NHS Buckinghamshire, Oxfordshire and Berkshire West Clinical Commissioning Groups

Policy	**Individual Rights Policy and Standard Operating Procedures**
Version Number	1.0
Version Date	September 2021
Review Date	September 2022
Responsible Owner	Governance Managers
Approving Body	Combined Executive Committee
Target Audience	All Staff

Document Control

Reviewers and Approvals

This document requires the following reviews and approvals:

Name	Version Approved	Date Approved
Information Governance Steering Group	1.0	September 2021
Executive Committees/Commissioning Executive	1.0	October 2021

Revision History

Version	Revision Date	Details of Changes	Author

Links or Overlaps with Other Key Documents and Policies

Document Title	Version and Issue Date	Link

Acknowledgement of External Sources

Title / Author	Institution	Link

Freedom of Information

If requested, this document may be made available to the public and persons outside the healthcare community as part of the CCGs commitment to transparency and compliance with the Freedom of Information Act.

Equality Analysis

OCCG aims to design and implement services, policies and measures that are fair and equitable. As part of the development of this policy its impact on staff, patients and the public have been reviewed in line with the CCG's legal equality duties.

Contents

1. INTRODUCTION

Buckinghamshire, Oxfordshire and Berkshire West Clinical Commissioning Groups (the BOB CCGs) are under a legal duty to comply with individual rights requests under the Data Protection Legislation, in relation to personal information that it holds. This policy and standard operating procedure (SOP) sets out the approach that the BOB CCGs will take in responding to these requests along with useful guidance and steps to follow when requests are received anywhere within the BOB CCGs.

2. SCOPE AND DEFINITIONS

Scope

It is the responsibility of ALL BOB CCGs staff to respond to and help process requests under the individual rights set out in data protection legislation as soon as it is received by the BOB CCGs.

Any personal data in relation to an individual, no matter what format, where or how it is stored by the BOB CCGs falls into the scope of information that can be requested by individuals (i.e. data subjects) under the 'Individuals Right's contained within the Data Protection Legislation. All requests must be reviewed, without delay to see if the request can and should be complied with.

Requests received by third parties in regard to access to a data subjects personal data (e.g. the Police or Home Office) should be handled using the process described within the Standard Operating Procedure.

Definitions

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the UK GDPR.

Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the UK GDPR.
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life

Abbreviation	**Meaning**
CCG	Clinical Commissioning Group
CSU	Commissioning Support Unit
DC	Data Custodian

DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPO/DDPO	Data Protection Officer/Deputy Data Protection Officer
FPN	Fair Processing Notification (privacy notice)
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SCW	South, Central and West CSU
SIRO	Senior Information Risk Owner
UK GDPR	UK General Data Protection Regulations

3. DETAILS OF THE POLICY AND COMPLIANCE WITH THE DATA PROTECTION LEGISLATION

3.1 ACKNOWLEDGING INDIVIDUAL RIGHTS

The UK General Data Protection Regulation (UK GDPR) provides rights for individuals which fall into 2 distinct categories:

1. Where an individual wants to know what (or why) data the CCG is processing about them and/or have access /a copy of that data.
2. Where an individual wants the BOB CCGs to make changes to what or how the BOB CCGs are processing their personal data, or for the BOB CCGs to pass on personal data to another party. In these requests, the individual is not requesting access to, or a copy of the data itself:

An individual or their representative can exercise several data subject rights to the CCG. These do not confer automatic agreement to the request but will be duly considered by the BOB CCGs (the SOP in Appendix A contains more in depth detail regarding each of the rights).

These rights include but are not limited to the following:-

- obtain from the CCG confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, request access to the personal data (a **Subject Access Request/Right of Access**)

- obtain from the CCG without undue delay the rectification of inaccurate or incomplete personal data processed by the CCG concerning him or her (**Right to Rectification**)
- obtain from the CCG the erasure of personal data concerning him or her in certain circumstances (**Right to Erasure**)
- obtain from the CCG restriction of processing of personal data concerning him or her in certain circumstances (**Right to Restriction**)
- receive the personal data concerning him or her, which he or she has provided to the CCG, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller in certain circumstances (**Right to Data Portability**)
- object to processing of an individual's personal data in certain circumstances (**Right to Object**)
- not be subject to a decision based solely on automated processing by the CCG (**Rights related to automated decision making including profiling**)

It should be noted that there are exemptions to some of these rights and whilst the BOB CCGs must acknowledge the request, there may be legal grounds for not complying with it. Detailed guidance can be found in the SOP in Appendix A.

