

Access to Information Policy

Policy Reference: IG08

Brief Summary: This policy provides a framework for the CCG to ensure compliance with the Freedom of Information Act 2000 and to provide guidance for responding to Subject Access requests and Access to Health Records Act (1990) requests. It also covers the re-use of Public Sector Information Regulations 2005 and Environmental Information Regulations 2004.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
1.0	25/02/2015	Final	New document. This Policy replaces CCG FOI Policy Approved by West Essex CCG Board	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG's Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7 th October 2016
Next Review Date	March 2019
Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Contents

1. Introduction	3
2. Purpose	3
3. Scope	4
4. Definitions and Terms	5
5. Roles and Responsibilities	5
6. Process, Public Interest Test and Exemptions	8
7. Requests for an Internal Review	10
8. Personal Information and Records	12
9. Re-Use Regulations and Copyright	13
10. Charging and the Appropriate Limit	13
11. Duty to Advise and Assist	14
12. Individuals Who Can Make a Request	14
13. Subject Access Requests- the rights of individuals	15
14. Audit & Monitoring Compliance	18
15. Dissemination and Implementation	19
16. Training	19
17. Related Documents	20
18. Equality & Diversity	20
19. Key Contacts	21
Appendix 1 ~ Publication Scheme	22
Appendix 2 ~ Environmental Information Regulations 2004 (EIR)	23
Appendix 3 ~ FOI Request Process and Timescales	25
Appendix 4 ~ Exemptions under Part II of the Freedom of Information Act 2000	27
Appendix 5 ~ Summary of the FOI Fee Regulations 2004	28
Appendix 6 ~ Procedures - Receiving and Processing an Access to Health Records Request	32
Appendix 7 ~ SAR / AHRA Procedure	37

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

1. Introduction

NHS West Essex Clinical Commissioning Group (the CCG) is committed to openness and transparency in the conduct of all of its business. It has a duty to comply with all aspects of the Freedom of Information Act 2000 (FOIA).

The FOIA came into force at the beginning of 2005 and gives individuals or organisations rights of access to information held by public bodies, including the right to request information held by a public authority. The Act also places an obligation on public authorities to proactively publish information within a publication scheme, please see Appendix 1 for further information.

In addition, there are also regulations which provide access to environmental information; these are the Environmental Information Regulations 2004 (EIR). Requests under EIR will be treated as an FOI request as per this policy, except where the regulations drastically differ. Please see Appendix 2 for further information regarding the EIR and differences with the FOIA.

The CCG also has a duty to comply with the Data Protection Act 1998, which gives every living person (or their authorised representative) the right to apply for access to their own records, irrespective of when they were compiled; this is known as a Subject Access Request (SAR).

The Data Protection Act 1998 supersedes the Data Protection Act 1984 and the Access to Health Records Act 1990. The exception to this is in relation to records of the deceased, which are still governed by the Access to Health Records Act 1990. This Act limits access to manual records made since 1st November 1991 unless earlier entries are necessary to make any later part of the records intelligible.

2. Purpose

The aim of this policy is to:

- ensure all Freedom of Information (FOI) requests are dealt with consistently, receiving a high quality response however and wherever the contact is made
- ensure that the CCG complies with all relevant regulations, laws and guidance
- provide clear routes for members of the public to make contact with the organisation so that they can appropriately request documents and information
- ensure that the CCG's Publication Scheme is up to date in order to provide access to information and to lessen the number of written requests the public has to make
- ensure that the necessary structures are in place for compliance with the FOIA
- ensure staff at all levels are aware of their responsibilities under the FOIA

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

- ensure timescales are met
- ensure the Governing Body of the CCG is fully informed on the operation of the FOIA and the implications for the organisation
- ensure that the CCG meets its obligations regarding 'subject access requests' under the terms of the Data Protection Act 1998
- ensure that the CCG meets its obligations regarding 'access to health records requests' under the terms of the Access to Health Records Act 1990
- set out clear guidelines for CCG staff to help make the access timely and within the legislation laid down by the Government
- ensure that all staff are aware of their responsibilities in the management of access to records.

The CCG will not normally charge for the provision of information that is provided as the result of an FOI request, however, there may be occasions where this is necessary. Please see Section 10 for details concerning our charging policy.

This policy deals with the rights of data subjects provided under Section 7 of the Data Protection Act 1998, whereby individuals can request access to their data.

3. Scope

This policy applies to those members of staff who are directly employed by the CCG and for whom the CCG has a legal responsibility. For those staff covered by a letter of authority, honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for, or on behalf of, the CCG. Further, this policy applies to all third parties authorised to undertake work on behalf of the CCG, including interims and contractors.

This policy provides a framework for the CCG to ensure compliance with the FOIA, DPA, AHRA, Re-use of Public Sector Information Regulations 2005 and EIR.

The CCG, wherever possible and within the limits set out by the Act's exemption, will make all information we hold available.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

4. Definitions and Terms

- **Freedom of Information Act (FOIA) 2000:** provides public access to information held by the public sector. It does this in two ways: public sector organisations are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities.
- **Environmental Information Regulations (EIR) 2004:** provide public access to environmental information held by public authorities. The Regulations do this in two ways, public authorities must make environmental information available proactively; and members of the public are entitled to request environmental information from public authorities.
- **Subject Access Requests:** the Data Protection Act (DPA) 1998, gives individuals access to their personal information held by organisations upon request.
- **Access to Health Records Act (AHRA) 1990:** gives access in certain circumstances to a deceased individual's health records.
- **The Re-Use of Public Sector Information Regulations (RPSI) 2005:** is about permitting re-use of information obtained from the public sector and how it is made available.

5. Roles and Responsibilities

Accountable Officers for NHS West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The Chief Officer is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Chief Officer has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance

Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

The Senior Information Risk Owner will act as the CCG'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).

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

The Senior Information Risk Owner will act as FOI lead at Governing Body level to:

- ensure organisational compliance with the FOIA;
- have lead responsibility for FOIs and the CCGs Publication Scheme;
- act as the champion for FOI awareness throughout the organisation;
- ensure that the general public and CCG staff have access to information about their rights under the FOIA;
- ensure processes are in place to assist for investigations into complaints / appeals;
- ensure that sufficient processes and structures are in place to administer FOI

Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. 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.

All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of information governance.

All staff are responsible for:

- Ensuring any Access to Information request directly received is forwarded to the Access to Information Team in a timely fashion.
- Ensuring enquirers receive accurate information about how to apply for information should it not be available online and for ensuring that any information requested from them, in relation to an enquiry under the FOIA, Data Protection Act and Access to Health Records Act is supplied within the timescales allowed.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Information Asset Owners (IAOs)

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 Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. 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.

