NHS
Wigan Borough
Clinical Commissioning Group

WBCCG Right of Access Procedure

DOCUMENT CONTROL PAGE	
Title	Right of Access Procedure
Supersedes	Information Rights Procedure: Information Access Process
Minor Amendments	Renamed / reviewed to reflect change of timescale / changes regarding the meaning of 'manifestly unfounded or excessive' following a ruling in a Court of Justice of the European Union (CJEU case).
Author	Judith Blagbrough (Governance Manager) / Chris Lawless (Snr IG Officer)
Ratification	Information Governance Operational Group – 13th September 2019
Application	
Circulation	All CCG employees, including Contactors, Agency workers and volunteers
Review	September 2021

Date Placed on the Intranet/SharePoint:	**EqIA Registration Number**
Following Approval	N/A

Contents

Introduction

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

2. Article 15 of the GDPR provides all living individuals with the right to obtain a copy of their personal data as well as other supplementary information.

3. The purpose of this procedure is to provide guidance to all Wigan Borough Clinical Commissioning Group (CCG) employees with clear guidance on how to manage all incoming "Right of Access" requests (formerly referred to as a Subject Access Request - SAR).

Scope

4. 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.

5. This procedure is designed to reflect best practice in handling requests for information about an individual. Full implementation of this procedure will enable the CCG to:

   - Comply with its legal obligations under the Data Protection Act 2018 / GDPR
   - Increase levels of trust and confidence by being open with individuals about the information that is held about them.
   - Provide better 'customer care'.
   - Improve the transparency of organisational CCG activities in line with public policy requirements.
   - Enable individuals to verify that information held about them is accurate.

Responsibilities and Definitions

6. **The General Data Protection Regulation 2016 (GDPR)** – This is European Union (EU) legislation which became directly applicable to all member states in 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.

7. **The Data Protection Act 2018** – This sits alongside the GDPR and fills the 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 which is the UK's supervisory authority.

8. **The Information Commissioner** (ICO) – The ICO's Office is the UK's independent authority set up to promote access and protect personal information.

9. **Personal Data** – This contains details that identify individuals from one data item or a combination of data items. The following are demographic data items that are considered identifiable are name, address, NHS Number, full postcode, date of birth, identification number Under GDPR location data and online identifiers (IP address and cookies) are included as identifiable data items.

10. **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, biometric data (where used for identification purposes) and genetic data.

11. For more information about special category data please refer 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/

12. **Personal Confidential Data** – This term came out of 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 the deceased as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

13. **One month** – This is calculated from the day 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 on 30 March the time limit starts from the next day 31 March. As there is no equivalent date in April the date for compliance is 30 April. If the 30 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.

14. **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.

15. **Data Controller** – Data Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of persona data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

16. **Data Processor** – Processors act on behalf of, and only on the instructions of, the relevant controller.

Article 15 - Right of Access

17. Under the GDPR individuals have the "Right of Access" and can request a copy of and / or request to view personal data held about them by an organisation. It helps individuals to understand how and why the CCG process their personal data. It also provides assurances that the CCG are complying with the law and the principles. In addition, it can also be checked for accuracy.

18. An individual and / or their legal representative can request access to their personal data processed by the CCG.

19. The table below outlines the request process including fee information, identity checks and requests made on "behalf of another" individual.

Right of Access – Article 15	
How can the request be made?	A request can be made verbally or in writing (including by social media) to any part of the organisation and it does not have to state it is a "right of access request" or refer to Article 15 of the GDPR as long as the individual is requesting access to <u>their own</u> personal data. The request does not have to be addressed to a specific person or to a contact point. If the request is made verbally (for example, via the telephone) the CCG recommend that such a request is confirmed in writing (please refer to appendix 1 which can be used by the requestor and may assist with their request). A written request provides verification that the CCG has all the relevant and necessary information required to process the request in a timely manner. If the request does not contain sufficient information or the requestor has asked for everything you can ask the requestor to