3.2 RECOGNISING AN INDIVIDUAL'S RIGHTS REQUEST

- A request can be made verbally or in writing.
- It can also be made to any part of the organisation and does not have to be to a specific person or contact point.
- A request does not need to mention the phrase containing the right being exercised or the relevant UK GDPR Article to be a valid request. As long as the individual has clearly described their request; this is valid. We will check with the requester that we have understood their request and request any Identification/authorisation (if required).
- We will record the details of all requests we receive.

The format that an Individual's Rights request is received may differ from request to request. In essence, if an individual writes to the BOB CCGs or speaks to the BOB CCGs and asks for access, changes or objections of any kind to the personal data the BOB CCGs are processing about them (whether perceived or actually processing their data) it should be considered and handled where appropriate as an Individual's Rights request.

Members of staff or the public who would like to exercise their individual rights under the UK GDPR can submit their requests to SCWCSU.Sar@nhs.net who will forward it onto the relevant Data Custodian/IAO.

3.3 REFUSING A REQUEST

If the CCG considers that a request is 'manifestly unfounded' or excessive we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request

In either case we will need to justify the decision.

3.4 CHARGING A FEE

- Individuals rights request are free of charge however the CCG may in some circumstances be able to charge a fee such as for repetitive requests
- We should base the reasonable fee on the administrative costs of complying with the request.
- If we decide to charge a fee we should contact the individual promptly and inform them.
- We do not need to comply with the request until we have received the fee.

3.5 INFORMATION FOR REQUESTORS

The CCG must inform the individual without undue delay and within one month of receipt of the request:

If the CCG are not taking action:

- the reasons for not taking action;
- their right to make a complaint to the ICO;
- their ability to seek to enforce a right through a judicial remedy

OR

If requesting further information:

- if requesting a reasonable fee or
- need additional information to identify the individual
- a need to extend the response time

OR

The request is being actioned:

- Respond to the request

3.6 CALCULATING RESPONSE TIME

Under the Data Protection Legislation the CCG has one Calendar month to respond to any request. In order to provide clarity to staff in the organisation, an operational decision has been taken to adopt a 28 day response time in line with the Information Commissioners Office suggestion of *'For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month*' see ICO Individual Rights Guidance for further details.

The SWC CSU will calculate the time limit from the day after they receive the request (whether the day after is a working day or not) until the corresponding date 28 days from that point.

3.7 EXTENDING THE RESPONSE TIME

The response time can be extended by a further two months if the request is complex or a number of requests have been received from the individual. There is a need to let the individual know without undue delay and within one month of receiving their request explaining why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request

3.8 VERIFYING IDENTITY

If the CCG has doubts about the identity of the person making the request more information can be requested. However, it is important that only information that is necessary to confirm who they are is requested. We will take into account what data we hold, the nature of the data, and what we are using it for.

We will let the individual know without undue delay that we need more information from them to confirm their identity. We do not need to comply with the request until we have received the additional information.

4. ROLES AND RESPONSIBILITIES

Roles and responsibilities for Information Governance are outlined in detail within the Information Governance Management Framework, Strategy and Policy.

All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the obligations under this policy.

5. TRAINING

All staff are required to complete training using the NHS Data Security Awareness Level 1 modules provided by NHS Digital via the e-LfH/ConsultOD platform, as outlined within the Training Requirements Policy.

6. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix B.

7. MONITORING COMPLIANCE AND EFFECTIVENESS

The application of this policy and the accompanying standard operating procedures will be monitored by the CCG through periodical reports to the Information Governance Steering Group.

8. REVIEW

This document may be reviewed at any time at the request of either staff or management, or in response to new legislation or guidance, but will automatically be reviewed bi-yearly.

9. REFERENCES AND ASSOCIATED DOCUMENTS

LEGISLATION

All staff are required to comply with Data Protection Legislation. This includes

- the UK General Data Protection Regulation (UK GDPR),
- the Data Protection Act (DPA) 2018,

- the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including

- the Human Rights Act 1998,
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations

Consideration must also be given to the

- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990

GUIDANCE

- CCG Standard Operating Procedures – Individuals Rights under the Data Protection Legislation and Access to Health Records Act
- ICO Guidance
- NHS Digital Confidentiality
- Dept. of Health and Social Care 2017/18 Data Security and Protection Requirements
- NHS England Confidentiality Policy
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- GMC guidance for managing and protecting personal information
- NHS Choices Your Health and Care Records

APPENDIX A: STANDARD OPERATING PROCEDURE AND THE INDIVIDUAL RIGHTS IN MORE DETAIL

This standard operating procedure (SOP) provides detailed guidance on how to process Individual's Rights requests under the UK General Data Protection Regulation

(UK GDPR) 2016 and Data Protection Act (DPA) 2018 (commonly referred to as the Data Protection Legislation).

