Bolton Clinical Commissioning Group

Individual Rights Procedure

Policy Number	**IG019**
Target Audience	**All staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**October 2018**
Last Review Date	**October 2018**
Next Review Date	**October 2020**
Policy Author	**GMSS IG Team**
Version Number	**V1.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2018	GMSS IG Team	First Draft
1.0	August 2018	IG Board	Approved

Analysis of Effect completed:	By:	Date:

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 procedure is to provide guidance to all Bolton CCG (henceforth referred to as "the CCG") employees on the rights of an individual under the GDPR.

2. Scope

2.1 This procedure applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority / honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. In addition, this procedure applies to all third parties and others authorised to undertake work on behalf of the CCG.

3. Definitions

3.1 **General Data Protection Regulation 2016 (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.

3.2 **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.

3.3 **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.

3.4 **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 (formally known as Sensitive Data). 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/

3.5 **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'.

3.6 **One calendar month** - This is calculated from the day after a request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month. For example - If a request is received a request on 30th March the time limit starts from the next day (31 March). As there is no equivalent date in April the date for compliance is the 30th April. 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.

3.7 **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.

4. Individual Rights under GDPR

4.1 The GDPR provides the following rights for individuals:

- The right to be informed (Article 12, 13 & 14)
- The right of access (Article 15)
- The right to rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 22)
- The right to withdraw consent (Article 7)
- The right to complain (Article 77)

5. The right to be informed

5.1 Articles 12, 13 and 14 of the GDPR relates to an individual's right to be informed. 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); be written in clear and plain language (particularly if addressed to a child) and provided free of charge. This is often referred to as a "Privacy Notice."

What information must be provided to individuals?

5.2 The following information under GDPR is required to be provided to individuals in a Privacy Notice.

- Name and contact details of the CCG (Data Controller).
- Data Protection Officer contact details
- Purpose/s of processing activities.
- Lawful basis for processing activities
- Legitimate interests for processing (if applicable)
- Categories of personal data processed
- Recipients or categories of recipients of the personal data
- Details of transfers of the personal data to any third countries or international organisations (if applicable).
- Retention periods for the personal data (how long we will hold the information and how we will decide on the retention period)
- Rights available to individuals in respect of the processing
- Details regarding the right to withdraw consent (if applicable)
- The right to lodge a complaint with the ICO
- Source of the personal data (if the personal data is not obtained directly from the individual it relates to).
- Details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable)
- Consequences for failure to provide information to the Data Controller
- Details of the existence of any automated decision-making, including profiling (if applicable)

5.3 A Privacy Notice must be provided to individuals at the time personal data is collected from them.

5.4 If personal data is obtained from other sources, individuals must be provided with "Privacy Notice" information within a reasonable period of obtaining the data and no later than one month.

5.5 Regular reviews should be undertaken to check the privacy notice remains accurate and up to date. If personal data is used for any new purpose(s) or the way data is being processed is changed, the privacy notice must be updated as soon as possible. These changes / updates must be communicated to citizens as soon as possible.

5.6 There are some circumstances when Privacy Notice information does not have to be supplied as detailed below:

- If an individual already has the information or if it would involve a disproportionate effort to provide it to them
- Providing the information to the individual would be impossible
- Providing the information to the individual would involve a disproportionate effort
- Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing
- There is a legal requirement to obtain or disclose the personal data
- The organisation is subject to an obligation of professional secrecy regulated by law that covers the personal data.

5.7 Privacy Notice information can be communicated by using a combination of different techniques including publishing on websites / intranets / notice boards, providing hard copy information via leaflets / posters and communications / briefing's to the public and staff.

5.8 User testing / public engagement is a good way to obtain feedback on how effective the delivery of privacy notice information is.

5.9 Being open and transparent helps to comply with other aspects of GDPR and build trust, but failure to inform citizens could potentially impose penalties from the ICO (as you can now be fined for breaching the GDPR principles) and lead to reputational damage.

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/

5.10 The CCG have updated their Privacy Notice in line with the GDPR requirements and published it on the CCG's website. The full Privacy Notice can be found at the following link:
https://www.boltonccg.nhs.uk/how-we-do-things/how-we-use-your-information

6. The right of access

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

6.2 An individual and / or their legal representative are the only people who can request

access to their personal data processed by the CCG.

6.3 The table below provides outlines how the request from an individual can be made including information about fees, identity checks and requests made on behalf of another individual.