FOI Lead / Access to Information Team and Information Governance Team (hosted by Basildon & Brentwood CCG)

The Access to Information Team is part of the larger Information Governance Team, they are responsible for the CCG's Publication Scheme, FOI Policy and processing of FOIs, Environmental Regulations, Subject Access and Access to Health Records requests. This includes day to day responsibility for the FOI Act, Data Protection Act and Access to Health Records Act and for ensuring that deadlines are met.

The Freedom of Information Lead will provide leadership and advice in terms of responding to requests, the use of exemptions and where necessary gain legal advice regarding whether it is appropriate to disclose the information requested.

All request details will be entered into a log and this will be maintained to monitor compliance to ensure all requests are answered in a timely manner.

The IG Team is also responsible for:

- Ensuring that, prior to the release of any information, the Access to Information Officer within the IG Team must be satisfied regarding the identity of the person making the request and that consent is in place where a request is made by a representative
- Ensuring that the Access to Information Officer does not release any information until this identification has taken place
- Providing advice to staff in the CCG on the withholding of certain information requested under the Data Protection Act
- Liaising with other organisations if relevant to process the access request in the event of shared records / data.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

If an applicant is making a request on behalf of another, such as a relative or a child, then consent, valid authority or evidence of parental responsibility of the patient, or lack of mental capacity, should be produced. Should further guidance be needed on obtaining valid consent please get in touch with the IG Team, who will be able to advise and assist.

CCG Responsibilities / FOI Liaison

The CCG is ultimately responsible for decisions made regarding Access to Information requests.

Senior officers of the CCG 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.

The FOI Liaison will be the key link between the Access to Information Team and the CCG. Wherever possible, the Team will send FOI requests directly to the manager within the CCG who the Team considers is most likely to hold the information in question, and send a copy to the FOI Liaison for information and monitoring purposes. In cases where the Team is unable to identify the lead manager, the request will be sent to the FOI Liaison to make a decision regarding who should handle the request within the CCG.

Part 1- Freedom of Information Act 2000

6. Process, Public Interest Test and Exemptions

The Access to Information Team will manage FOI requests for the CCG. For a summary of this process with the CCG, please see Appendix 3.

All requests for information with FOIA should be made in writing, in the form of a letter, fax or email. The enquirer should clearly identify the documents or information that they require, and supply a return address (which can be an email address) for the delivery of the information.

The FOIA only covers requests for recorded information and does not cover instances where explanations, opinions, comment, interpretations or unrecorded discussions are requested.

Where a request does not give sufficient detail to enable the CCG to process the request, the Access to Information Team will contact the applicant and advise them of the clarification that is required to make their application more detailed and to offer help with their request.

When clarification is sought from the requester the 20 working day deadline is restarted from when the clarification is received. The CCG will endeavour to ask for this clarification at the earliest opportunity. If, when sought, clarification is not received within a reasonable timescale

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

(approximately 3 months), the request will be considered cancelled and the requester will be notified of this.

The Access to Information Team will acknowledge receipt of the request within the first two full working days and provide the documents / information, or an explanation about why the information has not been disclosed within 20 full working days. A working day is defined by the Information Commissioner's Office (ICO) as one day within the working week (Monday to Friday), excluding all UK bank holidays (not just English bank holidays) and any other public holidays granted.

It might sometimes be necessary to extend this timeframe, for example to assess the public interest in releasing information. In these circumstances the Access to Information Team will endeavor to respond within 40 working days and notify the requester. Appendix 3 outlines the timescales for handling FOI requests.

Under the FOIA, information may be withheld if it is covered by an exemption. There are two categories of exemptions: qualified and absolute. Information covered by a qualified exemption can only be withheld if the public interest in withholding the information is greater than the public interest in releasing it. Information covered by an absolute exemption is not subject to this public interest test and can be withheld. The public interest test can be summarised as follows:

"In the majority of cases where an exemption applies, to some or all of the information requested, the authority will then have to consider whether it must override the exemption because it is in the public interest to release the information. This public interest test involves considering the circumstances of each particular case and the exemption that covers the information. The balance will lie in favour of disclosure, in that information may only be withheld if the public interest in withholding it is greater than the public interest in releasing it."

When the information requested falls under an exemption that is subject to the public interest test, the Access to Information Team will notify the provider of that information and the CCG FOI Liaison, both for awareness and to assist with assessing under the public interest test. The ICO categorises qualified and absolute exemptions, as laid out in Appendix 4.

The FOIA itself should be consulted for more detailed information on each exemption. If there is any doubt over whether an exemption applies the decision will be escalated to the Freedom of Information Lead responsible and legal advice gained where necessary.

If the CCG intend to withhold the information, there is a duty to explain this decision. This should be done within 20 working days, however if the CCG needs to consider the public interest test they are entitled to a reasonable extended period. In this case, within the 20 working day period the Access to Information Team should provide an estimate of when a decision can be expected and adhere to this, unless there is a good reason not to. If, while trying to reach a decision, it is realised that the original estimate was unrealistic the applicant must be kept informed. A record will be kept of any instances where estimates are not met.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

If the CCG does not hold the information that has been requested, but believes that some, or all of the information requested, is held by another public authority, the team will endeavor to advise the requester. In most cases this will mean:

- contacting or formally responding to the applicant and advising that we do not hold the information, but that it may be held by another public authority
- suggesting that the applicant reappplies to the authority which the team believe holds the information; and
- Providing contact details for that authority where possible.

Where a document contains some information that can be disclosed and some that is exempt, it should still be released, with the exempt information carefully blocked out (redacted).

Exempt information on hard copies should be concealed with a black marker pen and then double photocopied to ensure that it cannot be read. The exempt information should be blocked out from electronic versions and then saved as a new document. All redacted information must be accompanied by an explanation.

The Access to Information Team is not required to provide assistance to vexatious or repeated requests. A request would be classed as repeated if the team had already responded to the same or very similar request from the same applicant, or applicants appearing to act in concert, in a recent time period (approximately 3 months, but potentially longer / shorter dependent on the information and how frequently it is produced). A vexatious request can be identified as a request which subjects the organisation to inconvenience, harassment or expense and could be sent by one person or a number of persons working together.