Requests made under this legislation only relate to living individuals. The SOP will also cover requests received under the Access to Health Records Act (AHRA) 1990 which specifically relates to deceased individuals.

The SOP will cover the following UK GDPR and DPA rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

This SOP will also cover the rights of access to personal data for deceased individuals under the AHRA.

The SOP will provide detailed guidance on when each of the rights are available and provide procedural guidance on how to process each type of request.

All organisations that hold personal data or special categories of data are duty bound under the Data Protection Legislation and AHRA to comply with the above rights/requests.

This SOP is intended for all staff who are responsible for processing Individual Rights requests as well as any other staff whose role specifically requires them to manage requests of this nature.
It is essential that all staff responsible for such requests read, understand and follow this SOP.

SPECIFIC PROCEDURES

RIGHT TO BE INFORMED	FAIR PROCESSING NOTICE
RIGHT OF ACCESS	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED DECEASED INDIVIDUALS – DEALT WITH UNDER AHRA 1990 IN FAIR PROCESSING NOTICE APPLIES IN ALL CIRCUMSTANCES CAPACITY AND REPRESENTATIVES EXEMPTIONS APPLY NO CHARGE
RIGHT TO RECTIFICATION	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS APPLY NO CHARGE
RIGHT TO ERASURE	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS APPLY NO CHARGE
RIGHT TO RESTRICT PROCESSING	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE APPLIES IN ALL CIRCUMSTANCES EXEMPTIONS DO NOT APPLY NO CHARGE
RIGHT TO DATA PORTABILITY	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS DO NOT APPLY NO CHARGE
RIGHT TO OBJECT	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES SOME EXEMPTIONS APPLY NO CHARGE
RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES SOME EXEMPTIONS APPLY NO CHARGE

RIGHT TO BE INFORMED (ARTICLE 12-14)

Individuals have the right to be informed about the collection and use of their personal data under Article 12-14 of the UK GDPR. This is a key transparency requirement under the UK GDPR. We are obliged to provide individuals with information including, the purposes of processing an individual's personal data, the retention periods for that personal data and whether it will be shared with anyone else. This detail can be found in the organisations Fair Processing Notice (or Privacy Notice).

If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

How and what information should be provided

The information we provide to people must be

- concise,
- transparent,
- intelligible,
- easily accessible, and

- it must use clear and plain language

The Fair Processing Notice is published on websites.

We must regularly review, and where necessary, update our privacy information. We must bring any new uses of an individual's personal data to their attention before we start the processing.

THE RIGHT OF ACCESS BY THE DATA SUBJECT (SUBJECT ACCESS REQUEST – UK GDPR ARTICLE 15)

What is the right of access?
The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

What is an individual entitled to?
Individuals have the right to obtain the following from the CCG:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information such as
  - the purposes of processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipient we disclose personal data to;
  - retention period for storing personal data or, where this is not possible, our criteria for determining how long we will store it;
  - the existence of their right to request rectification, erasure or restriction or to object to such processing;
  - the right to lodge a complaint with the ICO or another supervisory authority;
  - information about the source of the data, where it was not obtained directly from the individual;
  - the existence of automated decision-making (including profiling); and
  - the safeguards we provide if we transfer personal data to a third country or international organisation

Much of this supplementary information is provided in our privacy notice.

What about requests made on behalf of others?

The UK GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney if the individual lacks mental capacity.

What about the records of deceased individuals?

The Data Protection Legislation only relates to living individuals. However requests for access to personal data relating to deceased individuals can also are made under another piece of legislation – the Access to Health Records Act (AHRA) 1990. The same rules apply regarding 'fees' etc. under the UK GDPR; however requests under the AHRA must be completed with 40 calendar days instead of 1 calendar month. The request must still be logged and actioned without undue delay.

Receiving a Request

The UK GDPR does not specify how to make a valid request. Therefore, an individual (or a third party acting on the individuals behalf) can make a request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point.

It does not have to include the phrase 'subject access' 'right of access' or 'Article 15'. However a request must be for access to personal data (including special categories of personal data) relating to the individual and not to information relating to other people. Therefore if a request is received it must be immediately logged with the SWCSU, who are responsible for processing such requests. The request must be logged on the team's right of access/SAR log immediately.

