collating the information, it is important to note that ALL recorded information is included – the ICBs Head of Information Governance and Risk or relevant colleague will determine whether an exemption or similar can be applied.
- 8.3.8 In cases of non-engagement with the FOI Teams directions this will be escalated to the Chief of staff and relevant Director.
- 8.3.9 The right of access under the Freedom of Information Act (FOIA) and the Environmental Information Regulations (EIR) extends to all recorded information held by the ICB, regardless of the format or storage medium.

8.4 Refusing a request

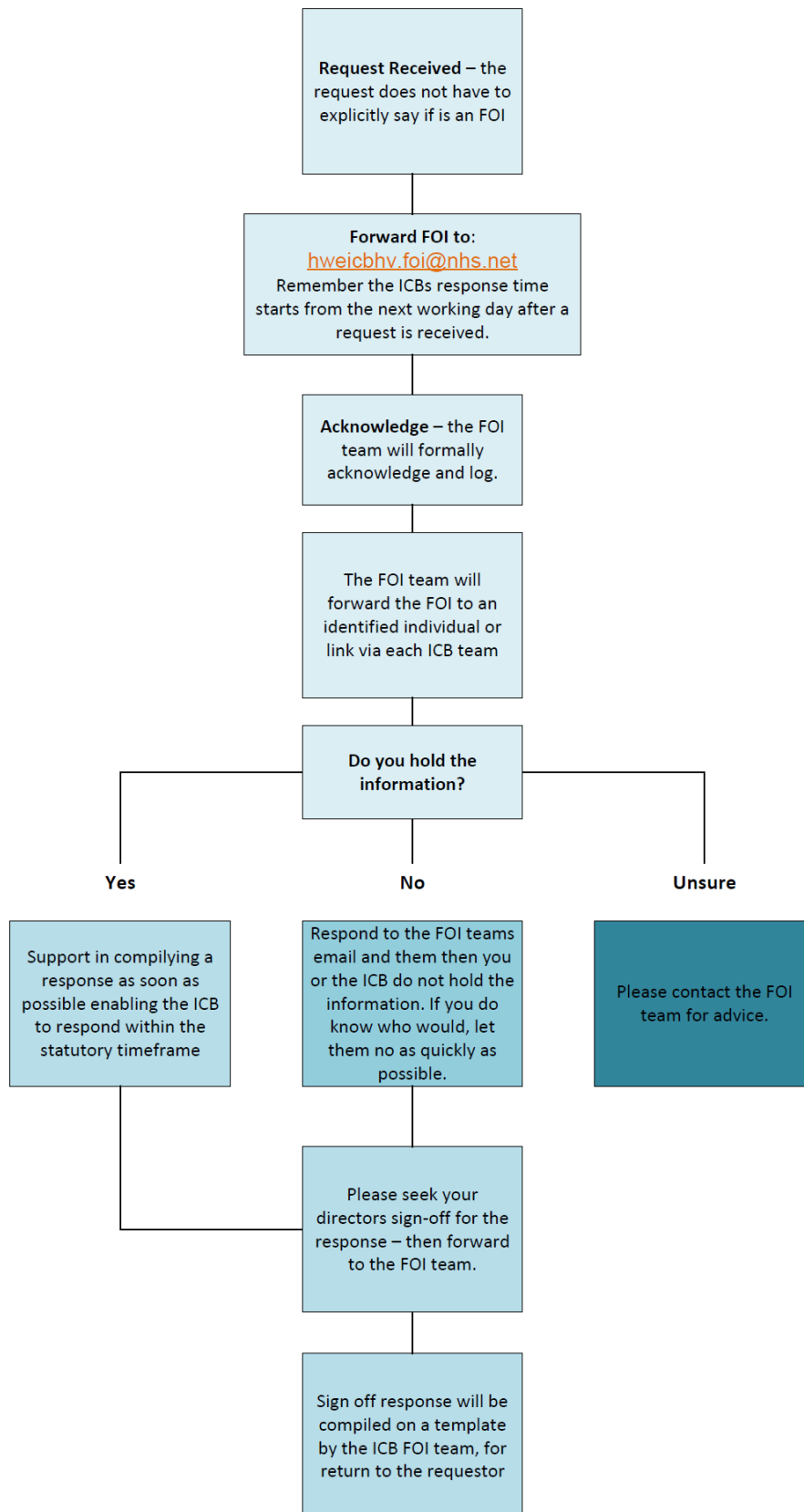
- 8.4.1 Where an exemption or partial exemption applies, an exemption response should be sent to the requestor, detailing the exemption and reason for the exemption, using the ICB response template.
- 8.4.2 All response letters should give requestors the option and outline the right to:
- (a) Ask for an internal review
 - (b) Make a complaint to the ICO; and
 - (c) Seek to enforce their right through a judicial remedy
- 8.4.3 All refusals to provide information requested must be approved by the ICB Data Protection Officer or an identified individual within their team.