It is also important to consider whether any third parties may be affected by the disclosure of information, for example if the information contains personal data or potentially commercially sensitive information. In these cases consent must be obtained wherever possible. If the third party refuses to consent, this does not always mean that the information should be withheld. Similarly, consent is not required if exemptions do not apply as the information will have to be disclosed regardless.

7. Requests for an Internal Review

Although a public body is not legally required to have an internal review procedure for FOI requests, the Section 45 Code of Practice makes clear that it is good practice to have a review procedure in place. The internal review procedure will ensure applicants are able to ask the CCG for an internal review if they are dissatisfied with the response to a request or the handling of a request.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Internal reviews should be conducted by a person who was not party to the original decision on whether to release the information requested. An internal review must be a fair and impartial review of the decisions made during the original discussion of whether to release the information. The person conducting the review must consider the information released against the information requested and make a full review of the papers associated with the original application.

It is best practice that the internal reviewer discusses the decisions made with the staff member, or members, who dealt with the original application in order to build a full picture regarding how decisions were made.

The circumstances relating to the original decision may have changed between the time the CCG made its decision about a request and the time it undertakes an internal review. The ICO guidance states that public bodies should reconsider the exemption and the public interest test on the basis of the circumstances as they existed at the time of the request, or at least within the agreed time frames. The FOIA does not stipulate a time limit for completion of an internal review but the Section 45 Code states that they should be dealt with in a reasonable time and the ICO recommend that:

- reviews should be completed within 20 working days of receiving the complaint;
- for complex complaints, or where it is necessary to reconsider the public interest test – reviews should be completed within 40 working days of receipt;
- If it appears that the deadline will not be met then the applicant must be advised as soon as possible and a second deadline set by which a response will be sent.

The internal review can have two outcomes; the original decision is reversed or is upheld. The outcome of the internal review must be recorded.

Where the original decision is reversed the applicant must be told and made aware of when they can expect the information originally requested to be provided to them. Where the original decision is upheld the applicant must be told and made aware of their further rights of appeal to the ICO.

The procedure on receiving a request for an internal review is as follows:

Person Responsible	Action to be taken
FOI lead	If complaint cannot be handled on an informal basis then request for internal review to be acknowledged within five working days along with details of internal review procedure
FOI lead	Independent person to be assigned to conduct internal review and relevant papers forwarded to them

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Head of IG, CCG SIRO / Other senior CCG staff	Reviewer to look at the original decision and discuss with people who handled the original request, with advise from Head of Information Governance.
FOI lead	Outcome of internal review to be discussed and agreed with the FOI lead, who communicates this to the applicant
FOI lead	If outcome is to reverse the decision then information to be sent to the applicant as soon as possible
FOI lead	If outcome is to uphold the decision then the applicant to be informed of their right to appeal to the Information Commissioner's Office (ICO)
FOI lead	Outcome of internal review to be recorded
CCG Accountable Officer	If procedures have not been correctly followed, the CCG (and CSU where appropriate) will apologise to the applicant and take appropriate steps to prevent a recurrence

All complaints regarding FOI requests should be sent to the CCG in the first instance, either by email or post, following the same route that a FOI request would. Contact details can be found in Section 5.

To complain to the Information Commissioner, please see the ICO web page at: <http://www.ico.gov.uk/complaints/getting/complain.aspx>

8. Personal Information and Records

Requests for access to or copies of personnel, staff, health or other personal records relating to the enquirer or third parties will be managed outside of the FOI section of this policy, please see page 14 onwards for further information on the management of Subject Access and Access to Health Records requests.

Requests for health related information about identifiable, living or deceased, individuals will be dealt with in accordance with the Data Protection Act (DPA) 1998 or Access to Health Records Act 1990, accordingly.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

9. Re-Use Regulations and Copyright

If there are concerns about information reaching a wider audience, without sufficient briefing relating to the circumstances surrounding the production of the data / document, or its context, then the CCG may indicate that the information is being supplied only for the use of the initial enquirer and cannot be re-used or reproduced in any format, or relayed on to other people, without the consent of the CCG.

CCG information supplied under the FOIA continues to be protected by the Copyright, Designs and Patents Act (CDPA) 1988.

For other forms of re-use, for example publishing the information, the permission of the organisation or person who owns the copyright would be needed. In the case of information produced by government departments and agencies, this can be re-used under the Open Government Licence. For information about this, please see: <http://www.nationalarchives.gov.uk/doc/open-government-licence/open-government-licence.htm>

If, however, the copyright is identified as belonging to somebody else, an application for permission would be needed.

For information about how to obtain permission from a third party, please go to Intellectual Property Office's website at: <http://www.ipo.gov.uk/>

Publishing the information or issuing copies may be subject to the provisions of the Re-use of Public Sector Information Regulations 2005 and will require the permission of the CCG and may require a fee.

10. Charging and the Appropriate Limit

The CCG may, in some circumstances, charge for releasing information in accordance with regulations.

A public authority is not obliged to comply with a request if it estimates that the cost of determining if it holds the relevant information, locating and retrieving this and, where necessary, extracting from a document would exceed the appropriate limit (see Appendix 5 for further details).

The appropriate limit is set down under Section 12 of the FOIA (£450 for public authorities). This figure is calculated at a rate of £25 per hour and therefore any request that exceeds 18 hours of combined work will normally be rejected.

Wherever possible, the Access to Information Team will work with the enquirer to try to reduce the amount of work involved so that some of the information can be provided. In certain circumstances

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

the CCG can offer the enquirer the option of paying for the information. In this instance, the enquirer would have to pay the full cost.

11. Duty to Advise and Assist

All public bodies have a duty to advise and assist applicants in requesting information (under Section 16 of the FOIA). This could involve assisting applicants in making their requests by suggesting what information is available and / or contacting applicants who have made broad requests in order to specify information required so that it may be identified.

Part 2- Subject Access Requests and Access to Health Records Act 1990

The Access to Health Records Act 1990 has now been repealed, except for the sections dealing with requests to records relating to the deceased.

The Data Protection Act 1998 is applicable to requests for access to records relating to living persons.

Under the Data Protection Act 1998, individuals have the right to:

- Access their records, subject to certain safeguards.
- Have copies of their records.
- Have these records explained if they are illegible or unintelligible.
- Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

Applicants do not have to give a reason for requesting access to records. The applicant's motives in requesting the records are irrelevant.

The 'data subject' could be a patient, contractor, member of staff or member of the public.

12. Individuals Who Can Make a Request

Subject access requests can be made by:

- The individual themselves.
- Individuals requesting access on behalf of a child for whom they have parental responsibility.
- A representative nominated by the individual to act on their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

- In certain situations a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent.
- Requests for information quoting the Data Protection Act may in fact be relevant to FOI and will therefore be processed as such.