The UK GDPR does not require individuals to make a Subject Access Request (SAR) using a particular form and cannot be used as a means for extending the timescales for compliance in its own right; however it is good practice to provide a means for individuals to identify all relevant details that the organisation will/may require in locating the information.

Subject Access Requests should be submitted to SCWCSU.Sar@nhs.net

Once a request is received it must be acknowledged without undue delay and at least within 48 hours of receipt into the organisation. The organisation has one calendar month to respond to a SAR, but an organisational decision has been taken to adopt a 28 day response time limit (in accordance with ICO guidance). Therefore all requests must be completed within 28 days of receipt. The timescale for responding may be extended by a further two months if the request is complex or if we have received a number of requests from an individual. However we must inform the individual within one month of receiving the request why the extension is necessary.

A request may be received for access to a deceased individual's personal data. This will not be dealt with under the rights offered by the UK GDPR. Please refer to the Access to Health Records section below.

Processing the Request

Once the request has been received and logged we must ensure that we are satisfied as to the identity of the individual making the request. The key is proportionality and we must only request enough information to confirm who they are. This must be requested without undue delay and at least within 48 hours of receipt of the request. The period for responding to the request begins once the ID has been received. Two forms of ID are required. Forms of ID which are acceptable:

Primary documents for proof of identity:	**Secondary documents for proof of identity**
• UK passport / other country passport • Driving Licence • Adoption certificate • Separation document • Annulment document • National ID card • NINO card with National Insurance Number • National Insurance contributions form • Medical card with NHS number Change of name document **Certified copies of documents** can be provided by: 1. Posting the original to us by recorded delivery 2. Bringing them into our offices for us to copy 3. Having the originals certified by an individual or organisation. For further details please visit the following website: Certifying-a-document	• Pay slip • Tenancy agreement, rent book or rent card • Utility bills such as gas, electricity and water • Fixed telephone bills • Railcard, travel card and bus-pass • Season ticket. • Bank or Building Society debit or credit cards • Store charge card • Bank or building society statement / passbook • Shares certificates • Life insurance policy • Trade Union membership card • State benefit Book/Notification letter • Sub-contractors certificate • P45 • EHIC – European Healthcare Insurance Card

If an individual makes a request electronically, the information should be provided in a commonly used electronic format, unless the individual requests otherwise.

A request under the right of access relates to the data held at the time the request is received. However, in many cases, routine use of the data may result in it being amended or even deleted while the request is being dealt with. Therefore it is reasonable to supply information that is held at the time the request is responded to, even if this is different to that held when the request was received. However, it is not acceptable to amend or delete the data if we would not otherwise have done so. Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

The UK GDPR requires that the information provided to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

This will be particularly important where the information is addressed to a child. Therefore the organisation may be required to explain particular references, acronyms or information which is provided to the individual.

If a request is received but more information is required in order to clarify the request this must be requested without undue delay. However we must only ask for information that is reasonably required to find the personal data covered by the request. The period for responding to the request begins once the additional information is received. However, if an individual refuses to provide any additional information, we must still endeavour to comply with the request i.e. by making reasonable searches for the information covered by the request.

Under the UK GDPR, in most cases a fee cannot be charged. However where the request is manifestly unfounded or excessive we may charge a “reasonable fee” for the administrative costs of complying with the request. We can also charge a reasonable fee if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies.

Requests Received from Representatives or Third Parties

The UK GDPR does not prevent an individual making a valid request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act on their behalf. In these cases, we must be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party’s responsibility to provide evidence of this entitlement. This may be in the form of a written consent/authority form evidencing that the third party has consent from the individual to access their personal data.

A Third Party Authorisation form (for a representative to complete) has been prepared for situations where this is necessary which can be found in section 6.

Guidance should be sought from relevant Caldicott Guardians and Data Protection Officers if there are any concerns over the nature of the information and whether there are concerns as to whether the data subject is aware of what might be shared with the representative.

Requests may also be received from those who hold power of attorney; if the individual lacks mental capacity. There are no specific provisions under the UK GDPR or Mental Capacity Act 2005 enabling a third party to exercise access rights on behalf of such

an individual therefore it is reasonable to assume that an attorney with authority to manage the affairs of an individual (or under a deputyship order) will have the appropriate authority.