9. ENVIRONMENTAL INFORMATION REGULATION (EIR)

- 9.1 When requested information is environmental – for example, information about land development, pollution levels, energy production, and waste management, the EIR applies. Requests are managed similarly to FOI requests; however, they do not need to be in writing.
- 9.2 Mostly, the conditions are the same as FOI requests with some slight differences which only apply in certain circumstances such as, where a request is not straight forward. Where this is the case, consultation with the ICB IG Team should be sought in any case (*Appendix 3: Main differences between FOIA and EIR*).



10. FOI (EIR) Request Flowchart



11. SUBJECT ACCESS REQUESTS (SARs)

11.1 Receiving a request

- 11.1.2 A SAR can be recognised by the information requested. It is a request for information that you hold about a living individual (See AHRA section for information about deceased patients).
- 11.1.3 A SAR request does not have to meet any specific criteria. It can be made verbally, in writing and via any channel of communication to anyone working within the ICB and does not have to state any legislation or that it is a SAR or Right of Access request. It should be clear that a request is made to access personal identifiable information about a living individual.

11.2 Who can make a request?

- 11.2.1 Requests may come from the individual themselves or a third party. Third party requests are valid requests and dealt with in the same way as if the individual was making the request, except that consent or another legal basis for requesting the information must be present. The response should always be sent to the requestor. (Appendix 4 for third party requests)

11.3 Response time

- 11.3.1 It is a legal requirement to respond to a SAR within a calendar month, starting from when you receive the request and ending on the corresponding calendar date in the next month.
- 11.3.2 Where further information is necessary, this should be requested without undue delay and the response time starts once this information has been received. Extensions may be applied in complex cases; however, extensions must be approved by the DPO.
- 11.3.3 Requested information must be disclosed unless a legally valid exemption or other exclusion applies. Redactions may be applicable to comply with other legal obligations such as to protect third party information. (Appendix 2 for exemptions, Redactions, list of third-party examples).

11.4 Managing a request

- 11.4.1 The department who holds the information is ultimately responsible for dealing with a SAR request and the person receiving the request is ultimately responsible for informing the IG team if they do not hold the information. In this case, the IG team will locate the appropriate team to deal with the request.
- 11.4.2 It is everyone's responsibility to identify a SAR and follow the procedures as set out in this policy. Note that requestors do not have a legal obligation to fill in any forms in relation to their request. (This may be different for third parties, i.e., law enforcement)
- 11.4.3 All SAR requests must be forwarded to the Information Governance Team (IG Team) without undue delay, using the following email address:
hweicbhv.sar@nhs.net.



- 11.4.4 The IG Team will maintain a log of SAR's; ensure that the required identity documentation and in cases of a third-party request ensure that the required consent or legal basis has been provided; and acknowledge the request, using the ICB's template. and if required request any further information needed to begin the process e.g., proof of identity/consent/legal basis/clarification of what information is being requested etc. if this has not already been established, (Appendix 5 for acceptable evidence from Requestor).
- 11.4.5 The IG Team will then request information from the departments who hold this. It is the departments responsibility to then extract and collate the information, redact third party information (Health or social care professionals who have been involved in providing care to the patient are not regarded as third parties, however if there is reason to believe that including their information may cause harm to them or anyone else, their information may be redacted). If more than one department holds information the departments will need to decide who is leading on this and send the collated and redacted documents to the IG Team. If the departments do not hold any information about the request they must inform the IG team. If there are any potential difficulties in collation or redaction then the departments must discuss this with the IG team who will be able to advise.
- 11.4.6 Please note that redactions apply in many cases. Redactions apply to any third-party identifiable information unless they have given consent. It is not our responsibility to get consent from third parties where their information is part of a SAR. This needs to be discussed with your Caldicott Guardian.
- 11.4.7 When collating the information, it is important that:
- (a) All recorded information is included (The right of access under UK GDPR and DPA 2018 extends to all recorded information held by the ICB, regardless of the format or storage medium)
 - (b) Necessary redactions have been applied and reasons given
 - (c) Necessary exemptions have been applied and reasons given
 - (d) The records have been checked for safeguarding notes/concerns and actioned accordingly
 - (e) The information is being sent to the right person and safely and securely according to ICB policy
 - (f) If information is being sent to a third party, the data subject has given consent and understands what they have given consent to (i.e. they are aware of all types of information that is being shared)
 - (g) Where consent is not there, there is legal justification to release the information anyway (i.e. court order)
- 11.4.8 The IG Team will send the information provided by the departments securely to the requestor, using the relevant ICB's response template. (Unless an exemption applies).
- 11.4.9 The requestor should be kept informed in case an extension to the deadline is applied or if further information is required and the new deadline for their request. Where further information is required, the response time pauses until the information has been received.



