NHS
Somerset
Integrated Care Board

INDIVIDUAL RIGHTS POLICY

Version:	1.1.1
Ratified by:	Information Governance, Records Management and Caldicott Committee
Date Ratified:	20 October 2021
Name of Originator/Author:	SCW Information Governance
Name of Responsible Committee/Individual:	Information Governance, Records Management and Caldicott Committee
Date issued:	20 October 2021
Review date:	20 October 2024
Target audience:	All Somerset ICB staff, including contractors and temporary staff

INDIVIDUAL RIGHTS POLICY

CONTENTS

INDIVIDUAL RIGHTS POLICY

VERSION CONTROL

Document Status:	Final
Version:	1.1.1

DOCUMENT CHANGE HISTORY		
Version	**Date**	**Comments**
0.1	23/05/2018	Creation of policy and incorporation of Subject Access Request policy and procedures
0.2	25/05/2018	Further review with GDPR considerations
0.3	23/07/2018	Following review by the GDPR working group
1.0	14 /02/19	Approved at IGRMCC
1.1	20/10/2021	Approved at IGRMCC
1.1.1	June 2022	Organisation change from CCG to ICB . Wording changes from CCG to ICB made.

Equality Impact Assessment (EIA) Form OR EIA Screening Form completed. Date:	

Sponsoring Director:	James Rimmer – Chief Executive
Author(s):	SCW Information Governance
Document Reference:	Individual Rights Policy v 1.1.1

INDIVIDUAL RIGHTS POLICY

1 INTRODUCTION

1.1 Somerset ICB is under a legal duty to comply with 'individual's rights' requests under the Data Protection Legislation, in relation to personal information that it holds. It is a legal requirement that all requests for personal information held by the ICB are handled in accordance with data protection legislation.

1.2 This policy and accompanying standard operating procedure (SOP) sets out the approach that the ICB will take in responding to these requests along with useful guidance and steps to follow when requests are received anywhere within the ICB.

2 SCOPE AND DEFINITIONS

Scope

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

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

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

Definitions

2.42.4

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the ICB or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the UK GDPR.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal

	information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the UK GDPR.
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Data Protection Legislation	Data Protection Legislation includes all UK legislation which applies to any personal data being processed. This includes, but is not limited to: UK GDPR The Data Protection Act 2018 Any other applicable national laws.

Abbreviation	Meaning
ICB	Clinical Commissioning Group
CSU	Commissioning Support Unit
DC	Data Custodian
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018

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

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

Acknowledging Individual Rights

3.1 The UK General Data Protection Regulation (UK GDPR) provides rights for individuals which fall into 2 distinct categories. Firstly, where an individual wants to know what data, the ICB is processing about them (or why) or they want access to that data (or to receive a copy).

3.1.1 Secondly where an individual wants the ICB to make changes to what or how the ICB is processing their personal data, or for the ICB to pass on their personal data to another party. In these requests, the individual is not requesting access to, or a copy of the data itself.

3.1.2 An individual or their representative can exercise several data subject rights to the ICB. These do not confer automatic agreement to the request but will be duly considered by the ICB – the Appendix and SOP contains more in-depth detail regarding each of the rights.

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

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

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

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

Recognising an Individual's Rights Request

3.2

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

3.2.1 The format in which an Individual's Rights request is received may differ from request to request. In general, if an individual writes to the ICB or speaks to the ICB and asks for access, changes or objects to any personal data the ICB is processing about them (whether perceived or actually being processed) the request should be considered and handled as an Individual's Rights request.

3.2.2 ICB Staff can submit a request for access to their personal data to the Information Governance team; verbally or in writing. A staff subject access request application form is available by emailing somICB.dataprotection@nhs.net

3.2.3 Completed forms or requests for access to staff records should be submitted to somICB.dataprotection@nhs.net

3.2.4 Members of the public who would like to exercise their individual rights under the UK GDPR can submit their requests to somICB.dataprotection@nhs.net.

Refusing a Request

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

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

In either case the ICB will need to justify the decision.

Charging a Fee

3.4

- Individuals rights request are free of charge however the ICB may in some circumstances be able to charge a fee such as for repetitive requests
- The fee must be reasonable and based on the administrative costs of complying with the request
- Where a fee is to be charged, the ICB will contact the individual promptly and inform them
- The ICB does not need to comply with the request until the fee has been received

Information for Requestors

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

3.5.1 If the ICB are not taking action:

- The reasons the ICB is not taking action;
- Their right to make a complaint to the ICO;
- Their ability to seek to enforce a right through a judicial remedy

OR

3.5.2 If the ICB is requesting further information:

- Whether the ICB is requesting a reasonable fee
- Whether the ICB needs additional information to identify the individual
- Whether the ICB needs to extend the response time

OR

3.5.3 If the ICB is actioning the request:

- Respond to the request

Calculating Response Time

3.6 Under the Data Protection Legislation the ICB has one Calendar month to respond to any request.

3.6.1 The ICB will calculate the time limit from the day after a request is received (whether the day after is a working day or not) until the corresponding date one month from that point.

Extending the Response Time

3.7 The response time can be extended by a further two months if the request is complex or there are a number of requests from the individual. The ICB will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

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

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

Verifying Identity

3.8 If there are doubts about the identity of the person making the request the ICB can ask for more information. However, it is important that the ICB only request information that is necessary to confirm who they are. The ICB will take into account what data is held, the nature of the data, and what it is being used for.

