HEALTHIER PEOPLE,
BETTER FUTURE

NHS
Heywood, Middleton and Rochdale
Clinical Commissioning Group

A Guide to Individual Rights

Reference Number:	DS003
Version:	V1.2
Name/Department of originator/author:	Information Governance Team
Approval Committee	Information Governance Management Group
Date Approved	July 2019
Review date:	July 2021
Target audience:	Citizens

DOCUMENT CONTROL

Policy Title:	A Guide to Individual Rights (formally entitled *"Individual Rights Procedure"*
Policy Area	Data Security / Information Governance
This policy Supersedes	N/A – New Procedure
Description of Amendment(s)	N/A – New Procedure
Published by:	Heywood, Middleton and Rochdale Clinical Commissioning Group, Number One Riverside, Smith Street, Rochdale, OL16 1XU
Intended Audience:	Citizens
Policy shared location	Internet

Document Approvals This document requires the following approvals:

Governance – Committee /Board/Other	Purpose	Outcome	Date
Information Governance Operational Group	Review and approval	Approved	31st August 2018
Information Governance Management Group	Review and approval	Approved	26th July 2019

Policy review control information

Version	Date	Reviewer Name(s)	Comments
Draft V0.1	July 2018	Chris Lawless & Lisa Winstanley (GMSS IG Team)	New Procedure
V1.0	Aug 2018	IGOG	Approved
V1.1	Jun 2019	Paul Fox (Senior IG Lead)	Revision of the individual rights procedure so that its written for the public audience
V1.1	Sept 2019	Paul Fox (Senior IG Lead)	Change to reflect ICO's guidance on the definition of one calendar month.
V1.2	Feb 2020	Paul Fox (Senior IG Lead)	DPO email address change

Contents

1. Introduction

1.1 The General Data Protection Regulation (GDPR) came into force on the 25th May 2018 along with the new Data Protection Act (May 2018).

1.2 The purpose of this guide is to explain the enhanced rights available to individuals and how we deal with any personal information requests or enquiries.

1.3 Please be aware that these rights are not absolute and are subject to conditions and exemptions. In some cases, your rights described within this document only apply if the processing activity is undertaken on specific legal grounds and/or in defined circumstances. Therefore, all of your rights are unlikely to be engaged in all cases.

2. Definitions

2.1 **General Data Protection Regulation (GDPR)** - This is a European Union (EU) legislation that became directly applicable in member states (e.g. the UK) on the 25th May 2018. The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

2.2 **The Data Protection Act 2018** – The updated Data Protection Act, enacted on the 23rd May 2018, sits alongside GDPR and fills gaps regarding data processing where flexibility and derogations are permitted. It also states the legislation on processing for law enforcement purposes, the intelligence services, and outlines the functions of the Information Commissioner's Office (ICO) which is the UK's supervisory authority.

2.3 **Personal Data** - This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

2.4 **Special Category Data** - This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. It was previously referred to as sensitive information. Under GDPR, this now includes biometric data and genetic data.

For more information about special categories of data please refer to the ICO guide at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

2.5 **Personal Confidential Data** - This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

2.6 **One calendar month** - This is calculated from the actual day a request is received (whether it is a working day or not) until the corresponding calendar date in the next month. For example, if a request is received on 30th March, the time limit starts from the same day and we have until the 30th April to comply with the request. If the 30th April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply with a request.

2.7 **Processing** – This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Individual Rights under GDPR

3.1 The GDPR provides the following rights for individuals. These will be covered in more detail later in this guide:

- 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
- The right to withdraw consent
- The right to complain

4 The right to be informed

4.1 Individuals have the right to be informed and this is a key transparency requirement under GDPR. Information provided to individuals must be clear and concise about

how the CCG processes data (including personal data, pseudonymised data and also anonymised data). The information about the processing must be easily accessible (for example, via a website or published on a leaflet). This is often referred to as a "Privacy Notice." Please refer to our privacy notice viewable on our website https://www.hmr.nhs.uk/download/our_organisation/policies_plans_and_reports/HMR-CCG-Privacy-Notice.pdf

For more detail on the right to be informed please refer to the link below:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

5. The right of access

5.1 The right of access is commonly referred to as 'subject access'. This gives individuals the right to request a copy of and / or to view their personal data held by an organisation. It helps you to understand how and why, as a CCG, we use your data and to provide reassurance that we are doing so lawfully. In addition, you can check your data for accuracy.