11.4.10 All response letters should give requestors the option and outline the right to:

- (a) Ask for an internal review
- (b) Make a complaint to the ICO; and
- (c) Seek to enforce this right through a judicial remedy

11.4.11 All refusals to provide information requested must be approved by the ICB DPO>

11.5 CCTV Footage

11.5.1 Access to personal data as part of a SAR must be forwarded to hweicbhv.sar@nhs.net.

Due to the cost implication of editing footage (to ensure redaction of third-party data) you might be unable to release CCTV footage as part of a SAR.

11.5.2 The requestor will be informed of this in writing within the 30-day time limit by the IG team. A viewing of CCTV footage may be offered instead if within the time limit in an area made private for the purposes of viewing footage only as recommended by the ICO.

11.5.3 If the requestor refuses the offer of viewing the footage, then relevant team may produce a report or transcript of the recording. However, this should not be offered instead of viewing. The ICB IG team will ensure a log is kept of all requests and the resulting decision.

11.5.4 All decisions made in relation to requests for CCTV footage must be discussed and approved by the ICB DPO.

11.6 Refusing a Request

11.6.1 Where an exemption or partial exemption applies, an exemption response should be sent to the requestor, detailing the exemption and reason for the exemption, using the ICB response template.

11.6.2 All response letters should give requestors the option and outline the right to:

- (a) Ask for an internal review
- (b) Make a complaint to the ICO; and
- (c) Seek to enforce this right through a judicial remedy

11.7 Third party requests

11.7.1 A data subject may instruct a third party on their behalf, in which case a response should be supplied to said third party. Evidence of consent by the data subject must be sought before the request is actioned (See Appendix 4: Other third-party requests under UK GDPR & AHRA).