The Right of Access – Article 15 of the GDPR	
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 Article 15 of the GDPR as long as the individual is requesting access to their own personal data. If the request is made verbally (via the telephone), it is good practice to have a process for recording details of this request. It is highly recommended to confirm the request in writing so you can then check the validity of the request, for example, their identification as this could be anyone calling to make a request. Obtaining a request in writing also assists to confirm with the requester that you have understood their request fully. This can prevent disputes about how the request has been interpreted.
What is the timescale for complying with a request?	The CCG has one calendar month to respond. This is calculated from the day after 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 if a number of requests have been received from the individual. The individual must be informed within one month of receipt of their 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 can be charged. If challenged this fee must be justified.
Can ID be requested?	Yes if you are unsure of the identity of the individual. This should be requested (as soon as possible) to provide enough information to enable you to confirm their identity. The period for responding to the request begins when you

	receive the additional information.
Can a third party make a request?	Yes, a Subject Access Request (SAR) 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 you 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 should be requested.
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, it is important to explain the issues in a way that is suitable for their age. Where, in the view of the appropriate health professional, a child lacks competency to understand the nature of his or her SAR application, the holder of the record is entitled to refuse to comply with the SAR. Where a child is considered capable of making decisions about access to his or her medical record, the consent of the child must be sought before a parent or other third party can be given access via a SAR.
Actions required if a request is refused.	If it is decided to refuse or reject a Subject Access Request, the individual must be informed without undue delay and within one month of receipt of the request. The individual must be informed of the reason for refusal and their right to make a complaint to the ICO. They can also if required enforce this right through a judicial remedy.

6.4 Recital 59 and 63 of the GDPR recommends that organisations 'provide means for requests to be made electronically, especially where personal data are processed by electronic means'. A Subject Access form that allows individuals to make their request via an electronic form to the CCG (if they wish to do so) will be emailed to the individual.

6.5 It must be noted that although an individual may use an application form, it must be made clear that this is not compulsory and it must not be used to extend the one month time limit for responding.

6.6 An individual must also be provided with information about data processing activities within the CCG when responding to a Subject Access Request. This information is outlined in the CCG's Privacy Notice. Therefore, a copy of the Privacy Notice must be provided with the information requested back to the individual requesting it. This will include information about data processing activities as per the Privacy Notice content detailed in the section above.

6.7 If an individual makes a request electronically the information should be provided in a commonly used electronic format, unless the individual requests otherwise. For example, if an individual does request that information is provided in hard copy and posted out to them, then you must honour this request.

6.8 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 (Recital 63). For the CCG, this would not 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.

6.9 All Subject Access Requests should be referred to the CCG SAR Lead (via the generic SAR email at bolccg.quality-team@nhs.net) immediately where it will be logged and dealt with appropriately.

6.10 For further information regarding subject access and the process for the CCG, please refer to the CCG Subject Access Request Procedure which is located on the CCG at: http://www.boltonccg.nhs.uk/about-us/our-policies

7. The right to rectification

7.1 Individuals have the right to have inaccurate personal data rectified (Article 16 of the GDPR). The 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.

7.2 This right has close links to the accuracy principle of the GDPR (Article 5(1) (d)). 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.

7.3 If a request for rectification is received, steps must be taken to rectify the data if deemed necessary. All arguments and evidence provided by the data subject should be taken into account and documented for audit trail purposes.

7.4 Determining whether personal data is inaccurate can be complex 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, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made should be noted in the individual's file. It must not be deleted.

7.5 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.

7.6 While the case is being considered, individuals also have the right under Article 18 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 should be restricted whilst the data is verified whether or not the individual has exercised their right to restriction.

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

7.8 It is good practice to place a note indicating that the individual challenges the accuracy of the data and their reasons for doing so.

7.9 A request for rectification can be refused if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either charge a reasonable fee to deal with the request or refuse it. If you decide to charge a fee you should contact the individual without undue delay and within one month. You do not need to comply with the request until you have received the fee.

The Right to Rectification – Article 16 of the GDPR	
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' or refer to Article 16 of GDPR as long as the individual has challenged the accuracy of their data asked for it to be corrected, or has asked that you take steps to complete data held about them that is incomplete. If a verbal request is made this can be challenging but there

	is a legal responsibility to identify that an individual has made a request. Staff should receive specific training to identify a request and ensure details of the request are recorded. It is also good practice to check the detail of the request to ensure that the individuals request is understood. This should be formally logged as this can help avoid later disputes about the request has been interpreted.
What is the timescale for complying with a request?	The CCG has one calendar month to respond which should be calculated from the day after 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 by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain 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 it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged you must be able to justify this admin fee.
Can ID be requested?	Yes, it is important that the identity of the individual is confirmed and enough information to enable confirmation of their identity can be requested. This should not delay the timeframe for compliance.