	narrow down the scope or provide more detail in relation to their request. However, if the requestor is insistent with their full request this must be processed (unless an exemption applies).
Confirm or deny processing	An individual has the right to ask the CCG if they are processing any personal data concerning him / her. If this is confirmed then a request for access can be made if the requestor so wishes.
What is the timescale for complying with a request?	**The timescale is one month**. This is calculated from the day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month. If a request is received on the 4th June the request must be completed by the 4th July. If this is not possible because the following month is shorter (and there is no corresponding calendar date) the date for a response is the last day of the following month. If the corresponding date falls on a weekend or on a public holiday you have until the next working day to respond. If a request is received on the 31st of a month e.g. the 31st March the time limit starts on that day. As there is no equivalent date in April the organisation CCG have until the 30 April to comply with the request If you receive a request please contact the CCG Access Request Lead immediately at: Governance.Team@Wiganboroughccg.nhs.uk immediately. The clock starts ticking the day the request is received and every day counts!
Can the timescale be extended?	Yes, you can extend the time to respond 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 requestor know within one month of receiving their request and explain why the extension is necessary. It is good practice to have regular communications with the requestor to keep them updated.
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 require clarification of identity. This must be requested as soon as possible and sufficient information must be provided by the requestor to enable you to confirm the requestor's identity and also where a representative is submitting a request, the consent or legal justification for this. Please see appendix 2 for information regarding appropriate documentation to verify identity. The period for responding to the request begins when you receive the additional information.
Can a third party make a request?	Yes, a request for information 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, general power of attorney, or court order must be requested. For more detail in relation to third party requests please see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access
The data is in active and in use after the request is received and will be amended and changed during the request. Should we send out the "old" version?	A request relates to data held at the time the request was received. However, in many cases the routine use of the data may result in it being amended or even deleted while dealing with the request. ICO guidance states it would be reasonable to supply information held when the response is sent out even if this is different to that held when the request was received. However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under Section 173 of the Data Protection Act 2018 it is a criminal offence for the CCG or a person employed by the CCG to alter, deface, block, erase, destroy or conceal data with the intention of preventing disclosure of information that a data subject enforcing his / her rights would have been entitled to receive.
Requests where an individual lacks mental capacity	There are no specific provisions within GDPR but the Mental Capacity Act 2005 enables a third party to exercise the right of access on behalf of such an individual. You require proof that they have the legal powers to do this. They must have proof a

	Power of Attorney to manage property or affairs or be a person appointed by the Court of Protection.
Requests for access to children's data	In England competence is assessed depending upon the level of understanding of the child. When assessing a child's competence it is important to explain the issues in a way that is suitable for their age. Even if a child is too young to understand the implications of access rights it is still the "right" of the child rather than of anyone else such as a parent or guardian. So it is the child who has a 'right of access' to the information held about them even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them. Before responding to a request for information held about a child competency should be considered. Is the child is mature enough to understand their rights? If so then you can usually respond directly to the child. The parent can exercise the child's rights a child's behalf if the child authorises this or if it is evident that this is in the best interests of the child. What matters is that the child is able to understand what it means to make a request for access and how to interpret the information they receive as a result of doing so. When considering borderline cases take into account: • The child's level of maturity and their ability to make decisions like this • The nature of the personal data • Any court orders relating to parental access or responsibility • Any duty of confidence owed to the child or young person • Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment • Any detriment to the child or young person if individuals with parental responsibility cannot access this information • Any views the child or young person has on whether their parents should have access to information about them. Where, in the view of the appropriate health professional, a child lacks competency to understand the nature of the right to request access, the holder of the record is entitled to refuse to comply with the right of access request. Where a child is considered capable of making decisions about access to his or her personal data / medical record, the consent of the child must be sought before a parent or other third party can be request access. **Important always seek the advice / permission from the Caldicott Guardian, and the Data Protection Officer (DPO) in**

	<u>such cases before releasing any data relating to a child or a third party.</u> Please refer to ICO Guidance for more detail on requests relating to a child: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/
Actions required if a request is refused.	If it is decided to refuse or reject a right of 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 the refusal and their right to make a complaint to the ICO. They can also if required enforce this right through a judicial remedy.