We will need to see evidence that the attorney holds a sealed power of attorney for health and welfare purposes (and in some circumstances for property and affairs) or a deputyship order from the Court of Protection. ID will also need to be requested if we are unsure as to their identity (see above section).

The Lasting Power of Attorney (LPA) gives the attorney authority to make decisions on behalf of the person who has requested the LPA (known as the Donor) and the attorney has a duty to act or make decisions in the best interests of the person who has made the LPA.

There are two different types of LPA:

1. A personal welfare LPA is for decisions about both health and personal Welfare.
2. A property and affairs LPA is for decisions about financial matters.

There may be times when carrying out the duties as an Attorney that s/he needs to access personal information about the Donor, for example from a doctor, to help make a decision that is in the Donor's best interests. Most of this information will be personal information relating to the Donor and much of it will be sensitive and/or confidential.

Providing the attorney is acting within the powers given within the LPA, s/he is entitled to ask for this information in the same way the Donor would have done if they had the capacity to do so. The attorney is only entitled to the information that is necessary for the decision(s) that have to be made e.g. the past medical history that has no bearing on the issue at hand should not be revealed.

Seek advice from relevant Data Protection Officers if concerns arise about releasing information under a particular LPA.

Requests for Information about Children

A child has a right under the UK GDPR to have access to their personal data regardless of their age. However children under a particular age will likely have their rights exercised by those who have parental responsibility for them.

Therefore before responding to a request for information about a child we must consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should respond directly to the child, unless the child authorises their parent (or an individual with parental responsibility) to act on their behalf.

To determine whether the child is mature enough to understand their rights we must take into account the following:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them
- any views the child or young person has on whether their parents should have access to information about them

Children aged over 16 years are presumed to be competent. Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR. However, children who are aged 12 or over are generally expected to have the competence to give or withhold their consent to the release of information from their health records. In Scotland, anyone aged 12 or over is legally presumed to have such competence. When assessing a child's competence, it is important to explain the issues in a way that is suitable for their age. The Gillick competency test or Fraser guidelines can also be used to determine whether a child is presumed to be of a sufficient age/maturity.

For further information on situations where the request has been made by a child, see the ICO guidance on children and the UK GDPR

Other People's Information

Responding to an access request may involve providing information that relates both to the individual making the request and to another individual.

The Data Protection Act 2018 says that we do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, we must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual

So, although we may sometimes be able to disclose information relating to a third party, we need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway.

For the avoidance of doubt, we cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else. Good practice would be to redact information that relates to another individual.

Requests for Deceased Individuals Records

The Access to Health Records Act 1990 (AHRA) provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person's health record.

There may be circumstances where individuals who do not have a statutory right of access under AHRA request access to a deceased patient's record. Current legal

advice is that the Courts would accept that confidentiality obligations owed by health professionals continue after death. Each request should be reviewed on a case by case basis and advice should be sought from the Caldicott Guardian if there are any concerns regarding disclosing any personal information.

Individuals who have a right of access under the AHRA are defined under Section 3(1)(f) of the Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record.

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice and speak to relevant Data Protection Officers.

There are different requirements to the UK GDPR/DPA in terms of timescales; Access to Health Records requests should be responded to within 40 calendar days and there can be no charge for the request. It is still a requirement to check the validity of the request (ID etc.). No prescribed form needs to be completed however we must be satisfied as to the identity of the individual making the request and we can therefore seek clarification from the requestor. If a request is received from a patient's personal representative evidence must be provided such as a sealed Grant of Probate or valid Will evidencing that the individual making the request is a personal representative. If the individual died intestate, the individual making the request can apply for Letters of Administration.

Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis. The public good that would be served by disclosure must outweigh both the obligation of confidentiality owed to the deceased individual, any other individuals referenced in a record, and the overall importance placed in the health service providing a confidential service.

Key issues for consideration include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. The views of surviving family and the length of time after death are also important considerations. The obligation of confidentiality to the deceased is likely to be less than that owed to living patients and will diminish over time.

Another important consideration is the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information abstracted from the record. If the point of interest is the latest clinical episode or cause of death, then disclosure, where this is judged appropriate, should be limited to the pertinent details.

If the deceased individual expressed a wish for information to remain confidential this should be upheld regardless of who is making the request unless there is an overriding public interest in disclosing.

For further guidance, please refer to the NHS Choices deceased individuals records

Refusing to Comply with a Request

If we consider that a request is ‘manifestly unfounded’ or excessive we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request

In either case we will need to justify the decision. For further advice please contact relevant Data Protection Officers.

