

Subject Access Request Policy



Subject Access Request Policy For Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 05 March 2019

Signed:

Signed:

Chair of the committee

Designated Senior Officer



Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	V5.0
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	05 March 2019
Date Policy is Effective From	Date of ratification
Review date:	January 2020
Expiry date:	March 2020
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff and staff working for the CCG
National Documents	
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
Kirstie Macmillan	Information Governance officer (NHSW)
Sally Roberts	Director of Governance Quality & Safety
Sara Saville	Head of Corporate Governance
Serena Causer	Corporate Governance Officer

Circulated to the following for consultation

Name/Committee/Group/	Designation
SQP	

IG Function Leads	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments
SQP	Remove definitions Make the reference to staff records clearer
IG lead	Greater clarity for staff records

Version Control Summary

Significant or Substantive Changes from Previous Version

This Subject Access Request Policy has been ratified by SQP for Walsall CCG. It was adapted from a policy written by Kirstie Macmillan for NHSW

Version	Date	Comments on Changes	Author
V0.2	Feb 2013	Removed majority of definitions Included WCCG employees in the purpose of the policy Included section on HR records	Sara Saville
V1.0	Feb 2013	Ratified version	Sara Saville
V3.1	May 2018	Reflect General Data Protection Regulation	Serena Ellis
V3.2	August 2018	Reflect Data Protection Act 2018, General Data Protection Regulation, Charges, Children and how SAR's can be requested	Serena Ellis
V4.1	Feb 2019	Rectification	Serena Ellis
V4.2	March 2019	Timeframe to respond to a SAR	Serena Ellis

Contents

- 1.0 Introduction 6
- 2.0 Purpose 6
- 3.0 Definitions..... 6
- 4.0 Who can make a request..... 7
- 5.0 How information can be provided..... 7
- 6.0 Types of Records and Exceptions 8
- 7.0 Consent..... 10
- 8.0 Monitoring..... 12
- 9.0 Charges12
- 10. Timeframe to respond12
- [11](#) Rectification.....13

1.0 Introduction

The Data Protection Act 2018 and General Data Protection Regulation came into force 25 May 2018, implementing the European Directive on the data protection and privacy for all individuals with regard to the processing of personal data and on the free movement of such data.

The Data Protection Act 2018 and General Data Protection Regulation enables individuals (referred to as data subjects) the right, certain to exceptions to view and obtain a copy of all personal data about themselves which is held in either computerised or manual formats.

Under Article 15 of the General Data Protection Regulation, data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them is being processed, and where that is the case access to information about themselves irrespective of when that information was created. To exercise this right, the data subject needs to make a written or verbal request for information where they are the subject of that information or data.

2.0 Purpose

The purpose of this policy is to provide guidance for the provision of personal data under Article 15 of the General Data Protection Regulation and Data Protection Act 2018.

This policy applies to all requests for access to personal data held by Walsall CCG and provides a framework for Walsall CCG to ensure compliance with the Legislation.

This applies to:

- Employees of Walsall CCG
- Patients or service users of the health services provided by Walsall CCG
- An organisation or individual from whom Walsall CCG commissions clinical or non clinical services

3.0 Definitions

Data Subject

An individual who is the subject of personal data. A data subject must be a living individual.

Subject Access Request

A Subject Access Request is a written or verbal, request from an individual asking to see information held about them.

4.0 Who can make a request

Subject Access Requests can be made by:

- The individual themselves – the data subject. This will either be a member of the public or a member of staff
- Those who have parental responsibility (if requesting a child's records)
- A representative nominated by the individual to act on their behalf such as Solicitors or a relative, although there must be a valid consent by the individual granting this authority
- In certain situations a person granted a Lawyer or Agent of the Court of Protection on behalf of an adult who is incapable of consent (please read the section Requests by the Police, Court Orders and Other Requests below)
- The Police (please read the section Requests by the Police, Court Orders and Other Requests below)

A Request can be put in writing or verbally to any department of WCCG:
You can seek advice from the Information Governance Manager
Jubilee House Bloxwich Lane Walsall WS2 7JL

Requests by the Police, Court Orders and Other Requests

No disclosure should be made unless authorisation is obtained from the patient / member of staff; or the request is for the purposes of crime or taxation; or is otherwise permitted under the Data Protection Act 2018 and General Data Protection Regulation.

Advice should be sought from the Caldicott Guardian or Data Protection Officer.

Original records must not be provided to the Police or Coroner without the authorisation of the Caldicott Guardian or Data Protection Officer.