20. Recital 59 and 63 of the GDPR states that organisation 'provide means for requests to be made electronically, especially where personal data are processed by electronic means'. A 'right of access' request facility (online form) allows individuals to make their request in an electronic format to the CCG (if they wish to do so). This is available via the CCG website and internal SharePoint site for staff requests.

21. It must be noted that completion of an application form is not compulsory and it must not be used to extend the time limit for processing.

22. If an individual makes a request electronically, the information is to be provided in a commonly used electronic format, unless the individual requests that information is provided to them in hard copy and posted out to them, the CCG must honour this request.

23. 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 doesn't apply at the moment as records are not stored in such a way. However for a GP practice, patient online access to the medical records offers this solution.

24. Article 15 states that an individual must also be provided with information about data processing activities within the CCG when responding to a subject access request. The privacy notice includes the information required under GDPR about data processing activities.

25. **<u>Therefore, the requestor must be provided with a copy of the appropriate CCG privacy notice along with the information requested.</u>**

Exemptions

Disclosure that may cause harm/third party information

26. Under the Data Protection (Subject Access Modification) Health Order 2000, the CCG has the right to deny patients access to all or part of their records if one of the following conditions applies.

27. If, in the opinion of the healthcare professional, disclosure of information is likely to cause serious harm to the physical or mental health or condition of the requestor.

28. Where records contain information that relates to an identifiable third party, the information may not be released unless:

    - The third party is a health professional who has complied or contributed to a health record, or who has been involved in the care of the individual.

    - The third party, who is not a health professional, gives their written consent to the disclosure of that information.

    - It is reasonable to dispense with the third party's consent (taking into account the duty of confidentiality owed to the other individual, any steps taken to seek his/her consent whether has been expressly refused).

29. All disclosure decisions must be documented (on the "Right of Access" Logbook). This information is required when disclosure is prevented in order to justify the decision to withhold information.

30. The CCG Caldicott Guardian / Data Protection Officer (DPO) must be advised and make the final decision if there appears to be any grounds for withholding information.

Child Protection/Safeguarding Concerns

31. There may be situations in which access to all or part of a child's health record can be refused – for example, where there are ongoing child protection issues, or where releasing information may put a child or young person at risk of harm. In these cases, advice must be sought from the appropriate managers and child protection professionals, as well as the Caldicott Guardian / DPO before releasing any information.

Records Relating to the Deceased

Access to Health Records Act 1990

32. Records relating to the deceased are not covered under the GDPR or the Data Protection Act 2018. A common law duty of confidentiality is owed to deceased person's records. For example, if the record contains a note made at the patient's request that they did not want a particular individual to know the details of their illness or their care, then no access should be granted to that individual. In addition, the record holder has the right to deny or restrict access if it felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

33. Records made after 1 November 1991 can be made available to a patient representative, executor or administrator via the Access to Health Records Act 1990. Any person with a claim arising from the death of a patient has a right of access to information specifically relating to the claim. The person making the request must explain why they need access to the records and to which part of the record supports their claim.

34. Checks regarding the deceased person's legal representative / executor or a will would need to be completed too in order to be satisfied the correct recipient has access / copies of records. Any wishes made in a will must be taken into consideration.

Requests made by Parties other than the data subject

Requests for access to records made by a patient representative

35. Any person can authorise a representative to request access to information held about them on their behalf. This must be completed in writing including confirmation of the representative's identity and the relationship to the requestor.

36. Representatives able to provide evidence that they are acting under a Power of Attorney (POA) or a Court of Protection Order will be granted the right to request access to information held about an individual.

37. Where an individual who is physically or mentally disabled and unable to provide written consent for a representative to seek access on their behalf the CCG will give the individual as much assistance as possible, in order to ascertain whether consent has been granted by other means to the representative.