If we do refuse to comply with a request we must explain the reasons we are not taking action; advise the individual of their right to make a complaint to the ICO and their ability to seek to enforce a right through a judicial remedy.

The ICOs address is:
Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Exemptions

There are a number of exemptions from the individual rights under the UK GDPR. The relevant exemptions have been detailed below.

Information required to be disclosed by law etc. or in connection with legal proceedings

Schedule 2, Part 1, paragraph 5 of the DPA 2018 provides an exemption when Information is required to be disclosed by law etc. or in connection with legal proceedings. The listed UK GDPR provisions (in Schedule 2, Part 1, paragraph 1) do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public

Crime and Taxation

Schedule 2, Part 1, paragraph 2 of the DPA 2018 provides an exemption for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of tax or duty from Articles 13-18 and 20-22, which includes the right of access provisions. Therefore if information is requested by a competent authority such as the Police, personal data can be disclosed without the consent of the data subject if the conditions in Schedule 1, Part 1, and paragraph 10 are met i.e. for the purposes of the prevention or detection of an unlawful act.

Legal Professional Privilege

Under Schedule 2, Part 4, paragraph 19 of the DPA 2018, information that relates to legal professional privilege is exempt from the right of access and duty to be informed provisions (Article 15, 13 and 14) of the UK GDPR.

Confidential References

Under Schedule 2, Part 4, paragraph 24 of the DPA 2018 confidential references (those references given in confidence) are exempt from the right of access provision (Article 15) as well as the duty to be informed under Article 13 and 14 of the UK GDPR if the personal data consists of a confidential reference for the purposes of including the education, training or employment of the data subject. This exemption also applies to the appointment of the data subject to any office, including that of a volunteer, or the provision of any service by the data subject.

Health data processed by a Court

Schedule 3, Part 1, paragraph 3 of the DPA 2018 states that the rights under Articles 13, 14, 15, 16, 17, 18, 20, 21 and Article 5 (General Principles) of the UK GDPR do not apply where health data is processed by a court, is contained in a report or other evidence under proceedings and rules detailed in the Data Protection Act 2018 or the data can be withheld in whole or in part from the data subject by the Court.

Requests made by others

Under Schedule 3, Part 1, paragraph 4 (1) (a), where the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject or (1) (c) where the data subject is incapable of managing his or her own affairs and a Court appointed representative is managing their affairs, the rights under Articles 13, 14, 15, 16, 17, 18, 20, 21 and Article 5 (General Principles) do not apply concerning health data where to comply with that request would

(a) release data given by the data subject in the expectation that it would not be shared with the person making the request on their behalf or;
(b) release the results of an examination or investigation carried out under the data subjects consent with the understanding that the result would NOT be disclosed or;
(c) release information that the data subject has expressly indicated should not be disclosed;

Serious harm from health data disclosure

Under Schedule 3, Part 1, paragraph 5 of the DPA 2018 health records may be withheld from disclosure under Article 15(1) and (3) of the UK GDPR when the serious harm test is met or where a controller who is not a health professional obtains an opinion from someone who appears to be an appropriate health professional. The "serious harm test" involves consideration of whether the application of the Article 15 Right of Access to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual. However, the opinion of the Health Professional will not be relevant if it was obtained prior to a period of 6 months before the request or, it is felt that it would be advisable to re-check that opinion;

Information already known by the Data Subject

Under Schedule 3, Part 1, paragraph 6 of the DPA 2018 an exemption cannot be applied to a request under Article 15 where it is apparent that the data subject has already seen or knows about the health information;

Disclosure of Records

Before supplying any information in response to a request, please check that we have the requester's correct postal or email address (or both) – whichever the requestor has asked for the information to be sent by. If sending paper copies, ensure the information is sent via Royal Mail Special Delivery. If the requestor chooses to collect the information; ID must be checked and the requestor must sign a collection receipt. The DPA/UK GDPR requires that the information you supply to the individual is in intelligible form. At its most basic, this means the information should be understandable by the average person. Therefore all records must contain explanations of codes or abbreviations where appropriate. Do not provide original records, only photocopies

If information has been withheld due to an exemption, for example, information relating to another individual, legal privilege etc. – this must be documented on the Individuals Rights Log (including justification for applying the exemption) and explained to the requestor that information has been redacted/removed in accordance with the provisions set out in the UK GDPR/DPA.

The requestor may ask for the information to be disclosed to them over e-mail. If this is the case, we must explain to the individual that the information will not be transmitted with encryption and therefore we cannot guarantee that the information will be sent securely. The individual will need to confirm that they understand this and agree for the information to be sent electronically (e.g. by confirming agreement in response to the email).