11.8 SARs for Children

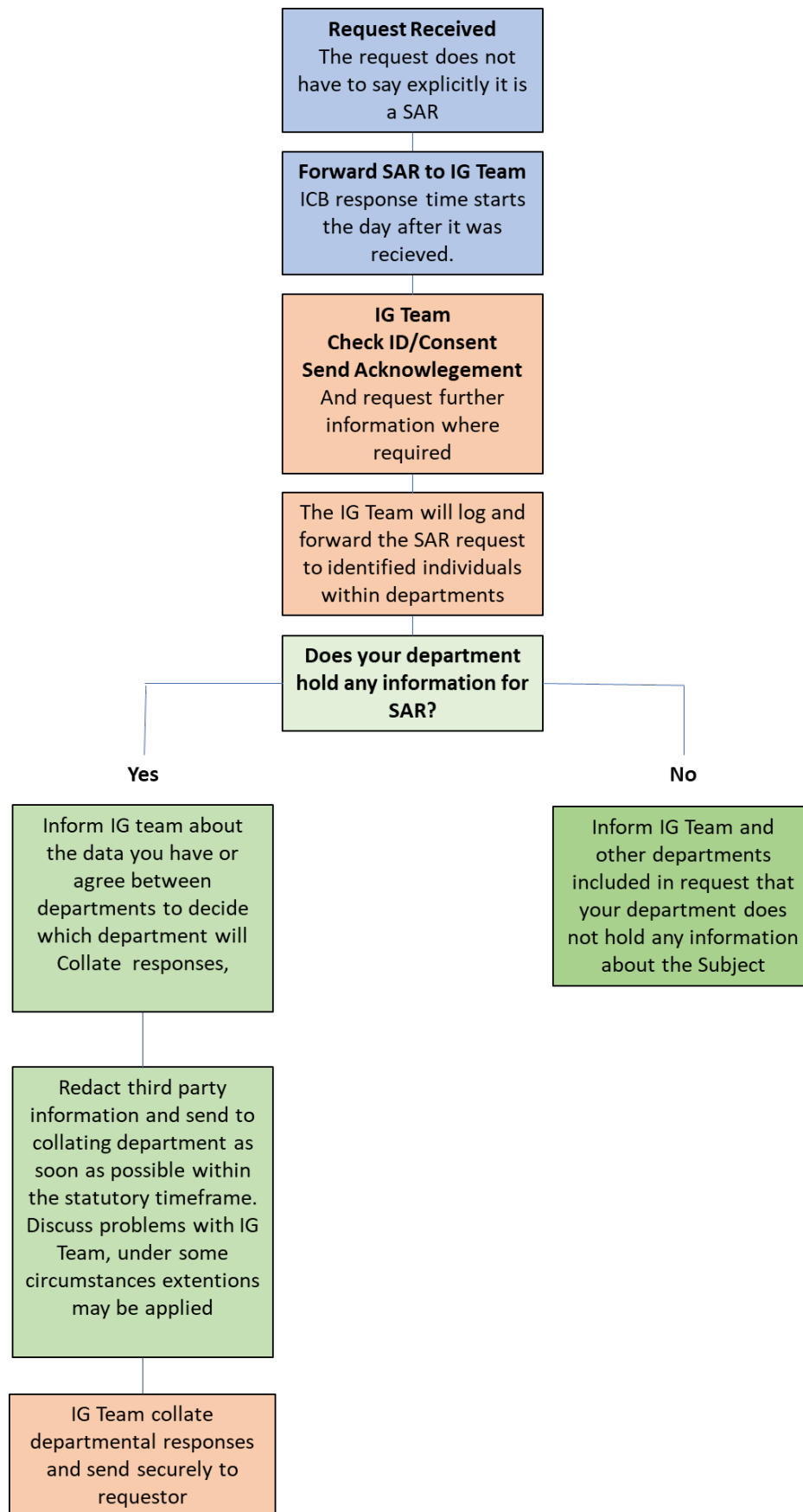
11.8.1 Children's information belongs to them, however where they lack capacity due to age, medical conditions or maturity, anyone with parental responsibility may access their information and act on their behalf.



- 11.8.2 When addressing SARs for children, it is important to establish who has parental responsibility and check all records for any safeguarding concerns or reasons not to share the information with parents.
- 11.8.3 Where there are authorities are involved, such as social services, they should be consulted.
- 11.8.4 Where there are any concerns over releasing children's information, the advice from a Caldicott Guardian must be sought. Where parents share responsibility but are no longer together, we set out advice in Appendix 6: Children's Medical Information – Handling Parental Requests.



12. SAR Flowchart



13. OTHER INFORMATION RIGHTS REQUESTS

SARs are only one of the eight individual rights under UK GDPR. All other information requests follow the same format and conditions to that of SARs, except that instead of information, an action is required.

Due to the complexity of these requests within the Health and Care sector, any Information Requests that are not The right to be informed OR The right of access (SAR) should be assessed by the IG Team before responding.

It will still be your responsibility to manage the request and send a response to the requestor.

13.4.1 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR and is reflected in the ICB's privacy statement. The information should be made available upon request and without undue delay.

13.4.2 The right to rectification – amending incorrect/update information

An individual can make a request for rectification verbally or in writing. In cases where the requestor does not agree with clinical opinions, it is not always appropriate to rectify this, but objections should be noted.

13.4.3 The right to erasure – request to delete information

This right only applies to data, where:

- (a) consent is required before data is collected, used or stored
- (b) when consent has been withdrawn and there is no other legal ground for processing
- (c) the data is no longer necessary for the purposes for which it was collected

Note - Where patient data is collected for direct medical care and staff data is collected for direct employment, consent is not used as the legal basis for collecting, using or storing data and therefore this right does not apply. (Appendix Exemptions)

13.4.4 The right to restrict processing – limiting the way data is used

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. (See exemptions)

13.4.5 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.