Requests for access by other organisations

38. Various external organisations and agencies may request information held about an individual. In almost all cases staff must not share any information unless they have the consent from the individual or where there is legal justification to disclose the information. Examples of requests from other agencies are listed below:

Solicitors

39. Solicitors may apply to see information held about their client, but informed explicit and signed consent must first have been obtained from the individual before a copy of the information is released. The solicitor should be given access only to the information that would otherwise have been made available to the individual, subject to the restrictions stated above.

Court Orders

40. A Court may order disclosure of information. Unlike a request from a solicitor a Court Order should be obeyed unless there is a robust justification to challenge it. The Court's decision is law, unless the CCG decides to appeal the order and take the case to a higher Court in an attempt to override the Court's decision.

41. Courts and Coroners are entitled to request original records. If they do, copies of the records must be retained by the CCG. Coroners normally give sufficient notice for copies to be made, but do have the power to seize records at short notice, which may leave little or no time to take copies.

42. All Court Orders or documents linked to a Court Order must be forwarded **immediately** to the CCG Access Request Lead via the generic information access email address.

Requests made by the Police

43. Personal data can be disclosed to assist in the prevention or detection of crime and the apprehension of prosecution of offenders via the Data Protection Act 2018.

44. The individual should be asked (if possible) for their informed, explicit and signed consent to disclose the information, unless this would prejudice the enquiry or court case.

45. For any request where the CCG are to consider releasing any information without consent, the access request must relate to a serious crime in line within the Crime and Disorder Act 1998 (for example, murder or rape). If the CCG consider the crime to not be serious enough to warrant release without consent

the police should be advised to obtain a Court Order or written approved signed consent (see above regarding Court Orders).

46. Any request by the police for access to information held about an individual must be accompanied by the relevant consent and official letter / form signed by Chief Superintendent of the requesting police force or equivalent.

47. The CCG Access Request Lead should be notified immediately of any access requests by the police (via the information access email address).

Department of Work and Pensions

48. Any request by the Department of work and Pensions for access to any information held about an individual must be accompanied by the relevant form.

Parental Responsibility

49. Children have the same rights as adults over their personal data including the right to request access to their personal data.

50. Parents or those with parental responsibility will generally have the right to apply for access to information held about a child, although disclosure may be refused if the child is deemed competent and refuses to give consent.

51. Parental responsibility is defined in the Children Act 1998 as 'all the rights' duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his/her property'.

52. Married parents both have parental responsibility, unless a Court Order has removed that status from any party. A separated or divorced parent who no longer lives with the child has parental responsibility unless a Court has removed that status from either party.

53. Parental responsibility ensures if the child is in care or custody. It is lost, however, if the child is adopted.

54. If the parents are not married, only the mother automatically has parental responsibility. The father may acquire it in the following ways:

- Registering the birth, along with the mother, as the child's father (for children born after 1 December 2003)
- Formal agreement with the mother (section 4 of the Children Act 1989) - agreement can then only be brought to an end by a Court.
- Marrying the mother
- Obtaining a court order

- Obtaining a residence order

55. In practice, parental responsibilities would include:

    - Safeguarding a child's health, development and welfare
    - Financially supporting the child
    - Maintaining direct and regular contact with the child

56. Parental responsibility can also be acquired:

    - Through appointment as the child's guardian
    - By way of a residence order from the Court
    - By anyone having an Adoption Order made in their favour

57. Through Section 2 (9) Children Act 1989 – "A person who has parental responsibility for a child may not surrender or transfer any part of that responsibility to another but may arrange for some or all or it to be met by one or more persons acting on his behalf".

58. A Local Authority can acquire parental responsibility by:

    - Emergency protection order (Local Authority)
    - Interim or Full Care orders (Local Authority)

59. In this case the parents do not lose parental responsibility but the local authority can limit the extent to which a person exercises their parental responsibility.

60. Where, in the view of a health professional, the child is not capable of understanding the application for access to records, the CCG is entitled to deny access as being against their best interests.

61. Legally, young people aged 16 and 17 are regarded to be adults for the purposes of consent to treatment and the right to confidentiality. As such, if a person of this age wishes any information about them to be treated as confidential this wish should be respected and they have the right to deny parental access to information held about them.