5.0 How information can be provided

Information can be provided in the following formats:

- Copies of Records
- Viewing Records
- Audio

In all cases the information will need to be understandable and easy to read. Where abbreviations and medical terminology are used an explanation should be provided. Original information should not be released.

Copies of Records

The individual or their representative will gain access to their information by receiving copies of their records either in paper or computerised format.

Viewing Records

There may be some cases where it is deemed more appropriate for the individual to view their records instead of receiving a copy. In this case, an appropriate member of staff from Walsall CCG should be in attendance when the individual views the records.

Audio

An individual may listen to an audio tape recording if it contains personal information about them. There should be in place arrangements to provide a transcript of the information.

6.0 Types of Records and Exceptions

There are rules for specific types of records and these are listed below:

Human Resource information

Before any information is released it must be checked by the line manager to ensure that it is all relevant to the member of staff requesting the information and redacted if it includes details of other staff members.

Health Records

Before any information is released, the health records must be inspected by the Caldicott Guardian. There are certain exemptions to the release of health information and these are described in more detail below:

Serious Harm

On inspection of the records the Caldicott Guardian or Data Protection Officer can advise that certain personal information is not released on the grounds that its release would be likely to cause serious harm to the physical or mental health of the patient or any other individual.

There is no definite requirement to inform the member of staff, patient or their representative that this information has not been released.

Third Party Exemption

Where a third party is mentioned within the patient's health record, the consent of this third party should be sought before the information is released. Where no consent has been obtained, the information should only be released if:

1. Considered reasonable to release the personal information without the consent of the individual, or
2. The information can be released whilst still protecting the identity of the 3rd party i.e. anonymise their personal information so they cannot be identified

The third party exemption would not normally apply to health professionals included within the health record who are currently or have previously contributed to the care of the patient concerned. Release of the health professionals information, however, can be restricted if disclosure may result in serious harm to the health professional.

Other Agencies Records

Other letters or reports from another agency, person or NHS Trust may be contained in a person's health record. Where this is the case the Caldicott Guardian or Data

Protection Officer should consider whether there is a need to approach those agencies or persons to secure agreement for the release of the information.

Factors to take into consideration are whether the other agency's information is already recorded in Walsall CCG's records and whether the other agency professionals would be in agreement with the release.

If there is any doubt, the agencies concerned should be contacted.

Other Exemptions

The exemptions listed above are the key ones for health records. However, the Data Protection Act 2018 and the General Data Protection Regulation includes a wide range of exemptions that exempts an organisation from releasing information

1. Deceased Patient Records

The right of access provided under the Data Protection Act 2018 only applies to living individuals. Requests for access to a deceased patient's record comes under Access to Health Records Act.

Requests can only be made by:

The patient's personal representative (usually the executor of the will or administrator of the estate) or

A person who may have a claim arising from the patient's death – release of any information will only be the minimum necessary to process their claim.

Only relevant information relating to the claim made should be released.

The Caldicott Guardian will need to inspect the records taking into account the following:

1. If it is known whether the deceased patient did not wish for their records to be disclosed or the records contain information about the deceased patient which was expected to be kept confidential
2. If the release of the information is likely to cause serious harm to the physical or mental health of any individual

Where a third party is mentioned within the patient's health record, the consent of this third party should be sought before the information is released. Where no consent has been obtained, the information should only be released if:

1. Considered reasonable to release the personal information without the consent of the individual, or
2. The information can be released whilst still protecting the identity of the 3rd party i.e. anonymise their personal information so they cannot be identified

The third party exemption would not normally apply to health professionals included within the health record who are currently or have previously contributed to the care of the patient concerned. Release of the health professionals information, however, can be restricted if disclosure may result in serious harm to the health professional

Other Records

Besides health records all other records held by Walsall CCG regarding individuals, patients and staff will also be liable for subject access requests by those individuals or representatives. The general procedure will apply as for health records, expect there will be no requirement for the Caldicott Guardian to review the information. Exemptions will mainly relate to third party references within the record

Individuals Living Abroad

Patients or individuals who used to live in the UK and have records held by Walsall CCG still have the right to make a Subject Access Request. The same procedure should be implemented as for an individual living in the UK.

Before information is released to individuals living abroad, the Caldicott Guardian should review the information to ensure it will not cause the patient harm and there needs to be appropriate mechanisms in place for the safe and secure transfer of the information.

When a patient moves abroad their GP health records are transferred to the relevant Commissioning Organisation and they are then retained for the recommended retention period as defined in the Department of Health's Records Management Code of Practice 2009.