7.10 If personal data has been disclosed to others, each recipient must be contacted and informed of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. The individual must also be informed about these recipients; this is highlighted in the Privacy Notice (refer to section 5).

7.11 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/

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

8.1 Individuals have the right to have personal data erased (Article 17 of the GDPR). 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 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 (i.e. in breach of the lawfulness requirement of the 1st principle)
- 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.

8.2 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 – Article 17 of the GDPR	
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' or Article 17 as long as one of the conditions listed in section 7.1 apply. If a verbal request is made this can be challenging but there is a legal responsibility to identify that an individual has made a request. It is advised that staff should receive specific training to identify a request and ensure details of the request are recorded. It is also good practice to check the detail of the request to ensure that you have understood their request. This should be formally logged as this can help avoid later disputes about the request has been interpreted.
What is the	The CCG has one calendar month to respond which should be

timescale for complying with a request?	calculated from the day after 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 by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain 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 it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged you must be able to justify this admin fee.
Can ID be requested?	Yes, it is important that the identity of the individual is confirmed and enough information to enable confirmation of their identity can be requested. This should not delay the timeframe for compliance.
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. Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent. 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 must be informed without undue delay and within one month of receipt of the request. You must 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.

8.3 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 must 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 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 you should take into account available technology and the cost of implementation.

8.4 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

8.5 The GDPR also specifies two circumstances where the right to erasure will not apply to special category data (see 3.4 for definition):

- 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 (egg a health professional).

9. The right to restrict processing

9.1 Article 18 of the 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.

9.2 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.

9.3 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 (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) 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 under Article 21 (the right to object), and you are considering whether your legitimate grounds override those of the individual.

9.4 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 (Article 16), 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 under Article 21(1), they also have a right to request you restrict processing while the objection is considered.

The Right to Restrict Processing – Article 18 of the GDPR	
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' or refer to Article 18 of the GDPR.
What is the timescale for complying with a request?	You must act upon the request without undue delay and at the latest within one month of receipt calculated from the day after you receive the request (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. You must let the individual know within one month of receiving their request and explain why the extension is necessary.
Can a fee be	In most cases a fee cannot be charged unless the request

charged?	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. If challenged you must be able to justify this admin fee. If a fee is requested you do not need to comply with the request until you have received the fee.
Can ID be requested?	If you have doubts about the identity of the person making the request you can ask for more information from the individual but this must be done without undue delay and within one month. You do not need to comply with the request until you have received the additional information.

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

9.6 Processes that enable restriction of personal data should be in place to do this if required.

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

9.8 The GDPR suggests a number of different methods that could be used to restrict data, such as:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from a website.

9.9 It is particularly important that consideration is taken as to how personal data that you no longer need to process is stored and but where the individual has requested you restrict (effectively requesting that you do not erase the data).

9.10 If using an automated filing system, technical measures must be used to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. A note should be placed on the system that the processing of this data has been restricted.

9.11 Once the data is restricted, processing must 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.

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

9.13 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.

9.14 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 must be informed before the restriction is lifted.

9.15 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 you inform an individual that the restriction is being lifted (on the grounds that you are satisfied that the data is accurate, or that your legitimate grounds override theirs), then the individual should be informed of the reasons for the refusal to act upon their rights under Articles 16 or 21. They should 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.

10. The right to data portability

10.1 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 them the right to request that a controller transmits this data directly to another controller.

10.2 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).

10.3 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.

10.4 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. Please note this data would need to be provided it to an individual if they make a Subject Access Request. In addition, it would be good practice to include this data in a response for data portability.

10.5 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.

10.6 If the requested information includes information about others (e.g. third party data) consideration would need to be taken whether transmitting that data would adversely affect the rights and freedoms of those third parties.

10.7 If the requested data has been provided by multiple data subjects (e.g. a joint bank account) all parties need to agree to the portability request. This means that agreement will have to be sought from all the parties involved.

10.8 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.

10.9 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.

10.10 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 must be secure.

10.11 Individuals have the right to ask you to transmit their personal data directly to

another controller without hindrance. If it is technically feasible this should be done.

10.12 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 (GDPR Recital 68). However, a reasonable approach should be taken and this should not generally create a barrier to transmission.