62. For online services only and where consent applies, under GDPR (in the UK) the age of consent for children is 13 and over.

Individuals living abroad

63. A request for access to information held about an individual made from outside the UK will be treated in the same way as a request made from within the UK. People living outside of the UK have the same rights of access to information an organisation holds about them as UK residents do.

The Right of Access Process

64. All information for access requests must be referred IMMEDIATLEY to the Access Request Lead at: Governance.Team@Wiganboroughccg.nhs.uk) where it will be logged and dealt with appropriately.

65. It can also be submitted by post to. The Governance Team, Wigan Life Centre, College Avenue, Wigan WN1 1NJ.

66. All communications should be marked private and confidential and care should be taken not to include any personal data in the subject line of an email where this is used.

67. The 'Access Request Lead' will respond to the requestor to acknowledge the request and will log it on the 'Access' Request Logbook'.

68. The one month timeframe commences from the date the request is received so it is important the 'Access Request Lead' is made aware of the request on the day it is received as every day counts.

69. If further information or ID is required from the requestor in order to process the request the 'clock' on the one month timescale can be stopped until the information is received. Once the 'Access Request Lead' has received the required information from the requestor the timeframe will re-commence. The access request logbook must be maintained and kept updated to evidence this.

Collating the information

70. The Access Request Lead will liaise with relevant department's Information Asset Owner (IAO) to ensure the required information is collated in a timely manner.

71. Once IAO's have collated the information they should review and complete an 'Access Request Disclosure' form – Appendix 3. The information must then be sent securely to the 'Access Request Lead' via the generic email address (Governance.Team@Wiganboroughccg.nhs.uk).

72. Once the required 'Access Request Disclosure' form is received, the Access Request Lead will proceed to process the request ensuring they check:

- The legality of the request

- That any information which needs to be redacted has been redacted (e.g. third party information / information likely to cause serious harm etc.).

73. The 'Access Request Lead' will organise with the most appropriate person to review and authorise the right of access request using the 'Access Request Release Form'.

74. In the case of staff records the SIRO will approve and for patients records the Caldicott Guardian will approve. In some cases, the agreement of the Data Protection Officer (DPO) may also need to be sought.

Final response to the requestor

75. The 'Access Request Lead' will send out the final response to the requestor together with the information requested and a copy of the appropriate CCG Privacy Notice. Or, or a statement to state that the CCG does not hold the information requested.