Please remember to keep a copy of the information disclosed

Retention

The log and all documentation relating to a particular request should be kept and retained for a period of three years. In the event of an appeal, the subject access request is retained for 6 years post closure of appeal.

Statistics

Quarterly figures will be by the SWCSU to the Data Protection Officer to ascertain how many individual right's requests has been received and whether they have been processed in accordance with the UK GDPR.

RIGHT TO RECTIFICATION (ARTICLE 16 AND 19)

The UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the UK GDPR (Article 5(1) (d)). However, although we may have already taken steps to ensure that the personal data was accurate when we obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If we receive a request for rectification we should take reasonable steps to check that the data is accurate and to rectify the data if necessary. We should take into account the arguments and evidence provided by the individual.

Processing the request

The request should be logged on the team's individual's rights log and acknowledged without undue delay and at least within 48 hours of receipt.

<u>The same conditions regarding timescales, ID and fees as explained in sections above</u>

In terms of taking reasonable steps; what steps are reasonable will depend on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort we should put into checking its accuracy and, if necessary, taking steps to rectify it. We may also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject. The UK GDPR does not give a definition of the term accuracy. However, the Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

If mistakes are recorded, it may be prudent to maintain the mistake but update the record to show the accurate information. For example, if a diagnosis for a condition is recorded on a patient's record which later is proved not to be the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as

the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified

It may also be difficult to argue that 'opinions' are inaccurate and therefore able to be rectified, but should be recorded as opinions on the record.

Whilst the request is being considered, the data should be restricted (in accordance with Article 18) until the data is rectified.

If we are satisfied that the information is accurate/complete then we must tell the individual that we will not be amending their data and provide them with the detail contained in section 5.2. Please ensure a note is recorded on the individual's record indicating that the individual challenged the accuracy of the data and their reasons for doing so.

If we have disclosed the personal data to other organisations/individuals, we must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individual about these recipients.

RIGHT TO ERASURE (ARTICLE 17 AND 19)

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

The right of erasure will not apply in all circumstances, and we must establish whether the above conditions apply before we can process such a request.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the UK GDPR. For further details about the right to erasure and children's personal data please read the ICO guidance on children's privacy.

Processing the request

The request should be logged on the team's individual's rights log and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2. apply Please see above

As described above, we must then determine whether the right of erasure applies to the particular request.

Exemptions

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims

The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care;

or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional)

If we have disclosed the personal data to others, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individuals about these recipients.

Where personal data has been made public in an online environment (such as social networks) reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable we should take into account available technology and the cost of implementation.

If we refuse to comply with the request for erasure due to the fact that it is manifestly unfounded or excessive we must adhere to the conditions set out in section 5.2 above.

RIGHT TO RESTRICT PROCESSING (ARTICLE 18 AND 19)

Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, we are permitted to store the personal data, but not use it.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely, but we will need to have the restriction in place for a certain period of time.

Processing the request

The request should be logged on the team's individual's rights log and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply Please see above

Individuals have the right to request that their personal data is restricted in the following circumstances:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for us to rectify it (Article 16), they also have a right to request that we restrict processing while we consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request us to restrict processing while we consider their objection request

Therefore, as a matter of good practice we should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

In order to restrict processing, we should consider the following options:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website

Once the data is restricted, we must not process the restricted data in any way except to store it unless:

- We have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;

- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest

If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individual about these recipients.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and we are investigating this; or
- the individual has objected to us processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and we are considering whether our legitimate grounds override those of the individual

Once we have made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction. Once we have done this we must inform the individual before we lift the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if we are informing the individual that we are lifting the restriction (on the grounds that we are satisfied that the data is accurate, or that our legitimate grounds override theirs) we should also inform them of the reasons for our refusal to act upon their rights under Articles 16 or 21. We will also need to inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy

If we refuse to comply with the request for restriction due to the fact that it is manifestly unfounded or excessive we must adhere to the conditions set out in section 5.2 above.

RIGHT TO DATA PORTABILITY (ARTICLE 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and

use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Processing the request

The request should be logged on the team's individual's rights log and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply Please see above

The right to data portability only applies when:

- Our lawful basis for processing this information is consent or for the performance of a contract; and
- We are carrying out the processing by automated means (i.e. excluding paper files)

The right to data portability only applies to personal data and allows data to be transferred from us as the controller to another controller (if the above conditions apply).