Individuals living abroad

Under the Data Protection Act 1998, former patients now living outside the United Kingdom have the same rights to apply for access to their UK health records. A request for access to health records will be treated in the same way as a request from within the UK.

Access to Health Records

A health record is defined as:

- consisting of information relating to the physical or mental health or condition of an individual **and**
- has been made by or on behalf of a health professional in connection with the care of that individual.

13. Subject Access Requests- the rights of individuals

The CCG has the following guidance for managing requests.

The Data Protection Act 1998 ensures the transparency of data processing by obliging organisations to explain to individuals how their data is used and by providing the right of subject access under Section 7.

Section 7 of the Act provides that individuals who request access to their data should:

- be informed whether or not they are the subject of any data being processed by a data controller organisation; and
- where data is being processed, be provided with an understandable copy of the information held about them on request.

It should also be provided in a 'permanent form' unless the provision of the information in this way would involve 'disproportionate effort'. Individuals also have the right to:

- a description of the personal data of which they are the data subject;
- a description of the purposes for which the data are being processed or are to be processed – this could be based on the information supplied to the ICO during notification or on some information specific to the applicant;
- any information available to an organisation on the source of the applicant's data; and

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

- where the applicant specifically requests it, the logic involved in any fully automated decision-taking that has or may have a significant effect on the individual concerned, such as a decision in relation to credit worthiness (except where the logic would constitute a trade secret).

Consent Issues

In most cases the consent to access personal information will be provided by the individual who is requesting the information, however, there may be cases where the individual is unable to consent or the individual is a child.

When an applicant is not able to produce written consent from the patient to access the patient information or is not able to evidence that he / she is entitled to access the patient information, the Access to Information Team will request further information from the applicant on the reason for the request to decide whether it would be justifiable to release the information to the applicant in any event.

In the event that the applicant is a solicitor the subject's written authority for release and identification must be obtained.

Shared Records

There are situations where a subject access request involves a health record that is shared between healthcare organisations. The modernisation and integration of health and social care will place a greater emphasis on shared records. In developing integrated health and social care service, the IG Team will set out its arrangements for managing the requirements of the Data Protection Act 1998 and Subject Access requests with its partners as part of any service reconfiguration or development.

The following principles will be followed where this is the case:

- Obligations under the Act are, in general, placed on the holder of the record. If records are shared between two health or NHS bodies, they will be joint data controllers. Responsibility for ownership of the record rests with the Secretary of State for Health although essentially, where both organisations are joint data controllers for the shared record, both are controlling how they are used. In order to deal with Subject Access requests effectively, the organisation receiving the Subject Access request will take responsibility for processing the request and for obtaining consent or refusal for the release of parts of the record relating to the other organisation. The Access to Information Team is obliged to deal with the access request and the authorisation to release the parts of the record in order to ensure the request is processed within the 40 working day timescale as required by the Data protection Act 1998.
- The Access to Information Team takes responsibility for the access request and joint liability for their release where each organisation has authorised its release.
- If the Access to Information Team does not agree with the decision made by the other organisation to withhold data from release and subsequently releases that element of the record, it will accept full liability.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

- The Access to Information Team must document the reasons for withholding certain information lawfully in the request log. The applicant may challenge the decision not to release information.
- If there is a refusal to disclose the record from the partner organisation, the organisation dealing with the access request should, in their response to the applicant explain the reason for the refusal and refer them to the other partner organisation directly if they wish to contest the refusal.

Other Records

In addition to health records, all other records held by the CCG containing individual's information are liable to subject access requests by those individuals or their representatives. This includes personnel, finance, complaints and administration records. Any 'third party' content of the record must be referred to the originating organisation for consent to release.

Deceased Patient Records

The rights to access under the Data Protection Act 1998 extend only to living individuals. Requests for deceased patients' records are made under the Access to Health Records Act 1990. Requests can only be made by:

- The patient's personal representative (usually the executor of the will or administrator of the estate) or
- Any person who may have a claim arising out of the patient's death - release of any information will only be the minimum necessary to process their claim. Only relevant information relating to any claim made should be released

A health professional must inspect records taking into account the following:

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

The same rules apply to third party information as with other health records. The CCG should afford the same level of confidentiality to deceased patient's records as for living ones. The Department of Health and General Medical Council agree that there is an ethical obligation to the relatives of the deceased in requiring that confidential obligations continue to apply, subject to certain mandatory disclosures.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Exemptions to the Release of Information

Both the Data Protection Act 1998 and the Access to Health Records Act 1990 make provisions for withholding information in certain circumstances which must be considered when a request is received.

Data identifying a Third Party

Where personal data relating to the applicant also identifies another individual, the applicant's right of access must be weighed against the other data subject's right to privacy. The Access to Information Officer will attempt, where practicable, to seek the consent of the third party to the release of their data. Where consent is obtained then the information can be released. Given the sensitive and confidential information that the CCG may hold, if there is any doubt about divulging third party information, legal advice must be sought before making a decision to release information.

Time Limits for Access

The Act imposes very specific duties, which have to be carried out within a very tight timescale.

From receipt of the application form, 14 days are allowed if the record holder needs more information, either to identify the record(s) asked for, or to check the identity of the person applying for access.

The information is to be supplied within 40 days from the date of the request for access or within 40 days from the date the Team has sufficient information to enable them to satisfy themselves regarding the identity of the person making the request and to locate what is requested.

14. Audit & Monitoring Compliance

The Access to Information Team will continually review and monitor the handling and logging of information requests.

The Access to Information Team will produce monthly performance reports, which will provide information regarding the number of requests received, types of requesters, how requests have been responded to and their compliance with the time limit.

This policy will be reviewed every two years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

IG Incidents

Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programs and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

15. Dissemination and Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

16. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (<https://www.igtt.hscic.gov.uk/igte/index.cfm>) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

17. Related Documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Confidentiality and Data Protection Act Policy
- Information Lifecycle Management Policy and Strategy
- Safe Haven Policy

18. Equality & Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

19. Key Contacts

For Requests

CCG FOI inbox	foi.weccg@nhs.net essexccgs.foi@nhs.net
CCG SAR / AHRA Inbox	weccg.sar@nhs.net essexccgs.sar@nhs.net
CCG Address for Postal Requests	NHS West Essex CCG Building 4, Spencer Close St Margaret's Hospital The Plain Epping Essex CM16 6TN

Within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance.
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager
CCG FOI Liaison	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Appendix 1 ~ Publication Scheme

The Information Commissioner's Office (ICO) defines seven classes of information that a public authority should make available via their Publication Scheme. These classes are listed below.