76. The response should be sent back to the requestor in the format requested.

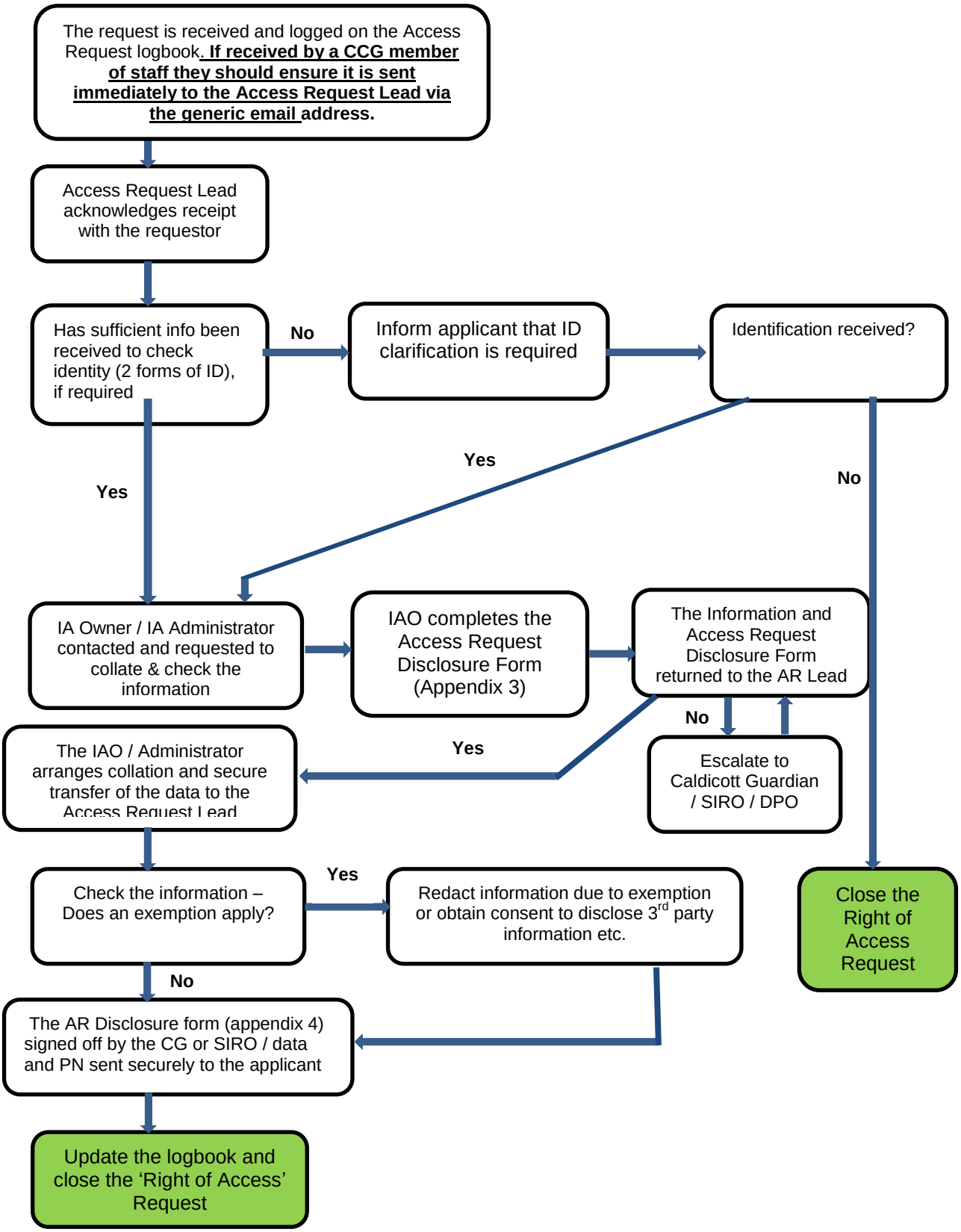
77. If email is used the information must be sent by NHS mail. If NHS mail is not an option then the [secure] method should be used which sends an encrypted email to a non-NHSmail account. Please refer to the Secure Transfers of Data Procedure which is located on SharePoint for more information.

78. If the method chosen is post, it should be sealed securely, marked private and confidential addressee only and sent by 'signed for' delivery.

Closure

79. Once the response has been sent to the requestor the 'Access Request Lead' the request can be marked as closed and the logbook updated accordingly.

80. Please refer to the flow chart on page 18 which also explains the information access process.


The request is received and logged on the Access Request logbook. If received by a CCG member of staff they should ensure it is sent immediately to the Access Request Lead via the generic email address.
Access Request Lead acknowledges receipt with the requestor
Has sufficient info been received to check identity (2 forms of ID), if required
No
Inform applicant that ID clarification is required
Identification received?
Yes
Yes
No
IA Owner / IA Administrator contacted and requested to collate & check the information
IAO completes the Access Request Disclosure Form (Appendix 3)
The Information and Access Request Disclosure Form returned to the AR Lead
No
Escalate to Caldicott Guardian / SIRO / DPO
Yes
The IAO / Administrator arranges collation and secure transfer of the data to the Access Request Lead
Check the information – Does an exemption apply?
Yes
Redact information due to exemption or obtain consent to disclose 3rd party information etc.
Close the Right of Access Request
No
The AR Disclosure form (appendix 4) signed off by the CG or SIRO / data and PN sent securely to the applicant
Update the logbook and close the 'Right of Access' Request

Monitoring and Reporting

81. The 'Access Request Lead' will routinely monitor the requests and report monthly statistics to the Senior IG Officer. This information will be fed through to the CCG Information Governance Operational Group (IGOG) and the Corporate Governance Committee (CGC) who will receive regular reports regarding the number of requests received and any issues relating to them such as difficulty obtaining information, internal reviews and complaints.