5.2 An individual and / or their legal representative are the only people who can request access to their personal data processed by the CCG.

5.3 The table below provides outlines how requests from individuals can be made including information about fees, identity checks and requests made on behalf of others.

The Right of Access	
How can the request be made?	The request can be made verbally or in writing to any part of the organisation and it does not have to state it is a subject access request or refer to GDPR as long as the individual is requesting access to their own personal data. If the request is made verbally (via the telephone) we may need to check the validity of the request, to ensure we are dealing with the right person. Obtaining a request in writing assists us in understanding your request fully. This can prevent disputes about how the request has been interpreted and is why we prefer you to complete our request form.

What is the timescale for complying with a request?	We have one calendar month to respond. This is calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.
Can the timescale be extended?	We may need to extend the deadline by a further two months if the request is complex or if a number of requests have been received from the individual. The individual will be informed of this within one month of receipt of the request, with an explanation as to why the extension is necessary.
Can a fee be charged?	No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee will be charged.
Can ID be requested?	Yes, if the organisation is unsure of the identity of the individual. The period for responding to the request begins when we receive the additional information.
Can a third party make a request?	Yes, a subject access request can be made via a third party. This could be a solicitor acting on behalf of a client or an individual who feels more comfortable allowing someone else to act for them. If a third party is making the request, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual. A written authority or general power of attorney document will be requested to support this.
Requests where an individual lacks mental capacity	There are no specific provisions in the GDPR but the Mental Capacity Act 2005 enables a third party to exercise subject access rights on behalf of such an individual.
Requests for access to children's data	Where a child is competent, they are entitled to make or consent to a SAR to access their record. 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. When assessing a child's competence, we will explain the issues in a way that is suitable for their age.

Actions required if a request is refused.	If it is decided to refuse or reject a subject access request, the individual will be informed within one month of receipt of the request. The individual will be informed of the reason for the refusal and the details of the ICO, if they wish to make a complaint.

5.4 GDPR also recommends that where possible, provision for remote access to a secure self-service system to provide an individual with direct access to his or her information. For the CCG, this wouldn't apply as records are not stored in such a way, but for a GP practice, patient online access to the medical records offers this solution.

5.5 All subject access requests should be referred to the CCG SAR Lead: HMRCCG.SAR@nhs.net

6. The right to rectification

6.1 Individuals have the right to have inaccurate personal data rectified. 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.

6.2 Steps may have already been taken to ensure that the personal data was accurate when obtained, but this right imposes a specific obligation to reconsider the accuracy upon request.

6.3 If a request for rectification is received, and if we agree the data is inaccurate, then we will rectify the data.

6.4 Determining whether personal data is inaccurate can be complex, especially if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is accurate and should be kept. In such circumstances, the fact that a mistake was made will be noted in the individual's file and will not be deleted.

6.5 It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective and it can be difficult to conclude that the record of an opinion is

inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

6.6 While the case is being considered, individuals also have the right to request restriction of the processing of their personal data. This is while they contest its accuracy and while it's being checked. As a matter of good practice, processing of the data in question will be restricted whilst the data is verified, whether or not the individual has exercised their right to restriction.

6.7 If you are satisfied that the personal data is accurate and does not require rectification, you will be informed of this and that there will be no amendment to your data. The decision for refusal will be explained and if you are unhappy with this decision, you have the right to make a complaint to the ICO.

6.8 A request for rectification can be refused if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive. If we consider that a request is manifestly unfounded, or excessive, we will either charge a reasonable fee to deal with the request or refuse it. If we decide to charge a fee, we will contact you within one month. We do not need to respond to the request until we have received the fee.

The Right to Rectification	
How can the request be made?	The request can be made verbally or in writing to any part of the organisation and it does not have to mention the phrase 'request for rectification,' as long as the individual has challenged the accuracy of their data or has asked that we take steps to complete data held about them that is incomplete. If a verbal request is made, we have a legal responsibility to identify that an individual has made a request.
What is the timescale for complying with a request?	We have one calendar month to respond which is calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.
Can the timescale be extended?	We may need to extend the timescale by a further two months if the request is complex or a number of requests have been received from the individual. The individual will be informed within one month of receiving their request and explain why the extension is necessary.