1. **Who we are and what we do:** Organisational information, locations and contacts, constitutional and legal governance.
2. **What we spend and how we spend it:** Financial information relating to projected / actual income and expenditure, tendering, procurement and contracts.
3. **What our priorities are and how we are doing:** Strategy and performance information, plans, assessments, inspections and reviews.
4. **How we make decisions:** Policy proposals and decisions; decision making processes, internal criteria and procedures, consultations.
5. **Our policies and procedures:** Current written protocols for delivering our functions and responsibilities.
6. **Lists and registers:** Information held in registers required by law and other lists and registers relating to the functions of the CCG.
7. **The services we offer:** Advice and guidance, booklets and leaflets, transactions and media releases; a description of the services offered.

The CCG Publication Scheme

The ICO guidance is clear that an organisation should not create information purely for the purposes of completing the model publications scheme. As a young developing organisation, we do not expect to hold all the information suggested in the ICO guidance for some time.

Below, we set out the information we envisage proactively publishing over the coming months. By continually challenging ourselves to release as much information as possible, in as timely and accessible way as possible, we can ensure that the body of information in the public domain grows in line with our growth as an organisation.

The CCG will endeavour to publish and make available the following information:

- the minutes and papers of CCG formal meetings (Governing Body), and further information about upcoming meetings;
- information about our Governing Body and senior team, and further information about the CCGs organisational design;
- press releases and corporate communications;
- basic information about our key partners as we build up relationships with stakeholders;
- information about the CCGs procurement processes and live contracts;
- internal policies and equalities analysis;
- the CCG business plan; and
- an annual report to cover our work (including our financial accounts).

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Appendix 2 ~ Environmental Information Regulations 2004 (EIR)

An EIR request may be made verbally as well as in writing and will be defined as an application for environmental information in written, visual, aural, electronic or any other material form on:

- a) the state of the elements of the environment – for example, air, atmosphere, water, soil, land, landscape and natural sites such as wetlands, coastal and marine areas, biological diversity and the interaction of these elements;
- b) factors affecting (or likely to affect) the environment – including energy, noise, radiation, waste, emissions, discharges and other releases into the environment;
- c) measures – such as policies, legislation, plans, programmes, environmental agreements and activities affecting or likely to affect the elements and factors referred to above;
- d) reports – on the implementation of environmental legislation;
- e) economic analyses – including cost benefit and other analyses and assumptions used within the framework of measures and activities referred to in (c); and
- f) the state of human health and safety – including the contamination of the food chain, conditions of human life, cultural sites and built structures insofar as they are or may be affected by the state of the elements of the environment.

Under the EIR, information is held by the public authority if it has been produced or received by it; is held by another person on its behalf; or which the public authority holds on behalf of a third party.

The EIR places various rights and duties on public authorities which include:

- A duty to actively disseminate environmental information;
- A duty to make information available on request. Information requests must be answered within 20 working days, unless the public authority reasonably believes that it is impracticable to answer the request in that timescale due to its complexity and volume, in which event the public authority may have 40 days in which to provide the information.
- A duty to provide advice and assistance to applicants;
- A right to charge for information provided. Under the EIR, there is no cost limit beyond which information requests need not be answered. The EIR states that a charge may not exceed “an amount which the public authority is satisfied is a reasonable amount”.

Exceptions – Under the EIR there is an express presumption in favour of disclosure. However the public authority can refuse to disclose the information if it would adversely affect the following matters:

- a) international relations, defence, national security or public safety;
- b) the course of justice, ability of a person to receive a fair trial or ability of a public authority to conduct a criminal or disciplinary inquiry;

Policy Ref: IG08

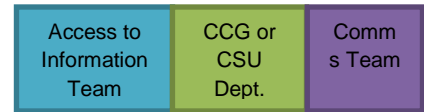
Version No: 3.0

Approval Date: 7th October 2016

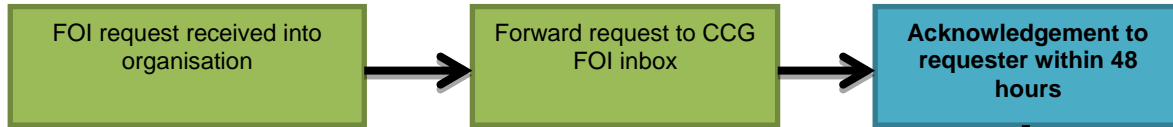
Review Due: March 2019

- c) intellectual property rights;
- d) the confidentiality or proceedings of any public authority where such confidentiality is protected by law;

Appendix 3 ~ FOI Request Process and Timescales



Process

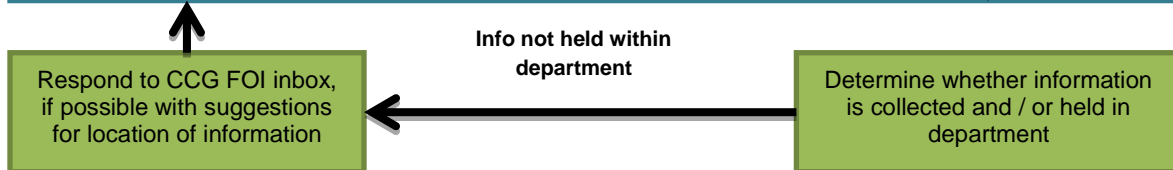


➤ CCG FOI Liaison copied into forwarding email for awareness and oversight.
 ➤ Comms liaison copied in if request is from a media source.
 ➤ If request is to multiple Essex CCGs (round robin), we will notify to enable collaborative responses

For each question:

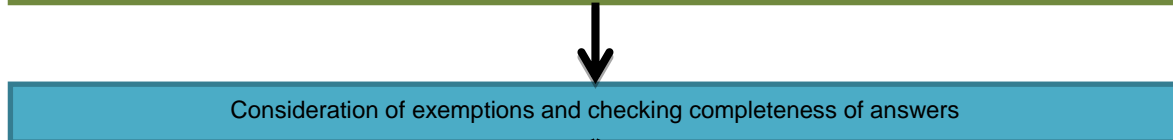
- Assess where information may be held and forward request to CCG/CSU Service to consider and provide information.
- Address question(s) to an individual (except where going to a team)
- Provide guidance and assistance where possible. This may not be possible if the FOI Team has no prior knowledge of the subject matter, or necessary where the request is simple and self-explanatory.