7.0 Consent

In the majority of cases the consent to access personal information will be provided by the individual whose information has been requested. There may however be cases where the individual is unable to consent

Children

Under the General Data Protection Regulation a child has the right of access to the information held about them.

Before responding to a request it is important to consider whether the child is mature enough to understand their rights, if it is clear that they are, then the request should be responded to. In some circumstances we will allow the parent to exercise the child's rights on their behalf if the child authorises this, or it is evident that this is in the best interests of the child.

It is important that a child is able to understand in broad terms what it means to make a subject access request, when considering borderline cases, it is important to take into account the following:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them

Consent for children under the age of 13 will be the responsibility of those who have parental responsibility. This enables those with parental responsibility to request access to their children's records and release of the information is normally done in the best interests of the child.

Those who have parental responsibility are:

1. The mother i.e. to include either the birth mother or adoptive mother
2. The father, if both parents are married. If one parent is granted a Residence Order (previously known as custody) this does not take away parental responsibility from the other parent. The order merely determines who a child is to live with
3. For births after the 1st December 2003 the unmarried father if included on the birth certificate
4. If parents are not married and the birth was before the 1st December 2003 the father will only have parental responsibility by virtue of a court order, or because the mother and father of the child have entered into a formal parental responsibility agreement. This agreement is drawn up through their Solicitor
5. If parents marry after the child's birth the father automatically obtains parental responsibility by virtue of this event
6. The Local Authority if the child is subject to a Care Order – in this event the parents and Local Authority share parental responsibility
7. Adults in receipt of a Special Guardianship Order (Adoption and Children Act 2002)

For this persons aged 16 to 18 who do not have the capacity (as per the Fraser Guidelines) to consent it may be that the responsibility still remains with those who have parental responsibility. This will apply to the right to access records.

When a child is considered to be 'competent' and is therefore able to fully understand the consequences and process of a subject access request they should be able to make a subject access request themselves.

The ruling from the Fraser / Gillick case defined competence as:

'Sufficient understanding and intelligence to enable him or her to understand fully what is proposed'

The decision on whether a child is competent should be made by the Health Professional who has current responsibility for providing clinical care to that child. Failing this, the decision should be made by a Health Professional who has the necessary skills and experience and is most suitable to advise on such matters.

Where it has been agreed that a child is competent and those with parental responsibility make a subject access request to view their child's records, the child should be approached for their consent to the release of the records.

Where a child has given information and specifically requested that it is not released to those with parental responsibility then it shouldn't be released if the parents make a subject access request for that child's records.

Mentally Incapacitated Adults

In law it is the case that another adult cannot consent for another adult. However, where an adult is mentally incapacitated and is unable to consent to a subject access request of their records, a person who has been granted power as an attorney under a Lasting Power of Attorney (LPA) or a deputy appointed by the new Court of Protection, can in certain circumstances make a request on their behalf in relation to the management of their property and welfare.

Decisions however, can be made to release a patient's information (where the patient cannot consent) to relatives or carers by health professionals where it can be justified. This is done in the patient's best interests and only the necessary information to support their care will be released. Decisions should be made on a case by case basis taking into account impact on the patient, relatives and any known views of the patient when they were able to consent, and their health needs.

Any decision regarding disclosure should be documented stating the justification for disclosure, what was disclosed, when and to whom.

8.0 Monitoring

The policy will be monitored through the information governance report received by the Audit and Governance committee.

9.0 Charges

In most cases charges will not apply to comply with a subject access request. Charges will only be applied where the request is excessive or the requester requests further copies of their data following a request.

For further advice please speak to a member of the Corporate Governance Team.

10.0 Timeframe to respond

All requests must be responded to without delay and at the latest within one month of receipt of the request. This time can be extended by a further two months where requests are complex or numerous. However, if this is the case the individual must be informed within one month of the receipt of the request and explain why the extension is necessary.

11.0 Rectification

Article 5(d) of the GDPR requires that personal data shall be "accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that

personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”.

11.1 When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the personal data in question has been disclosed to others, each recipient must be contacted and inform of the rectification - unless this proves impossible or involves disproportionate effort. If asked, the individual must be informed about these recipients.

11.2 Timescale to comply with a request for rectification

A response to a request for rectification must be complied with within one month of receipt of the request. This can be extended by two months where the request for rectification is complex.

If a decision is taken not to take action in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy. Advice should be sought from the Data Protection Officer.