Can a fee be charged?	No fee is charged unless the request is ***proved*** to be manifestly unfounded or excessive. If it is decided it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee will be charged.
Can ID be requested?	Yes, it is important that the identity of the individual is confirmed.

6.10 If personal data has been disclosed to others, each recipient will be contacted and informed of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort.

6.11 There are some exemptions from the right to rectification which are broadly associated with the reason data is being processed. For more information about this and the right to rectification, please refer to the ICO website on the link below:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

7. The right to erasure ("the right to be forgotten")

7.1 Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances which are as follows:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for
- The lawful basis for holding the data was **consent** and the individual now withdraws their consent
- Legitimate interests was the basis for processing, and the individual objects to the processing of their data and there is no overriding legitimate interest to continue this processing
- The personal data is being processed for direct marketing purposes and the individual objects to that processing
- The data is being processed unlawfully
- There is a duty to comply with a legal obligation to have the data erased
- The personal data is being processed to offer information society services to a child.

7.2 Please note the right to erasure does not apply for healthcare data processed by the CCG. Consent is not a legal basis for processing personal data for direct care and administration in the NHS and therefore this right does not apply. Even if this right

applied (thus if consent was obtained), it would become problematic to deliver effective care and treatment to patients if, for example, some of their previous medical history had been deleted. This would impose a high patient safety risk.

The Right to Erasure	
How can the request be made?	The request can be made verbally or in writing to any part of the CCG and it does not have to include the phrase 'request for erasure.'
What is the timescale for complying with a request?	The CCG has one calendar month to respond which is calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.
Can the timescale be extended?	The timescale to respond can be extended by a further two months if the request is complex, or a number of requests have been received from the individual. The individual will be informed within one month of receiving their request and explain why the extension is necessary.
Can a fee be charged?	No fee is charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee will be charged.
Can ID be requested?	Yes, it is important that the identity of the individual is confirmed.
Requests for access to children's data	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 GDPR. For further details about the right to erasure and children's personal data please refer to the ICO guidance regarding children's privacy at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/
Actions required if a request for erasure is refused.	If a request for erasure is refused, the individual will be informed within one month of receipt of the request. We will also inform the individual of the reason for refusal and their right to make a compliant to the ICO, along with their ability to enforce this right through a judicial remedy.

7.3 GDPR specifies two circumstances where other organisations need to be informed about the erasure of personal data:

- Where the personal data has been disclosed to others - each recipient of this will be contacted and informed of the erasure, unless this proves impossible or involves disproportionate effort.
- The personal data has been made public in an online environment (for example on social networks, forums or websites). Steps will 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 will take into account available technology and the cost of implementation.

7.4 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.

7.5 GDPR also specifies two circumstances where the right to erasure will not apply to special category (sensitive) data:

- If the processing is necessary for public health purposes in the public interest (e.g. 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)
- 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 (eg a health professional).

8. The right to restrict processing

8.1 GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

8.2 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 you hold or how the data has been processed. In most cases, it will not be required to restrict an individual's personal data indefinitely, but there will need to have the restriction in place for a certain period of time.

8.3 Individuals have the right to request restriction of the processing of their personal data in the following circumstances:

- The individual contests the accuracy of their personal data and you are verifying the accuracy of the data
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead
- You no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to you processing their data and you are considering whether your legitimate grounds override those of the individual.

8.4 Although this is distinct from the right to rectification and the right to object, there are close links with those rights as per below:

- If an individual has challenged the accuracy of their data and asked for you to rectify it, they also have a right to request you restrict processing while you consider their rectification request; or
- If an individual exercises their right to object, they also have a right to request you restrict processing while the objection is considered.

The Right to Restrict Processing	
How can the request be made?	The request can be made verbally or in writing to any part of the organisation and it does not have to include the phrase 'request for restriction.'