If nothing is heard from respondent within 10 days, a follow up phone call will be made to ensure the request has not been overlooked

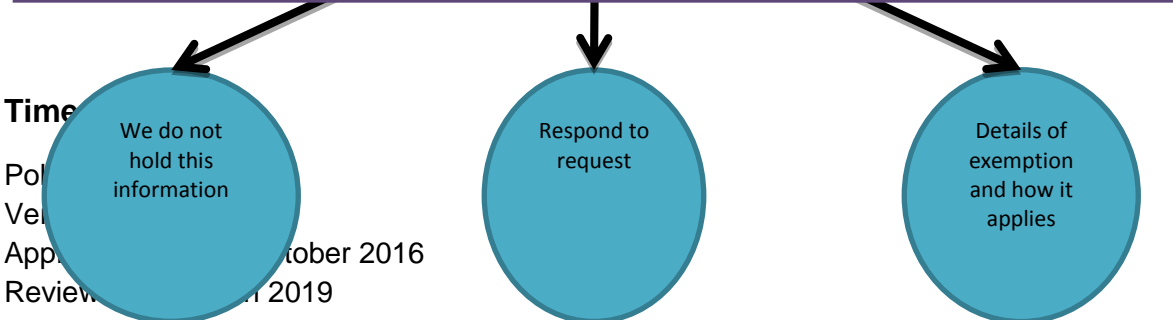


Info not held by CCG or providers
 Info held

Information gathered, or notification that information is not held by CCG, and returned to FOI Team via CCG FOI inbox **within 10 working days**.
 If any information is potentially exempt, raise with FOI Team for consideration and discussion.



If request from MP, Councillor, or Media, response sent to comms liaison for approval prior to release.



Time

Policy
 Version
 Approved: October 2016
 Review: 2019

Day 0	Request received into organisation via email, post or website.
IMMEDIATELY	Request forwarded to CCG FOI inbox. If postal request, scan and forward to CCG FOI Inbox.
Within 2 working days	Request acknowledged and deadline provided to requester.
Within 2 working days	Request forwarded to appropriate CCG / CSU staff members to obtain and provide information back to the Access to Information Team.
Within 10 working days	Information returned Access to Information Team, via either the central FOI email address, or the individual CCG inboxes.
10 working days	If nothing has been heard from respondent, either acknowledgement of request, or confirmation that request is being looked into, call to ensure the request has not been overlooked.
10, 15, 17 and 19 working days	If information not yet received: Reminder sent to appropriate person, escalated to SIRO and Heads of Department as deadline draws nearer.
Within 10 – 20 working days	Exemptions considered. If complex public interest test considerations then notify requester that extra time is needed and estimate response (no longer than 40 days) Approval for release gained via communications where necessary.
Within 20 working days	Response sent to requester.
Within 40 working days	If complex public interest test was considered response sent to requester.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Appendix 4 ~ Exemptions under Part II of the Freedom of Information Act 2000

The ICO categorises qualified and absolute exemptions as below:

Qualified exemptions:

- information intended for future publication;
- national security;
- defence;
- international relations;
- relations within the United Kingdom;
- the economy;
- investigations and proceedings conducted by public authorities;
- law enforcement;
- audit functions;
- formulation of government policy;
- prejudice to effective conduct of public affairs (except information held by the House of Commons or the House of Lords);
- communications with Her Majesty and honours;
- health and safety;
- environmental information (as this can be accessed through the Environmental Information Regulations);
- personal information (as this is covered by the Data Protection Act 1998);
- legal professional privilege; and
- commercial interests.

Absolute exemptions:

- information accessible to applicant by other means;
- information supplied by, or relating to, bodies dealing with security matters (a certificate signed by a Minister of the Crown is conclusive proof that the exemption is justified. There is a separate appeals process against such certificates);
- court records;
- parliamentary privilege (a certificate signed by the Speaker of the House for the House of Commons, or by the Clerk of the Parliaments for the House of Lords is conclusive proof that the exemption is justified);
- prejudice to effective conduct of public affairs (only applies to information held by House of Commons or House of Lords);
- personal information (as this is covered by the Data Protection Act);
- information provided in confidence; and
- prohibitions on disclosure where a disclosure is prohibited by an enactment or would constitute contempt of court.

Further information and guidance on the exemptions can be found on the website of the Information Commissioners Office (ICO): <https://ico.org.uk/>

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Appendix 5 ~ Summary of the FOI Fee Regulations 2004

The following summary is in line with Statutory Instrument 2004 No. 3244:

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

<http://www.legislation.hmsso.gov.uk/si/si2004/20043244.htm>

Introduction

Under the FOIA, the Regulations governing the appropriate limit, and the fees that can be charged for requests for information, came into force, along with the Act's new rights of access to information, on 1 January 2005.

The appropriate limit

The 'appropriate limit', for the purposes of Section 12 of the Freedom of Information Act 2000 and Section 9A of the Data Protection Act 1998, has been set at £600 for central government and Parliament; and **£450** for other public authorities, including local authorities, police, the **health service** and education.

The appropriate limit has to be applied, separately, to the duty under Section 1(1) (a) of the FOIA to confirm or deny whether the information is held. It is only if it would cost more than the appropriate limit to confirm or deny, by itself, that the obligation to do so is removed.

It will often be immediately obvious that the cost will not exceed the appropriate limit. But if a request is more complicated and likely to take longer to answer, the public authority will have to consider on a case by case basis if it wishes to estimate whether the appropriate limit would be exceeded in advance.

The Regulations set out what may be taken into account when public authorities are estimating whether the appropriate limit has been exceeded. The costs are limited to those that an authority reasonably expects to incur in:

- determining whether it holds the information requested,
- locating the information or documents containing the information,
- retrieving such information or documents, and
- extracting the information from the document containing it (including editing or redacting information).

The authority may take into account the costs attributable to the time that their staff are expected to spend on these activities.

In order to achieve consistency, all public authorities should use the same hourly rate when estimating staff-time costs, regardless of the actual costs. The **hourly rate** is set at **£25** per person per hour. If the costs attributable to the time spent on these activities, at

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

£25 per person per hour, would cost **more** than the appropriate limit of £450 to answer, the public authority is not obliged to answer it.

But, if a request would cost **less** than the appropriate limit to answer, it **cannot charge for** the areas listed above under what may be taken into account in relation to the request.