13.4.6 The right to object – objection to process an individual's information

The right to object to the processing of their personal data applies in certain circumstances. The only absolute right in this regard is that an individual has the right to object stop their data being used for direct marketing.



13.4.7 Rights in relation to automated decision making and profiling

This type of decision-making can only be carried out where the decision is: necessary for the entry into or performance of a contract; or authorised by domestic law applicable to the controller; or based on the individual's explicit consent.



14. INFORMATION OF DECEASED PATIENTS

- 14.1 Although the Access to Health Records Act 1990 (AHRA) has been replaced by the DPA 2018 and UK GDPR in relation to *living individuals*, the AHRA remains in place and must be complied with for access to health records requests of *deceased patients*.
- 14.2 Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes, photographs, and tissue samples taken for diagnostic purposes.
- 14.3 They may also include reports written for third parties such as insurance companies. Unlike a SAR, a AHRA request only covers information within the health record of the deceased. It is also important to note that the duty of confidentiality still applies beyond a person's death.

14.4 Receiving a request

- 14.4.1 A AHRA request can be recognised by the information requested. It is a request for information that you hold about a deceased individual.
- 14.4.2 A AHRA request does not have to meet specific criteria, it does not have to state any legislation or that it is a AHRA request, however it should be made in writing.

14.5 Who can make a request?

- 14.5.1 Unless the patient requested confidentiality while alive, only their personal representative and any other person who may have a claim arising out of their death has a right of access to information in their records.

14.6 Response time

- 14.6.1 If no entries, additions or amendments have been made to the record in the 40 calendar days prior to the date of the request, the response time is 21 calendar days from the date of receiving the request.
- 14.6.2 If entries, additions or amendments have been made to the record in the 40 calendar days prior to the date of request, the response time is 40 calendar days from the date of receiving the request.
- 14.6.3 Where further information is necessary, this should be requested without undue delay and the response time starts once the information has been received.

14.7 Managing a request

- 14.7.1 Only information which is directly relevant to a claim should be disclosed. Redactions may be applicable to comply with other legal obligations such as to protect third party information. UK GDPR still applies if the information requested contains information about living individuals.
- 14.7.2 All AHRA requests must be forwarded to the IG Team without undue delay, using the following email address: hweicbhv.foi@nhs.net. This is for tracking and logging purposes only.



- 14.7.3 The department who receives the request is ultimately responsible for dealing with the request and this includes responding to the requestor if they do not hold any of the requested information.
- 14.7.4 It is everyone's responsibility to identify a AHRA request and follow the procedures as set out in this policy.
- 14.7.5 Once the request has been received, the receiver should send an acknowledgement email/letter to the requestor, using the ICB's template and AHRA request application form, asking for evidence of the requester that they have the right to access the requested information. We have 14 days to request further information from the requester. The response time begins once we have received all information needed to action the request. (Appendix for acceptable evidence from Requestor).
- 14.7.6 In straight forward cases, the information should be gathered and sent securely to the requestor, using the relevant ICB's response template, unless an exemption applies.
- 14.7.7 Redactions may apply to any third-party identifiable information unless they have given consent. It is not our responsibility to get consent from third parties where their information is part of a health record. Care professionals who have been involved in providing care to the patient are not regarded as third parties, however if there is reason to believe that including their information may cause harm to them or anyone else, their information may be redacted. This needs to be discussed with your Caldicott Guardian.
- 14.7.8 When collating the information, it is important that:
- (a) Only the medical record has been included and only what is necessary in relation to the claim
 - (b) Necessary redactions have been applied
 - (c) Necessary exemptions have been applied and reasons given
 - (d) The records have been checked for any wishes from the deceased person and/or any notes/concerns in relation to the release of the information have been considered
 - (e) The information is being sent to the right person and safely and securely according to ICB policy
 - (f) If information is being sent to a third party, the person with authority has given consent
 - (g) Where consent is not there, there is legal justification to release the information anyway (i.e. court order)
 - (h) All response letters should give requestors the option and outline the right to:
 - (i) Ask for an internal review
 - (j) Seek to enforce this right through a judicial remedy

14.8 Refusing a Request

- 14.8.1 There are cases where a request may be refused in full or partially. This may be because there are concerns that releasing the information or some of it may cause serious emotional or physical harm to someone, or because the patient did not wish for any of their information to be released.