The Right to Lodge a Complaint

82. If an individual or their representative is not satisfied with the outcome of their request, for example, if they feel information has been withheld or recorded incorrectly, or that they have not been allowed sufficient time to view the information, they can lodge a complaint initially with the CCG and if unhappy with the outcome, this can then be raised with the Information Commissioners Officer (ICO).

83. The complaint/concern can be sent to the CCG's Data Protection Officer /Snr IG Officer at:

    Email: DPO@wiganboroughccg@nhs.uk
    Wigan Life Centre, College Avenue, Wigan WN1 1NJ

84. If the matter is not resolved the requestor can then escalate the matter to the Information Commissioner's Officer (ICO) at the details below, and may also seek independent legal advice.

    Information Commissioner's Office
    Wycliffe House
    Water Lane
    Wilmslow
    Cheshire SK9 5AF

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

    Telephone: 0303123 1133

Training

85. Specific training will be provided to the 'Access Request Lead'. Please refer to the CCG Data Security Training Needs Analysis for further details

Dissemination and Implementation

86. All staff are aware of the right of individuals to request access to information the CCG holds about them and the requirement of the CCG to respond within the statutory timeframe.

87. This procedure will be published on the CCG's SharePoint and awareness will be raised via staff briefings and regular communications.

Other Relevant Documents

88. This procedure should be read in conjunction with the following CCG policies:
    - Individual Rights Procedure
    - Data Security Protection and Confidentiality Policy
    - Records Management Policy
    - Secure Transfer of Data Procedure

Further information and 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

- 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

- The Data Protection (Subject Access Modification) (Health) Order 2000
  https://www.legislation.gov.uk/uksi/2000/413/contents/ma

- The General Data Protection Regulation
  https://gdpr-info.eu/

Appendix 1 – 'Right of Access' request form

Under the General Data Protection Regulation you have the right to request any personal information we may hold about you as an organisation. This is known as 'Right of Access' request (formerly called a Subject Access Request).

We kindly request that you please complete this form and send it back to:

Email: Governance.Team@wiganboroughccg.nhs.uk please ensure you add "Right of Access Request" in the subject field of the email.

Address: Governance Team, Wigan Life Centre, College Avenue, Wigan WN1 1NJ

1. Applicant's Full Name

   ……

2. Applicant's Date of Birth

   ……

3. Applicant's Current Address

   ……

   ……

   ……

4. Applicant's Previous Address (if applicable)

   ……

   ……

   ……

5. Applicant's Telephone Number:

   Home Telephone No: ……

   Mobile Telephone No ……

6. The information requested is about me?

Yes ☐ No ☐

If **Yes**, please go to Question 8

7. The Applicant (whose data is being requested) must give permission for the information to be released to their representative.

I give my permission for…….. to request access to my personal information as described in question 8 (below) of this form.

Signature of Data Subject……

Print Name: ……

Name of representative and address where information is to be sent:

……

……

……

……

8. To help us search for the information you require please tell us the about the information you require with as much detail as possible. For example, copies of personnel file between (date) and (date). This will help us to complete your request in a timely manner. If we do not receive enough information to process you request, we may be unable to proceed with your request.

……

……

……

……

……

……..

9. I confirm that I am the Data Subject

Signed: ……

Print Name: ……..

Date: ……..

I enclose a photocopy of 2 of the following items as proof of identity (one to be a photographic copy).

Please tick on the attached form which 2 forms of identity have been enclosed.

10. I confirm that I am the representative

Signed: ……..

Print Name: ……

Date: ……..

Appendix 2 – ID Checklist

Acceptable ID documents for the 'right of access' requests

To make a Right of Access Request for yourself, you will be asked to provide two forms of ID documentation, one being proof of identity and one to confirm your address, before any information will be released.