An authority may not take into account any costs other than those set out in the Regulations. In particular, it may not take account of the expected costs of:

- the time taken to **check** that a **request** for information **meets the requirements** of the FOIA;
- **considering** whether the information requested should be withheld in reliance on **an exemption** (this includes any costs incurred through seeking legal advice about whether exemptions apply);
- **considering** whether a request is **vexatious** or a **repeated** request;
- **obtaining authorisation** to send out the information;
- the time taken to **calculate any fee** to be charged; or
- **advice and assistance** provided under Section 16 of the FOIA.

Requests costing less than the appropriate limit

If a request would cost less than the appropriate limit to answer and there is no other basis on which it may be refused or otherwise dealt with, the public authority must comply with the request. It **cannot charge for** the areas listed above under what may be taken into account in relation to the request. The fees that can be charged are much more restricted than when the appropriate limit is exceeded, with the public authority bearing the majority of the costs of the request.

Authorities can **develop their own policies** on charging fees below the maximum, with the discretion to charge a lower fee or waive fees altogether. In cases where the appropriate limit has not been exceeded, the maximum fee that could be charged is based on an authority's estimate of the costs that it reasonably expects to incur in:

- informing the person making the request whether it holds the information; and
- Communicating the information to the person making the request.

This **includes the costs of:**

- putting the information in the applicant's preferred format, so far as this is reasonably practicable, as set out in Section 11(1) of the Act;
- reproducing any document containing the information, for example photocopying or printing; and
- postage and other forms of communicating the information.

When the appropriate limit has not been met, it is only these costs which may be taken into account for the purposes of calculating the maximum fee. In addition, no account can be taken of staff time in undertaking these activities, nor of the costs involved with

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

calculating whether the appropriate limit would be exceeded. For example, if the appropriate limit was not exceeded and you were providing information to an applicant:

- you could not charge for the time taken to locate, retrieve or extract the information or to write a covering letter to the applicant explaining that the information is being provided,
- you could charge for the cost of paper when photocopying or printing the information and printing the covering letter, as well as the cost of postage.

Public authorities have a duty to give effect to an applicant's **preferred format** for receiving information, so far as this is reasonably practicable. This may include:

- summarising the information;
- providing the applicant with a copy (for example by photocopying or printing);
- allowing the applicant reasonable opportunity to inspect a record containing the information;
- producing material in an applicant's preferred format (for example by putting it onto CD); or
- translating information into a different language at the request of the applicant. If a public authority regularly works in the language requested and has an in-house translation service, it should consider waiving any translation costs. However, public authorities are not obliged under the Act to translate documents if this would not be 'reasonably practicable'.

Authorities can charge for the actual costs incurred, but charges are expected to be reasonable. For example, in most cases, **photocopying and printing** would be expected to cost no more than 10 pence per sheet of paper.

In some cases, authorities may be required by **other legislation** to produce information in a particular format or a different language at no additional cost (and should not therefore charge for it as part of complying with the FOIA). For example, the requirement to make reasonable adjustments for disabled people under the Disability Discrimination Act 1995 could require an authority to produce material in a format such as Braille or on audio tape.

Where the maximum fee would be very low, less than £5 or £10, public authorities are encouraged to consider waiving the fee altogether.

If a public authority proposes to charge a fee for answering a request, it must **issue a fees notice** to the applicant, stating the fee. The fees notice should usually be issued before any costs are incurred in preparing to communicate the answer to the request. When an authority issues a fees notice, the applicant has three months to pay. If payment is not forthcoming, the authority does not have to answer the request (Section 9(2) of the Act).

Requests for information have to be answered promptly and in any event not later than the **twentieth working day** following date of receipt. However, where the authority has given

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

a fees notice to the applicant, the working days in the period beginning with the day on which the fees notice is given to the applicant, and ending with the day on which the fee is received by the authority, are to be disregarded in calculating the twentieth working day following the date of receipt.

If the actual cost of answering the request turns out to be greater than the estimated cost charged by way of a maximum fee, the authority must **bear the additional cost**. The FOIA does not allow for authorities to issue another fees notice to cover the additional cost. But if the actual cost of answering the request proves to be less than the fee charged, the public authority should consider **refunding** the excess money to the applicant.

Requests costing more than the appropriate limit

If requests would cost more than the appropriate limit to answer, the public authority is not obliged under Section 1 of the FOIA to answer it. However, Section 16(1) requires the authority to **'provide advice and assistance**, and see if the question could be refined to a more manageable level, or resubmitted in part, to bring it below the appropriate limit'.

Fees and information that is exempt under the FOIA

Information that is exempt through one of the exemptions listed in Part II of the Act is not affected by the FOI fees regime.

Information is (absolutely) exempt if it is 'reasonably accessible' to the applicant.

Information will always be considered reasonably accessible if:

- the authority is obliged to communicate it to the applicant under some other Act, or
- the information is made available in accordance with the authority's Publication Scheme.

Authorities **can charge fees** outside the terms of the Regulations for providing information **through the Publication Scheme**, provided that this is made clear as part of the scheme. For example, this could include set fees for specific pieces of information, or information about how any fees would be charged (such as a set rate per hour of work, a scale of charges, or the market rates for the work).

VAT

The rules apply equally to requests that are above or below the appropriate limit. The key determining factor relating to VAT charges is whether the information is available from another source that is not a public authority.

- If an authority was asked for information which was only available from that or another public organisation, any fees charged would not attract VAT.
- If an authority was asked for information that was available from another source that is not a public organisation, any fees would attract VAT.
- Fees charged for information that is provided in accordance with a public authority's Publication Scheme will attract VAT.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Appendix 6 ~ Procedures - Receiving and Processing an Access to Health Records Request

Stage one – receipt of request

Subject access requests (SARs) should always be received in writing and may be received either by the CCG, or directly into a CSU working on behalf of the CCG.

On receipt of a SAR the administrator will:

- Log the request onto the SAR spread sheet under the next available reference number
- Create a folder, with the reference number as the name, within the AHR section of the IG drive. All templates filled in to be sent to the applicant should be saved in this folder (using the format “SAR [Template Name] XX [patient initials] YYYYMMDD”)
- Create a sub-folder within the SAR inbox, with the reference number as the name. All electronic communications sent in relation to this request should be stored in this folder until the request is closed.

If the request has sufficient information to be processed and the applicant’s identity has been proven (and consent provided if via a nominated representative), the administrator will send the applicant a letter of acknowledgement stating that their request will be processed within 40 calendar days, and that they will receive an accurate invoice once the information is ready to be released (the request is put on hold until such a fee is received). This acknowledgement will provide them with the deadline.