The data must be provided in a structured, commonly used and machine readable format. We may need to seek advice and assurance from the IT team to determine how the data can be transferred. Further details on how the data can be transferred can be found on the ICO's guidance webpages under 'Right to Data Portability'. We are responsible for ensuring the data is transmitted securely.

We can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Please refer to section 5.2 for details on what information must be provided to the individual if we are refusing to comply with their request.

RIGHT TO OBJECT (ARTICLE 21)

An individual has the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and

- processing for purposes of scientific/historical research and statistics

Overview

An individual has the right to object to:

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

Processing the request

The request should be logged on the team's individual's rights log and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply Please see above

Performance of a legal task or organisation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Direct Marketing Purposes

We must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.

We must deal with an objection to processing for direct marketing at any time and free of charge. We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Research Purposes

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

We can refuse to comply with a right to objection if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Please refer to section 5.2 for details on what information must be provided to the individual if we are refusing to comply with their request.

RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING (ARTICLE 22)

The UK GDPR applies to all automated individual decision-making and profiling. Article 22 of the UK GDPR has additional rules to protect individuals if we are carrying out solely automated decision-making that has legal or similarly significant effects on them. The processing is defined as follows:

- Automated individual decision-making (making a decision solely by automated means without any human involvement).

- Examples include an online decision to award a loan; or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do.

- Profiling (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain

circumstances. We can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent

If we're using special category personal data we can only carry out processing described in Article 22(1) if:

- we have the individual's explicit consent; or
- the processing is necessary for reasons of substantial public interest

Profiling (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Profiling can be part of an automated decision-making process. The UK GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the UK GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.
A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention

We must inform individual if we are using this form of processing and if we are, we must:

- give individuals information about the processing;

- introduce simple ways for them to request human intervention, express their point of view or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended
- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects. If our processing does not match this definition then we can continue to carry out profiling and automated decision-making but we must still comply with the GDPR principles. We must identify and record our lawful basis for the processing. We need to have processes in place so people can exercise their rights. Individuals have a right to object to profiling in certain circumstances. We must bring details of this right specifically to their attention

FORMS/TEMPLATES TO BE USED

Name of Form/Template	Document
Template Individual Rights and AHR Log	 Template Individuals Rights & AHR Log.xls
Article 15 Acknowledgement Letter	 Article 15 Acknowledgement Let
Article 15 Disclosure Letter	 Article 15 Disclosure Letter.docx
Article 15 Third Party Authorisation Form	 Individual Rights Requests third party

Consent to disclose records	Consent from DS Letter_Form.doc
CHC Consent letter	2018_09_04AHRA_CHC_Consent_DRAFT_
Article 16-22 Acknowledgement and Outcome Letters	Articles 16 to 22 letters.docx
Staff Subject Access Request Application Form	20180208_Data Subject Access Reque
Access to Health Records Acknowledgement Letter	Access to Health Records Acknowledge
Access to Health Records Application Form	Access to Health Records Application F

APPENDIX B: EQUALITY IMPACT ASSESSMENT

Individual Rights Policy

1 What is it about? *Refer to the Equality Act 2010*
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Individuals Rights Policy details how the BOB CCGs will meet legal obligations and NHS requirements concerning the exercising of Individual Rights over the processing of their personal information and the arrangements in place to support this.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the exercising of Individual Rights to be of equal status across all groups of people.
d) What are the barriers to meeting this potential?

Barriers may arise where Individuals may experience difficulties in exercising their rights i.e. those who may lack the mental capacity to do so, are deemed particularly vulnerable at a given point in time, where those Individuals are children or where there are language barriers or there is a need to convey the information in a particular way for ease of accessibility reasons.
2 Who is using it? ***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy in response to legislative requirements.
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.
3 Impact ***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created with regard to the policy itself, only in respect of communicating how individuals can exercise their rights.
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? The BOB CCGs will pay particular attention to the NHS Accessibility Standards and offer all appropriate help and assistance to enable those experiencing difficulties to exercise their Rights.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested?

No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? Given consideration to providing the guidance to individuals in different formats to aid accessibility.
b) What will you do now and what will be included in future planning? Implement different methods of communication and ways of applying for individuals to exercise their rights.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Angela Sumner** angelasumner@nhs.net	Date completed: **02-07-18** Proposed EIA review date: **01-04-19**
Signature of director/decision-maker **Add signature** Name of director/decision-maker **Insert Name and Position**	Date signed **Insert date**