3.8.1 The ICB will let the individual know without undue delay that additional information is required from them to confirm their identity. The ICB do not need to comply with the request until the additional information is received.

4 Roles and Responsibilities

ICB Governing Body

4.1 It is the role of the ICB Governing Body to define ICB policy in respect of Information Governance, taking into account legislative and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy. These activities are delegated to the Clinical Executive Committee.

Information Governance, Records Management and Caldicott Committee (IGRMCC)

4.2 The IGRMCC is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the ICB and raising awareness of Information Governance.

Information Asset Owners

4.3 Information Asset Owners (IAO's) are responsible for ensuring that Individual Rights requests are processed and responded to in line with Data Protection Legislation.

Information Governance Lead

4.4 The Information Governance and Data Protection Manager will co-ordinate and oversee all Individual Rights requests, ensuring that they are responded to in line with Data Protection Legislation.

ICB Data Protection Officer and the SCW IG team

4.5 The ICB Data Protection Officer will provide advice and guidance in complex or disputed situations or decisions where required.

Information Asset Owners and Administrators

4.6 IAAs/IAOs are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and to provide the Information Governance and Data Protection Manager with any support necessary to fulfil the requests.

ICB Staff

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

5 TRAINING

5.1 All staff are required to complete training using the NHS Data Security Awareness Level, accessible through ConsultOD, or approved face to face training (if offered). Bespoke training on Individual's Rights will be provided to relevant teams where the need is identified.

6 PUBLIC SECTOR EQUALITY DUTY – EQUALITY IMPACT ASSESSMENT

6.1 An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix 2.

7 MONITORING COMPLIANCE AND EFFECTIVENESS

7.1 The application of this policy and the accompanying standard operating procedures will be monitored by the ICB through quarterly updates to the IGRMCC.

8 REVIEW

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

9 REFERENCES AND ASSOCIATED DOCUMENTS

Legislation

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

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

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

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

Guidance

9.29.2

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

THE INDIVIDUAL RIGHTS IN MORE DETAIL

THE RIGHT TO BE INFORMED (UK GDPR ARTICLES 12, 13 AND 14)

The ICB must provide individuals with information including (but not limited to):

- Our purposes for processing personal data,
- Our retention periods for that personal data, and
- who it will be shared with

This is called 'privacy information' or 'Fair Processing Information' and we must provide privacy information to individuals at the time we collect personal data from them. If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

How and what information should be provided

The information we provide to people must be

- concise,
- transparent,
- intelligible,
- easily accessible, and
- it must use clear and plain language

We put our Fair Processing Notice on our website.

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

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

What is the right of access?

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

What is an individual entitled to?

Individuals have the right to obtain the following from the ICB:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information such as
    - the purposes of processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient we disclose personal data to;
    - retention period for storing personal data or, where this is not possible, our criteria for determining how long we will store it;

* the existence of their right to request rectification, erasure or restriction or to object to such processing;
* the right to lodge a complaint with the ICO or another supervisory authority;
* information about the source of the data, where it was not obtained directly from the individual;
* the existence of automated decision-making (including profiling); and
* the safeguards we provide if we transfer personal data to a third country or international organisation

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

What about requests made on behalf of others?

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

What about the records of deceased individuals?

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

THE RIGHT TO RECTIFICATION (UK GDPR ARTICLE 16 AND 19)

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

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

What do we need to do?

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

THE RIGHT TO ERASURE (UK GDPR ARTICLE 17 AND 19)

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

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

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

RIGHT TO RESTRICT PROCESSING (UK GDPR ARTICLE 18 AND 19)

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

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

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

THE RIGHT TO DATA PORTABILITY (UK GDPR ARTICLE 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

THE RIGHT TO OBJECT (UK GDPR ARTICLE 21)

An individual has the right to object to

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

RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING AND PROFILING (UK GDPR ARTICLE 22)

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

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

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

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

EQUALITY IMPACT ASSESSMENT

1 What is it about? ***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Individuals Rights Policy details how the ICB will meet its legal obligations and NHS requirements concerning the exercising of Individual Rights over the processing of their personal information and the arrangements in place to support this.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the exercising of Individual Rights to be of equal status across all groups of people.
d) What are the barriers to meeting this potential? Barriers may arise where Individuals may experience difficulties in exercising their rights i.e. those who may lack the mental capacity to do so, are deemed particularly vulnerable at a given point in time, where those Individuals are children or where there are language barriers or there is a need to convey the information in a particular way for ease of accessibility reasons.
2 Who is using it? ***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy in response to legislative requirements.
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.
3 Impact ***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created with regard to the policy itself, only in respect of communicating how individuals can exercise their rights.
b) What can be done to change this impact? If it cannot be changed, how can this impact be mitigated or justified? The ICB will pay particular attention to the NHS Accessibility Standards and offer all

appropriate help and assistance to enable those experiencing difficulties to exercise their Rights.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? Given consideration to providing the guidance to individuals in different formats to aid accessibility.
b) What will you do now and what will be included in future planning? Implement different methods of communication and ways of applying for individuals to exercise their rights.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.