All forms of acceptable documentation are listed in the tables below. Please note, One document from each of the tables below should be provided (please send copies not originals):

Please tick against the documents you have provided

PROOF OF IDENTITY	
Acceptable Photo Personal Identity Documents	
	Current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passports
	Passports of non-EU nationals containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK *****
	Current UK (or EU/other nationalities) Photo-card Driving Licence (providing that the person checking is confident that non-UK Photo-card Driving Licences are genuine
	A national ID card and/or other valid documentation relating to immigration status and permission to work*****
Any documents not listed above are not acceptable forms of identification e.g. organisational ID card.	
Acceptable Non-Photo Personal Identity Documents	
	Full UK Birth Certificate – issued within 6 weeks of birth
	Current Full Driving Licence (old version); (Provisional Driving Licences are not acceptable)
	Residence permit issued by Home Office to EU Nationals on inspection of own-country passport
	Adoption Certificate
	Marriage/Civil Partnership certificate
	Divorce or annulment papers
	Police registration document
	Certificate of employment in HM Forces
	Current benefit book or card or original notification letter from the Department of Work and Pension (DWP) confirming legal right to benefit
	Most recent HM Revenue and Customs (previously Inland Revenue) tax notification
	Current firearms certificate
	Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
	GV3 form issued to people who want to travel in the UK without valid travel documents
	Home Office letter IS KOS EX or KOS EX2
	Building industry sub-contractors certificate issued by HM Revenues and

	Customs (previously Inland Revenue)

CONFIRMATION OF ADDRESS	
To confirm the address, the following documents are acceptable:	
	Recent utility bill or certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible*****
	Local authority tax bill (valid for current year)*****
	Current UK photo-card driving licence (if not already presented as a personal ID document)
	Current Full UK driving licence (old version) (if not already presented as a personal ID document)
	Bank, building society or credit union statement or passbook containing current address
	Most recent mortgage statement from a recognised lender*****
	Current local council rent card or tenancy agreement
	Current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit
	Confirmation from an electoral register search that a person of that name lives at the claimed address*****
	Court Order*****

****The date on these documents should be within the last 6 months (unless there is a good reason for it not to be e.g. clear evidence that the person was not living in the UK for 6 months or more) and they must contain the name and address of the applicant***.

Please return securely and marked private and confidential:

Post: Governance Team (Right of Access Request), Wigan Life Centre, College Avenue, Wigan WN1 1NJ

Email: Governance.Team@wiganboroughccg.nhs.uk Please ensure you write Right of Access Request in the subject field of the email.

Appendix 3 – Access Request Disclosure Form

Information Asset Owner Name:	
Department:	
Details of information supplied: **Please include number of copies / date ranges / page numbers and source**	
Format information to be supplied: **Email / hard copy**	
I confirm that the information provided for the 'Right of Access' request is a complete and accurate record of the information requested by the applicant.	
Signed:	
Date:	

Appendix 4 – Access Request Release Form

Before release of any documents this form must be signed by the appropriate person (SIRO or CG or IOA). It should be held by the 'Access Request Lead'

Documents must not be released directly to the applicant and all documentation must come via the secure generic access request email.

1. Applicant's Full Name

   ……

2. Applicant's Date of Birth

   ……

3. Applicant's Current Address

   ……

   ……

   ……

AUTHORISER'S DECLARATION – Please tick relevant box or boxes	
1. I agree to the attached records being released to the above named person or the person's named representative	☐
2. Part or whole of the records have been withheld on the grounds that:	☐
a. Disclosure is likely to cause serious harm to the physical or mental health of the person or of another individual	☐
b. Access would disclose information relating to, or provided by, a third party who has not consented to their information being disclosed	☐
c. The record contains information the person expressly stated must not be released	☐
d. The person is under 16 and I do not think he / she fully understands what an application to see their records means	☐

Staff Name: ……..

Post held: …….

Signature: ……

Date: ……..