10.13 If you provide information directly to an individual or to another organisation in response to a data portability request, you are not responsible for any subsequent processing carried out by the individual or the other organisation. However, you are responsible for the transmission of the data and need to take appropriate measures to ensure that it is transmitted securely and to the right destination.

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

10.15 Other provisions in the GDPR must be complied with. For example, whilst there is no specific obligation under the right to data portability to check and verify the quality of the data transmitted, reasonable steps should already be in place to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the GDPR.

10.16 The personal data must be provided in a format that is structured, commonly used and machine-readable. These terms are not defined in the GDPR however the following document titled “Open Data Handbook” explains these further, please click on the link below to view:

http://opendatahandbook.org

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

10.18 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.

10.19 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 - Article 20 of the GDPR	
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 or refer to Article 20 of the GDPR.
What is the timescale for complying with a request?	An organisation has one calendar month to respond which should be calculated from the day after 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 by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain 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 it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged you must be able to justify this admin fee and the individual should be informed promptly of this.
Can ID be requested?	If you have doubts about the identity of the person making the request you can ask for more information.
Actions to be taken if the request is refused	You can refuse to comply with a request for data portability 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 must be informed without undue delay and within one month of receipt of the request along with the reasons you are not taking action and their 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. Or/ you can request a "reasonable fee" to deal with the request. In either case you will need to justify your decision

For more information relating to data portability please refer to articles 13, 20 and recital 68.

11. The right to object

11.1 Article 21 of the 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.

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

11.3 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.

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

11.5 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.

11.6 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 must stop.

11.7 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.

11.8 An individual must 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.

11.9 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.

11.10 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.

11.11 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 must document and demonstrate that their legitimate grounds override those of the individual.

11.12 If the CCG are satisfied that processing the personal data in question does not need to stop, the individual should 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.

11.13 Processing for archiving / scientific / historical research / statistical purposes - Where processing personal data for these purpose, 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

11.14 The Data Protection Act 2018 (Part 6 of Schedule 2) sets out exemptions for this processing. Section 19 of 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.

11.15 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.

11.16 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 – Article 21 of the GDPR	
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' or refer to Article 21 of the GDPR. 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?	You must act upon the request without undue delay and at the latest within one month of receipt calculated from the day after you receive the request (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. You must 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 cannot be 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 you have doubts about the identity of the person making the request you can ask for more information from the individual but this must be done without undue delay and within one month. The period for responding to the objection begins when the information is received.
Grounds for refusal / actions to be taken if the request is refused	You can refuse to comply with a request 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 must be informed without undue delay and within one month of receipt of the request along with the reasons you are not taking action and their 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. Or/ you can request a "reasonable fee" to deal with the request. In either case you will need to justify your decision.

11.17 GDPR states that individuals must be informed of their right to object at the time of the first communication with them (via Privacy Notice information) 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.

11.18 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.

11.19 If processing personal data for research or statistical purposes information about the right to object (along with information about the other rights of the individual) should be included in the Privacy Notice.

11.20 Where an objection to the processing of personal data is received and there are grounds for refusal the processing must 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 must be clearly marked so that it is not processed for purposes the individual has objected to.

12. The right to prevent automated individual decision making including profiling

12.1 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.

12.2 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."***

12.3 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.

12.4 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."

12.5 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.

12.6 If processing special category personal , you can only carry out processing described in Article 22(1) if:

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

12.7 Decisions based solely on automated processing about children should 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/

12.8 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 you can carry out solely automated individual decision-making (as described in Article 22(1)), 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.

For further information on DPIA's and for a copy of the proforma please refer to the Privacy Impact Assessment Policy at:
http://www.boltonccg.nhs.uk/about-us/our-policies

12.9 These provisions are designed to increase individuals' understanding of how we might be using their personal data. We must 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 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.

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

13.1 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.

13.2 Inappropriate or invalid consent could destroy trust, harm the reputation of the CCG and thus the CCG may be subject to penalties / fines from the Information Commissioner's Office (ICO).

13.3 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 must be clearly communicated (for example, via Privacy Notices / consent forms etc) and there must be easy and user friendly methods available and amenable to withdraw consent at any time.

14. The right to lodge a complaint with the ICO

14.1 Article 77 of the 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. The ICO with which the complaint has been lodged will

inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78. For more detail please refer to Recital 141 and 143.

14.2 Individuals are informed about the right to lodge a complaint via the CCG's Privacy Notice for patients and for staff.

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

Michael Robinson
Michael.robinson1@nhs.net

14.4 If an individual is unhappy with the response given, they have the right to lodge their 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

Appendix A - Brief Guide to the Rights of an Individual under GDPR

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This underpins the principles of GDPR.