What is the timescale for complying with a request?	We will act upon the request within one month of receipt calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month. This may be extended by a further two months if the request is complex or you have received a number of requests from the individual. We will let the individual know within one month of receiving their request and explain why the extension is necessary.
Can a fee be charged?	In most cases a fee is not charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee will be charged. If a fee is requested, we will not comply with the request until the fee is received.
Can ID be requested?	If we have doubts about the identity of the person making the request, we will ask for more information from the individual and we will not comply with the request until we have received the additional information.

8.5 As good practice, processing of the data will be restricted whilst the accuracy or the legitimate grounds for processing the personal data in question is considered.

8.6 Processes that enable restriction of personal data will be in place to do this, if required.

8.7 The definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data.

8.8 To restrict data we may need to:

- Temporarily move the data to another processing system;
- Make the data unavailable to users; or
- Temporarily remove published data from a website.

8.9 Once the data is restricted, processing will cease except to store it and unless:

- The individual has consented;
- 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.

8.10 If the personal data in question is disclosed to others, each recipient will be contacted and informed of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the individual will be informed about these recipients.

8.11 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 you are investigating this; or
- The individual has objected to you 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 you are considering whether your legitimate grounds override those of the individual.

8.12 Once a decision has been made on the accuracy of the data, or whether legitimate grounds override those of the individual, a decision can be made to lift the restriction. If this is the case the individual will be informed before the restriction is lifted.

8.13 As noted above, these two conditions are linked to the right to rectification. This means that we will inform an individual that the restriction is being lifted (on the grounds that we are satisfied that the data is accurate, or that your legitimate grounds override theirs), then the individual will be informed of the reasons for the refusal to act upon their rights. You will also be informed of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy.

9. The right to data portability

9.1 The right to data portability gives individuals the right to receive personal data they have provided to a controller (the CCG) in a structured, commonly used and machine readable format. It also gives the right to request that a controller transmits this data directly to another controller.

9.2 The right to data portability applies when:

- The lawful basis for processing the information is consent **or** for the performance of a contract; and
- Processing is being carried out by automated means (i.e. excluding paper files).

9.3 Examples of where this right may be exercised include the history of website usage or search activities, traffic and location data; or ‘raw’ data processed by connected

objects such as smart meters and wearable devices.

9.4 It does not include any additional data created, based on the data an individual has provided. For example, if data is provided by an individual to create a user profile then this data would not be in scope of data portability.

9.5 The right to data portability only applies to personal data and not anonymous data. However, pseudonymised data that can be clearly linked back to an individual (e.g. where that individual provides the respective identifier) is within scope of the right.

9.6 The right to data portability entitles an individual to receive a copy of their personal data; and / or have their personal data transmitted from one controller to another controller.

9.7 Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store. This can be achieved by either:

- Directly transmitting the requested data to the individual; or
- Providing access to an automated tool that allows the individual to extract the requested data themselves.

9.8 This does not create an obligation to allow individuals more general and routine access to systems – only for the extraction of their data following a portability request. There may be a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, both methods will be secure.

9.9 Individuals have the right to ask to transmit their personal data directly to another controller without hindrance.

9.10 The technical feasibility of a transmission should be considered on a request by request basis. The right to data portability does not create an obligation to adopt or maintain processing systems which are technically compatible with those of other organisations. However, a reasonable approach should be taken, and this should not generally create a barrier to transmission.

9.11 If data is provided to an individual, it is possible that they will store the information in a system with less security than the CCG. Individuals should be aware of this so that they can take steps to protect the information they have received.

9.12 The personal data will be provided in a format that is structured, commonly used and machine-readable.

9.13 When personal data is received that has been transmitted as part of a data portability request, this will be processed in line with data protection requirements.

9.14 In deciding whether to accept and retain personal data, consideration should be taken as to whether the data is relevant and not excessive in relation to the purposes for which it will be processed. There also needs to be consideration as to whether the data contains any third-party information.

9.15 New controllers need to ensure that there is an appropriate lawful basis for processing any third-party data and that this processing does not adversely affect the rights and freedoms of those third parties. If personal data is received which there is no reason to keep, it should be deleted as soon as possible. When data is accepted and retained, it becomes the controller's responsibility to ensure compliance with the requirements of the GDPR.