14.8.2 Where this is the case, this should be discussed with the Caldicott guardian and any refusals to provide information must be approved by the ICB DPO and justified under relevant legislation.

14.8.3 All response letters should give requestors the option and outline the right to:

- (a) Ask for an internal review
- (b) Make a complaint to PCSE; and
- (c) Seek to enforce this right through a judicial remedy

14.9 Requests from Third Parties

14.9.1 Requests from third parties authorised by a personal representative and any other person who may have a claim arising out of their death should be dealt with in the same way as if it was the personal representative or other person who may have a claim arising out of their death, as long as they can evidence consent. The response should then be sent to the third party. There are other third parties that may make a claim; (*see Appendix 4 for further information*).

15. FEES

Information requests do not generally incur a fee and should be given free of charge. There are some exceptions where requests are not as straight forward and where excessive information may be requested or where the costs incurred to the organisation may be disproportionate.

These are rare circumstances and mostly apply to FOI requests. Appendix 2: Exemptions and Fees provides more information in relation to fees. Where fees may be charged, this needs to be signed off by the IG Team.



Appendix 1: Response times and Extensions

Type of Request	Applicable legislation	Response time	Pause	Extensions
Freedom of Information (FOI) Request	Freedom of Information Act 2000 (FOIA)	Promptly and within 20 working days from receipt of request.	Response time starts when all information to process the request has been received.	Where more time is required to determine whether the balance of the public interest lies in maintaining an exemption; or • further time to consider whether it would be in the public interest to confirm or deny whether the information is held is required. Time not specified but ICO recommends no more than extra 20 working days .
Environmental Information Regulation Request	Environmental Information Regulation (EIR)	Within 20 working days from receipt of request.	Response time starts when all information to process the request has been received.	Legislation has provision to extend the response time to 40 working days, but only for complex and voluminous requests.
Information Rights Requests including SARs	UK GDPR & Data Protection Act 2018 (DPA 2018)	Promptly and within 1 calendar month from date of receipt of the request; or within one month of receipt of any information requested to confirm the requester's identity.	Response time starts when ID has been received, however this should be requested promptly. Response time pauses where additional information is required.	Yes. By a further two months if the request is: complex; or you have received several requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.
Access to Medical Records of deceased patients	Access to Health Records Act 1990 (AHRA)	If the records were updated during the 40 days before request, within 21 days. If the records were updated more than 40 days before the date of request, within 40 days.	More information must be requested within 14 days of request. Response time starts when necessary information is received.	



Appendix 2: Exemptions & Fees

Type of Request	Exemption	Fees
FOI Requests	<p>Generally, exemptions may be applied if:</p> <ul style="list-style-type: none"> • It would cost too much or take too much staff time to deal with the request (costs exceeds £450. Equivalent to 18 hours of combined staff time). • The request is vexatious. • The request repeats a previous request from the same person. • If it would be contrary to the UK General Data Protection Regulation (the UK GDPR) or the Data Protection Act 2018 (the DPA2018), i.e. releasing personal data. • Releasing the information may impact research projects, crime investigations, or have any adverse effect on others in one way or another and/or may not be in the public interest. <p>All exemptions can be found in Part II of the FOI Act, at sections 21 to 44. https://www.legislation.gov.uk/ukpga/2000/36/part/II</p>	Where costs incurred exceeds appropriate limit of £450.
EIR Request	<p>Generally, exemptions may be applied if the request:</p> <ul style="list-style-type: none"> • Is manifestly unfounded. • Is formulated in too general a manner. • Against the interest of the protection of the environment • Would be contrary to the UK General Data Protection Regulation (the UK GDPR) or the Data Protection Act 2018 (the DPA2018), i.e., releasing personal data. • Releasing the information may impact research projects, crime investigations, or have any adverse effect on others in one way or another and/or may not be in the public interest. <p>All exemptions can be found in Part II of the EIR, at sections 12. https://www.legislation.gov.uk/ukxi/2004/3391/regulation/12/made</p>	Where reasonable and justified.
SARs and other Information Rights Requests	<p>Generally, exemptions may be applied if the request:</p> <ul style="list-style-type: none"> • Is manifestly unfounded; or • Is manifestly excessive. • Can cause harm to anyone • Would be contrary to other data protection principles <p>A list of all exemptions can be found here: https://www.legislation.gov.uk/eur/2016/679/contents</p>	Not usually. Only when manifestly unfounded, excessive, or repetitive.
AHRA requests	<p>Generally, exemptions may be applied if:</p> <ul style="list-style-type: none"> • The deceased did not want information to be released • Anyone involved in the care of the deceased patient believes that they did not want information to be released • The information, if released could cause harm to anyone • Would be contrary to other data protection principles <p>See the legislation for more information https://www.legislation.gov.uk/ukpga/1990/23/section/4</p>	No fees may be applied.