If the applicant has not supplied sufficient information for the request to be processed the administrator will send a standard letter to the applicant, requesting proof of identity. The 40 calendar days will then start upon receipt of the proof of identity.

If the request is from a representative of the individual, a signed letter of consent must also be included with the request.

Stage two – processing of request

On receipt of proof of identity, a member of the team must confirm that the accompanying identification documents are valid. This is to ensure that the applicant is authorised to access the information. Forms of identity should include a photocopy of the applicant’s driving licence,

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

passport or birth certificate; in addition to other relevant information confirming the applicant's address, for example, a copy of a utility bill.

Following receipt of identity documents, the date received should be entered onto the spread sheet, this will automatically calculate the due date. An acknowledgement letter should be sent to the applicant notifying them when they should expect to receive a response.

A request for the information should be made to the relevant department. If an individual has requested all information held on them within the organisation, a search of all relevant databases and filing systems (including archived systems) should be initiated.

Types of personal information that might be held by the CCG are:

- HR files if the applicant is / was a member of staff or applied for a post within the CCG
- Complaints files
- Patient or client files or reports such as delayed transfers or applications for funding
- Payments made or received by the applicant
- Information held by other organisations on behalf of the CCG.

Stage three – reviewing the information

All information that has been collated must be carefully reviewed by an appropriate member of staff:

- For non-health records; either a member of the team that created the information or of the IG Team.
- For health records; an appropriate health professional of the team that created the information.

If any 'third party' individual, not including health professionals, is named or has provided information about the applicant, the following must be considered by the team prior to releasing the information:

- Is it possible to comply with the request without revealing information which relates to and identifies any third party individuals? If so the third party information must either be removed prior to releasing the information or alternatively consent of the third party must be obtained.
- Careful consideration must be given prior to disclosure to ensure that the applicant would not suffer any harm or distress on receipt of the information. This will be the subject of discussion with the relevant departmental manager.
- If a third party individual does not consent to releasing the information and the IG Team are not satisfied that it would be reasonable to disclose the information, it should be withheld.

However, as much of the information requested should be given without disclosing the identity

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

of the third party where possible unless it is reasonable given all of the circumstances to disclose without consent.

If the third party information has previously been provided to or is already known by the applicant, or it is generally available, it would be considered reasonable to disclose the information without third party consent. The spread sheet must be updated with details of the course of action and reasoning behind why consent was not sought or considered not appropriate.

The IG Team must check the information thoroughly to ensure that any codes or acronyms are explained to the applicant.

It must be decided by the IG Team whether there are any grounds for withholding the information under the Act's exemptions. Examples include safeguarding national security, crime and taxation, and parliamentary privilege.

Any police requests recorded by the IG Team should not be routinely disclosed when dealing with a subject access request without considering the following:

- How long is it since the police request was received? Is the investigation now closed?
- What details were obtained from the police officers requesting the information?

If there is any doubt as to whether the information regarding police requests should be disclosed, the Head of Information Governance should be consulted. Enquiries will then be made to establish if releasing the information would prejudice the detection and prevention of a crime.

The spread sheet must be updated with details of any information which is withheld and the exemptions used.

Once the review is completed, the screening form should be filled in by the reviewer, indicating any information to be redacted or withheld, and signed to show they approve of the release once the redactions have been applied.

Stage four – requesting the fee

If the request is for health records (CHC, Mental Health, and so on.):

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

- The maximum that can be charged is £10. This maximum will be charged in all instances in order to partially recover costs for complying.

If the request is for corporate records (not in relation to the health care of the subject):

- If records are held in electronic form, the maximum that can be charged is £10. As with non-health records we will always charge this maximum to partially cover costs.
- If records are held either wholly or partly in non-electronic form, the maximum that can be charged is £50. In these cases, the actual cost of supplying the records is calculated (including producing a copy) using the charging template. Once this charge has been calculated, the template should be saved into the folder for the appropriate reference number (using the format "SAR Charging Template XX (patient initials) YYYYMMDD")

The fee should be communicated to the applicant using the invoice template, highlighting that if we have not received this fee within 3 months of the date of the letter, the request will be considered cancelled and no further action will be taken. If, at a later date, the applicant wishes to obtain the information again, a new request will have to be submitted.

Stage five – releasing / refusing the information

As soon as the request has been processed, the information which has been judged to be the applicant's personal data should be released using the applicant's preferred method (sent via post or email; or attending the offices for collection or viewing). In all instances the applicant should be informed of what information, if any, is available and the purpose of holding this information.

If the information is to be sent to the applicant, the standard letter should be used and copies included. The information must be sent by Special Delivery annotated '**Private and Confidential**', '**Addressee only**' and packaged securely in a double envelope. The Special Delivery reference number should be logged onto the SAR spread sheet.

If the applicant has chosen to collect the information from the relevant CCG office, then a receipt will be required to be signed and photographic ID (for example, passport or driving licence) must be provided to confirm the recipient's identity.

If the applicant has chosen, and the CCG has agreed to allow the information to be viewed, a member of the IG Team will write to the applicant to arrange a convenient time and place that is both suitable to the CCG and the applicant within 40 calendar days of receipt of the fee.

Ideally the viewing should be of photocopied information. Any copies required by the applicant can then be removed as they are being viewed. If there is no other choice but to view the original record, the process must be witnessed by a member of the IG Team, or senior CCG staff member, who must ensure that the applicant is not left alone with the records at any time.

Policy Ref: IG08

Version No: 3.0

Approval Date: 7th October 2016

Review Due: March 2019

Up to a maximum of one hour will normally be allowed for the applicant to spend viewing the information. However, this time may be extended, if justified, with the Team's discretion. The applicant will be informed of the time allowance prior to and as a condition of the viewing.

Following release of the information, copies of the documentation should be stored manually in accordance with the Records Management Procedures. However, any redacted documents will be retained in accordance with the requirements of the Data Protection Act. The date of release and file reference should then be recorded onto the spread sheet.

If the application has been denied, restricted, or no information has been found, the applicant should be notified in writing using the standard letter. There is no requirement to explain the reason for denying or restricting the information. However, a member of the IG Team may consider disclosing if this would not contravene any of the Act's principles.

All decisions must be recorded on the spread sheet.

Once a request is closed all emails within the sub-folder of the SAR inbox should be dragged and dropped into the folder within the IG drive, and the sub-folder deleted from Outlook.

Appendix 7 ~ SAR / AHRA Procedure