The Right to Data Portability	
How can the request be made?	The request can be made verbally or in writing to any part of the organisation and it does not have to include the phrase 'request for data portability'.
What is the timescale for complying with a request?	The CCG has one calendar month to respond which is calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.
Can the timescale be extended?	The timescale to respond can be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual will be informed within one month of receiving their request and explain why the extension is necessary.
Can a fee be charged?	No fee is charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee will be charged.
Can ID be requested?	If we have doubts about the identity of the person making the request, we will ask for more information.
Actions to be	We can refuse to comply with a request for data portability

taken if the request is refused	if it is manifestly unfounded or excessive, also taking into account whether the request is repetitive in nature. If the request is refused, the individual will be informed without undue delay and within one month of receipt of the request along with the reasons we are not taking action. We will explain the right individuals have to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy. Or we may request a "reasonable fee" to deal with the request.

10. The right to object

10.1 GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask the CCG to stop processing their personal data.

10.2 Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

10.3 Individuals can also object if the processing is for:

- A task carried out in the public interest
- The exercise of official authority vested in you
- Your legitimate interests (or those of a third party).

In these circumstances, the right to object is not absolute.

10.4 If processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

10.5 Direct Marketing - An individual can ask that the CCG stop processing their personal data for direct marketing at any time. The CCG does not undertake direct marketing at time of writing.

10.6 This is an absolute right and there are no exemptions or grounds for refusal. Therefore, when an objection to processing for direct marketing is received processing the individual's data for this purpose will stop.

10.7 However, this does not automatically mean that the individual's personal data should be erased and, in most cases, it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

10.8 An individual will give specific reasons why they are objecting to the processing of their data when this has been processed for a task carried out in the public interest or official authority and / or in your legitimate interests. These reasons should be based upon their particular situation. In these circumstances, this is not an absolute right and processing can continue if:

- Compelling legitimate grounds for the processing can be demonstrated, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

10.9 If deciding whether there are compelling legitimate grounds which override the interests of an individual, the reasons why they have objected to the processing of their data should be considered.

10.10 In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (e.g. the processing is causing them financial loss), the grounds for their objection will have more weight.

10.11 In making a decision on the individual's interests, the rights and freedoms should be balanced with the CCG's own legitimate grounds. During this process, the organisations will document and demonstrate that their legitimate grounds override those of the individual.

10.12 If the CCG are satisfied that processing the personal data in question does not need to stop, the individual will be informed of this decision and informed of their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce their rights through a judicial remedy.

10.13 Processing for archiving / scientific / historical research / statistical purposes - Where processing personal data for these purposes, the right to object (including the right of access, rectification and restriction on processing) is more restricted and the Data Protection Act 2018 allows the UK to provide derogations from these rights if it is likely to render impossible or seriously impair the achievement of the specific purposes.

10.14 The Data Protection Act 2018 sets out exemptions for this processing. The DPA 2018 provides safeguards to ensure that personal data is not processed by researchers to support measures or decisions with respect to particular individuals

and is not processed in such a way as will or is likely to cause substantial damage or distress to anyone.

10.15 If an objection is received, it might be possible for processing to continue if it can be demonstrated that there is a compelling legitimate reason or the processing is necessary for legal claims.

10.16 If it is decided the processing should not cease, the individual should be informed of this decision with an explanation and information relating to their right to make a complaint to the ICO or another supervisory authority, as well as their ability to seek to enforce their rights through a judicial remedy.

The Right to Object	
How can the request be made?	The request can be made verbally or in writing to any part of the organisation and it does not have to include the phrase 'objection to processing.' It can also be made to any part of your organisation and does not have to be to a specific person or contact point.
What is the timescale for complying with a request?	We will act upon the request within one month of receipt calculated from the same day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month. This can be extended by a further two months if the request is complex or you have received a number of requests from the individual. We will let the individual know within one month of receiving their request and explain why the extension is necessary.
Can a fee be charged?	No, a fee is not charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided it is manifestly unfounded or excessive or further copies are requested, a reasonable admin fee can be charged.
Can ID be requested?	If we have doubts about the identity of the person making the request, we will ask for more information from the individual, but this will be done within one month. The period for responding to the objection begins when the information is received.
Grounds for	We can refuse to comply with a request if it is manifestly

refusal / actions to be taken if the request is refused	unfounded or excessive also taking into account whether the request is repetitive in nature. If the request is refused, the individual will be informed within one month of receipt of the request along with the reasons we are not taking action. You have the right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy. We will request a "reasonable fee" to deal with the request.