Appendix 3: Main Differences between FOIA and EIR

The main differences between FOIA and EIR are:

- ✓ The range of bodies covered by the EIR is wider to allow for consistency with the EC Directive and includes public utilities and certain public private partnerships and private companies, such as those in the water, waste, transport and energy sectors.

- ✓ Requests for environmental information need not be in writing.

- ✓ The information held by a public authority includes holding information held on behalf of any other person.

- ✓ The duty to provide advice and assistance requires a public authority to respond within 20 working days when requesting more particulars from the applicant.

- ✓ The time limits for responding to a request apply to ALL requests including those involving consideration of the public interest. Regulation 7 allows for an extension from 20 to 40 working days for complex and high-volume requests.

- ✓ No exception is made for requests that will involve costs more than the 'appropriate limit' within the meaning of the Fees Regulations made under sections 9, 12 and 13 of the FOIA. Except in specified limited circumstances, ALL requests must be dealt with, and any charges imposed must be reasonable.

- ✓ There are differences in the exceptions available under EIR and the exemptions available under FOIA.

- ✓ The requirement for public authorities to have in place a complaints and reconsideration procedure to deal with Code of Practice – Environmental Information Regulations 2004 February 2005 Code under Regulation 16 (with foreword) 5 representations alleging non-compliance with the EIR is mandatory.



Appendix 4: Other third-party requests under UK GDPR & AHRA

Court order

Any court orders for access to information must be complied with. (Solicitor requests are not court orders and must therefore be treated as a normal SAR request).

Coroners

Coroners (or their offices) have a legal right to access the records of a deceased individual to support their inquests. You must provide the information requested by the coroner.

Medical examiners

Medical examiners may request the records of deceased people for independent scrutiny. There is a legal basis for healthcare organisations to share relevant confidential patient information with medical examiners. This is covered by a section 251 approval following an application to the Confidentiality Advisory Group by NHS England.

The Care Quality Commission (CQC)

The CQC has a legal right to access the records of living and deceased people, where required in the course of its investigations. The CQC Code on Confidential Patient Information provides further information.

The Police

The police may request records of deceased people as part of their investigations. Where confidential information about a deceased person is required for a purpose beyond individual care, such as research, service evaluation or national clinical audit, the requester should obtain approval from the Health Research Authority, under section 251 of the NHS Act 2006.

Sharing information with family members or individuals close to a deceased patient

There are times when it is appropriate to share information with a family member or an individual close to the deceased. However, this would be outside the remit of AHRA, which would be in the form of a formal written request to access the record.

While the UK GDPR does not apply, the common law duty of confidentiality still applies to the health and care records of the deceased. The circumstances therefore need to be carefully considered and decisions justified. If the patient had authorised the sharing of information in their lifetime (for example, to enable someone to pursue a complaint on their behalf), then that sharing should continue. Sharing general information about a patient's death with those close to the patient where there is no reason to believe that the patient would have objected to such disclosure will be permissible. Where it is difficult to reach a decision, contact your Caldicott Guardian.

You should also consider the likelihood of the disclosure causing unnecessary harm or distress to the family; for example, a hereditary condition which is communicated without the involvement of an appropriate health and care professional but where sharing would be in the best interests of family members. In cases such as these, speak to an appropriate health and care professional about how best to communicate the information.

The likelihood of information sharing being of benefit to the family of the deceased should also be given careful consideration; for example, sharing certain information could reduce the emotional or mental harm experienced by grieving relatives.



Appendix 5: Acceptable verification and ID

UK GDPR states that “The controller should use all reasonable measures to verify the identity of a data subject who requests access”. There are no specific requirements for what documentation is required, however we list some examples below. If it is clear to you that the requestor is who they say they are, you do not need to request further information. There needs to be a documented process in place to record if and how identity and other evidence has been verified for each case. If you are not satisfied that the requestor is who they say they are you should use the below as guidance for what to request.