- Individuals must be provided with information regarding the processing of personal data – this is known as a “Privacy Notice”
- Privacy notice information must be provided to individuals at the time their personal data is collected from them.
- If personal data is obtained from other sources individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.
- Privacy notice information does not have to be provided if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information provided to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including websites, layering, dashboards, and communications. User feedback is a good way to get feedback on how effective the delivery of your privacy information is.
- The Privacy Notice must be regularly reviewed and where necessary updated. Any new uses of an individual’s personal data to their attention the processing starts.
- User testing should be undertaken to evaluate how effective privacy information is.
- Getting the right to be informed correct can help to ensure compliance with other aspects of the GDPR and build trust with people, but getting it wrong can leave the organisation open to fines and lead to reputational damage.

What should be provided in a Privacy Notice?

- The name and contact details of the organisation.
- The contact details of the data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).

- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

The right to access – subject access

Individuals have the right to access their personal data and this is commonly referred to as "subject access".

- The request for subject access can be made by an individual verbally or in writing. Please note if made verbally, it is highly recommended to request written confirmation of this
- The timeframe for compliance is one calendar month
- No, a fee cannot be charged unless the request can be proved to be **manifestly unfounded or excessive or further copies** are requested. If this is the case a reasonable admin fee can be charged however this fee must be justified.

An individual is entitled to:

- Confirmation that you are processing their personal data;
- A copy of their personal data requested; and
- Other supplementary information regarding data processing – this corresponds to the information that is detailed in the CCG Privacy Notice

The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- The request for rectification can be made by an individual verbally or in writing.
- The timeframe for compliance is one calendar month
- No, a fee cannot be charged unless the request can be proved to be **manifestly unfounded or excessive or further copies** are requested. If this is the case a reasonable admin fee can be charged however this fee must be justified.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5) (1) (d)).

The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as ‘the right to be forgotten’.

- The request for erasure can be made by an individual verbally or in writing.
- The timeframe for compliance is one calendar
- The right is not absolute and only applies if data is no longer required, processing is based on consent and this is withdrawn, data has been unlawfully processed, an individual objects and there is a need to have the data erased, the data has been deleted to comply with a legal obligation and where the data has been collected in relation to the offer of information society services

The right to request restriction

Individuals have the right to request the restriction or suppression of their personal data.

- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, the personal data can be stored but it must not be used.
- The request for restriction can be made by an individual verbally or in writing.
- The timeframe for compliance is one calendar
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).
- If there is a decision to lift a restriction on processing the individual must be told.
- If data is shared with any recipients and it is restricted those recipients must be told.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- It allows individuals to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to where processing is based on consent and processing is carried out by automated means.
- The request for data portability can be made by an individual verbally or in writing.
- The timeframe for compliance is one calendar month.

The right to object

The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies it may be possible to continue processing if it can be shown that there is a compelling reason for doing so.
- Individuals must be told about their right to object (included in Privacy Notices).
- An individual can make an objection verbally or in writing.
- The timeframe for compliance is one calendar month.

Rights related to automated decision making including profiling

The GDPR has provisions on:

- Automated individual decision-making and profiling
- Automated individual decision-making is making a decision solely by automated means without any human involvement
- Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process
- Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract; or authorised by Union or Member state law applicable to the controller or it is based on the individual's explicit consent.
- If any processing falls under Article 22 it must be identified and individuals MUST be informed and given information about the processing.

Appendix B – Further Information / Useful Links

- Information Commissioners Office (ICO)
  https://ico.org.uk/

- Information Governance Alliance (IGA)
  https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

- British Medical Association (BMA) – GDPR Guidance
  https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr

- Data Security and Protection Toolkit (DSPT)
  https://www.dsptoolkit.nhs.uk/

- The Data Protection Act 2018 (DPA 2018)
  https://www.gov.uk/government/collections/data-protection-act-2018

- The General Data Protection Regulation 2016 (GDPR)
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

- Health Research Authority (HRA)
  https://www.hra.nhs.uk/

- Open Data Handbook - published by Open Knowledge International and is a guide to 'open data'. The Handbook is updated regularly and you can read it here:
  http://opendatahandbook.org

- W3C candidate recommendation for XML:
  http://www.w3.org/TR/2008/REC-xml-20081126/

- W3C's specification of the JSON data interchange format
  https://tools.ietf.org/html/rfc7159

- W3C's list of specifications for RDF
  http://www.w3.org/standards/techs/rdf#w3c_all