10.17 GDPR states that individuals will be informed of their right to object at the time of the first communication with them (via Privacy Notice) where:

- Personal data is processed for direct marketing purposes,

Or the lawful basis for processing is:

- Public task (for the performance of a task carried out in the public interest),
- Public task (for the exercise of official authority vested in you), or
- Legitimate interests.

10.18 If one of the conditions above applies, the right to object should be brought, explicitly, to the individual's attention. This information should be presented clearly and separately from any other information.

10.19 Where an objection to the processing of personal data is received and there are grounds for refusal the processing will stop. This could mean that personal data may need to be erased but this may not be appropriate data if there is a need to retain the data for those purposes. For example, when an individual objects to the processing of their data for direct marketing, their details can be placed onto a suppression list to ensure that the organisation continues to comply with their objection. However, the data will be clearly marked so that it is not processed for purposes the individual has objected to.

11. The right to prevent automated individual decision-making including profiling

11.1 Automated individual decision-making and profiling is a decision made by automated means without any human involvement. Examples of this include an online decision to award a loan; and a recruitment aptitude test which uses pre-programmed algorithms and criteria.

11.2 Automated individual decision-making does not have to involve profiling, although it

often will do. The GDPR says that profiling is:

"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."

11.3 Organisations use profiling to find something out about individuals' preferences, predict their behaviour and make decisions. Automated individual decision-making and profiling can lead to quicker and more consistent decisions, but if they are used irresponsibly there are significant risks for individuals.

11.4 GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

11.5 Automated decision-making can be carried out when this 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.

11.6 If processing special category personal, we can only carry out processing if:

- There is individual's explicit consent; **or**
- The processing is necessary for reasons of substantial public interest

11.7 Decisions based solely on automated processing about children will not be made if this will have a legal or similarly significant effect on them. Please refer to the ICO Guide on Children: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

11.8 Automated decision-making including profiling is considered to be high-risk processing therefore GDPR requires that a Data Protection Impact Assessment (DPIA) is completed. This will identify potential risks in order to have a plan in place to mitigate them.

As well as restricting the circumstances in which we can carry out solely automated individual decision-making, GDPR also:

- Requires individuals are provided with specific information about the processing;
- Are obliged to take steps to prevent errors, bias and discrimination; and
- Gives individuals rights to challenge and request a review of the decision.

11.9 These provisions are designed to increase individuals' understanding of how we might be using their personal data. We will ensure that we:

- 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;
- Ensure that individuals can obtain human intervention / express their point of view; and obtain an explanation of the decision and challenge it;
- Put appropriate technical and organisational measures in place, so that we 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.

12. The right to withdraw consent (where used as the legal basis for processing)

12.1 One of the legal basis for processing personal data is consent. GDPR sets a high standard for consent. It must be freely given, unambiguous and involve a clear affirmative action (an opt-in) and records kept to demonstrate consent. Pre-ticked opt-in boxes cannot be used and consent should be separate from other terms and conditions.

12.2 The right to withdraw consent - GDPR gives data subjects a specific right to withdraw consent where this is used as a legal basis for processing. This right will be clearly communicated (for example, via our privacy notices / consent forms etc) and there will be easy and user friendly methods available and amenable to withdraw consent at any time.

13. The right to lodge a complaint with the ICO

13.1 GDPR gives data subject the right to lodge a complaint with a supervisory authority (the Information Commissioner's Office (ICO)) where an individual considers that the

processing of personal data relating to him or her infringes this regulation.

13.2 Complaints relating to the way the CCG have processed personal data should be directed in the first instance to the CCG's Data Protection Officer (DPO) at the details below:

Karen Hurley (CCG Director of Operations, Executive Nurse and DPO)
Email: hmrccg.dpo@nhs.net

Postal address: NHS HMR CCG, PO Box 100, Rochdale, OL16 9NP

13.3 If an individual is unhappy with the response given, they have the right to make a complaint to the Information Commissioner's Office (ICO) via the contact details below:

- Website - https://ico.org.uk/make-a-complaint/ for more information relating to making a complaint
- Telephone: 0303 123 1133