Request	ID	Other evidence
FOI & EIR	Not required	Not required
SARs and Information Requests	Birth Certificate & Current Photo ID Or Current Passport Or Current British Driver's licence	Not required
Access to Health Record of deceased patient	Birth Certificate & Current Photo ID Or Current Passport Or Current British Driver's licence	Probate Or Letter of administration (In some cases, this may not be needed, depending on clinician decision to disclose information to family members)
Parents requesting access to children information (they may only get access if children are not competent or have given consent) Records must be checked for potential safeguarding issues	Birth Certificate & Current Photo ID Or Current Passport Or Current British Driver's licence	Evidence of parental responsibility, this can be a copy of the child's birth certificate where the parent must be listed for evidence to be valid Or a court order



Appendix 6: Children's Medical Information – Handling Parental Requests

Where parents are no longer together, it is important to find the right balance in order to fairly handle requests to access the record of a child, deny access to such records, or amend them. A mother or father can **(a) request access** and/or **(b) seek to update, amend or add** to their child's medical record, or personal data contained within the record.

Whether you should act and, if so, how much you then disclose / update will come down to three key considerations:

- (a) Does the child have capacity?
- (b) Does the parent have parental responsibility?
- (c) Would disclosure / updating the record be in child's best interests?

Our responsibility is to the child and to their health. We must ensure that their right to confidentiality is respected. And we must also respect any genuine expectations of confidentiality from either parent.

If the child does have capacity and this has been declared by a clinician, then their consent must be sought in relation to releasing their information to their parents. If the child declines, then the information should not be shared, unless there is a good reason to do so and it may be harmful not to. A Caldicott Guardian should be involved in making this decision.

If the child does not have capacity (generally under the age of 12) then information may be shared with anyone who has parental responsibility, unless there are any safeguarding concerns on the system, or any member of staff is aware of any potential harm that may be caused by sharing the information.

Note: The other parent does not need and should not be notified of a request by another parent, unless there are concerns over anyone's safety. As an ICB it is not our responsibility to get involved in parent disputes and we must act only on information that we have.



Appendix 7: Equality Impact Assessment and Health Inequality Impact Assessment

Title of policy, service, proposal etc being assessed:

NHS Hertfordshire and West Essex Information Requests Policy

What are the intended outcomes of this work?

The policy is aimed at supporting the management and monitoring of Information Governance within the ICB, including Freedom of Information Act (FOI) requests, Subject Access Requests (SAR). These requests are based on statutory duties.

How will these outcomes be achieved?

The policy will be supported with wider organisational development.

Who will be affected by this work?

This policy is aimed at all staff and those working for or with the ICB.

Evidence

Impact Assessment Not Required

- The drafting and analysis of this policy has been based on external Information Governance advice, linking with colleagues managing requests and their completion, ensuring key areas of statutory compliance are met, and basing the process on the key principle of keeping the ask and approach simple.
- The method by which FOI and SAR requests can be made and are responded to is clearly documented through statute and regulator guidance (e.g. Information Commissioners Office) – therefore, reasonable adjustment can be made where possible, for those requesting seek support in having their request answered.

How will you share the findings of the Equality analysis? This can include sharing through corporate governance or sharing with, for example, other directorates, partner organisations or the public.

The completed EqIA will be published on the CCG website either as part of the report on the proposals or separately on the equality and diversity pages.



Monitor and Evaluation

4. How will you monitor and evaluate the effect of your work on health inequalities?

The policy will be kept under review and the process it supports. This impact assessment will be renewed at the point of policy review, unless a review is triggered earlier. In respect of process, the ICB is seeing month on month increases in FOI requests. We are not aware of complaints be raised over access with FOIs or SARs, however and as with all areas of the ICB, this will be kept a watch on and the ICB has a clear complaints process in place.

For your records

Name of person(s) who carried out these analyses:

Simone Surgenor – Deputy Chief of Staff – Governance and Policies

Redouane Serroukh – Head of Information Governance and Risk. DPO for the ICB

Date analyses were completed:

03.08.2023

Equality and Diversity Lead Sign off

The requirements of this proposal are set by statute and regulatory guidance. Therefor a full equality impact assessment is not required as the actions to be taken are not within the control of the ICB. The author has identified potential disability impact and a mitigating action. Paul Curry, Equality and Diversity Lead, 3 August 2023.

