

INDIVIDUAL RIGHTS POLICY

This policy has been created by SCW but approved and adopted for use by NHS Devon and applies to all staff working for and within NHS Devon.

Policy number	
Version	1.0
Approved by	Audit and Risk Committee
Document author	SCW CSU Information Governance Services
Executive lead	SIRO
Date of approval	08/02/2023
Next due for review	08/02/2024



Version control sheet

Version	Date	Author	Comment
V1.0	11/1/2023	SCW IG Services	Introduction of new policy to the ICB



Equality Statement

Equality, diversity and human rights are central to the work of the NHS Devon Integrated Care Board (ICB). This means ensuring local people have access to timely and high quality care that is provided in an environment which is free from unlawful discrimination. It also means that NHS Devon will tackle health inequalities and ensure there are no barriers to health and wellbeing.

To deliver this work NHS Devon staff are encouraged to understand equality, diversity and human rights issues so they feel able to challenge prejudice and ensure equality is incorporated into their own work areas. NHS Devon staff also have a right to work in an environment which is free from unlawful discrimination and a range of policies are in place to protect them from discrimination.

NHS Devon's equality, diversity and human rights work is underpinned by the following:

- NHS Constitution 2015.
- Equality Act 2010 and the requirements of the Public Sector Equality Duty of the Equality Act 2010.
- Human Rights Act 1998.
- Health and Social Care Act 2012 duties placed on NHS Devon to reduce health inequalities, promote patient involvement and involve and consult the public.



Contents

Equality Statement	3
1. Introduction	5
2. Scope and definitions.....	5
3. Details of the policy and compliance with the Data Protection Legislation	7
4. Roles and responsibilities	10
5. Equality Analysis.....	11
6. Training.....	11
7. Dissemination/publication	11
8. Monitoring compliance and effectiveness	11
9. Review.....	11
10. Stakeholder /consultation information	Error! Bookmark not defined.
11. References and associated documents	11
Appendix A: The Individual Rights in more detail	13
Appendix B: Equality Impact Assessment	17
Appendix C: Process Flow Chart	Error! Bookmark not defined.



1. Introduction

NHS Devon 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 NHS Devon are handled in accordance with data protection legislation.

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

2. Scope and definitions

Scope

It is the responsibility of **all** NHS Devon 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 NHS Devon.

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

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

Definitions

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to NHS Devon 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 or gender identity.
Data Protection Legislation	Data Protection Legislation includes all UK legislation which applies to any personal data being process. This includes, but is not limited to: • UK GDPR • The Data Protection Act 2018 • Any other applicable national Laws.

Abbreviation	Meaning
CSU	Commissioning Support Unit
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPO	Data Protection Officer
FPN	Fair Processing Notification (privacy notice)
UK GDPR	UK General Data Protection Regulations
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICB	Integrated Care Board
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

3.1 Acknowledging Individual Rights

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 (or why) data NHS Devon is processing about them and/or have access /a copy of that data.

Secondly where an individual wants NHS Devon to make changes to what or how it is processing their personal data, or for NHS Devon 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:

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

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

- obtain from NHS Devon confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, request access to the personal data (a **Subject Access Request/Right of Access**)
- obtain from NHS Devon without undue delay the rectification of inaccurate or incomplete personal data processed by NHS Devon concerning them (**Right to Rectification**)
- obtain from NHS Devon the erasure of personal data concerning them in certain circumstances (**Right to Erasure**)
- obtain from NHS Devon restriction of processing of personal data concerning them in certain circumstances (**Right to Restriction**)
- receive the personal data concerning them, which they have provided to NHS Devon, 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**)
- object to processing of an individual's personal data in certain circumstances (**Right to Object**)
- not be subject to a decision based solely on automated processing by NHS Devon (**Rights related to automated decision-making including profiling**)

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

3.2 Recognising an Individual Rights Request

- 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

The format that an Individual Rights request is received may differ from request to request. In essence, if an individual writes to NHS Devon or speaks to NHS Devon and asks for access, changes or objections of any kind to the personal data it is processing about them (whether perceived or actually processing their data) it should be considered and handled where appropriate as an Individual Rights request.

NHS Devon Staff can also submit a request for access to their personal data to the Data Protection team, verbally or in writing.

Members of the public who would like to exercise their individual rights under the UK GDPR can submit their requests to NHS Devon via the following mailbox:

d-icb.dataprotection@nhs.net

Requests can also be submitted to any part of the organisation or individual members of staff and do not have to be to a specific person or contact point, but staff must then forward as soon as possible to the above mailbox.

3.3 Refusing a Request

If NHS Devon 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 we will need to justify the decision.

3.4 Charging a Fee

- Individual rights requests are free of charge however NHS Devon may in some circumstances be able to charge a fee such as for repetitive requests
- We should base the reasonable fee on the administrative costs of complying with the request



- If we decide to charge a fee we should contact the individual promptly and inform them
- We do not need to comply with the request until we have received the fee.

3.5 Information for Requestors

NHS Devon must inform the individual without undue delay and within one month of receipt of the request:

If NHS Devon are not taking action:

- the reasons we are 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

If we are requesting further information:

- if we are requesting a reasonable fee or
- need additional information to identify the individual
- we need to extend the response time

OR

We are actioning the request:

- Respond to the request

3.6 Calculating Response Time

Under the Data Protection Legislation, NHS Devon has **one** Calendar month to respond to any request. For practical operational purposes, NHS Devon has taken the decision to adopt a 28-day response time in line with ICO advice. In order to provide clarity to staff the timeframe starts on the day the request is received (whether the day after is a working day or not) until the 28th day from receipt. However, if the 28th day is at the weekend or on a bank holiday the next working day will be used as the latest date to provide a response as per national guidance.

For further details on national guidance please visit [ICO Individual Rights Guidance](#).

3.7 Extending the Response Time

We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICOs 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

3.8 Verifying Identity

If NHS Devon has doubts about the identity of the person making the request we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. We will take into account what data we hold, the nature of the data, and what we are using it for.

We will let the individual know without undue delay that we need more information from them to confirm their identity. We do not need to comply with the request until we have received the additional information.

4. Roles and responsibilities

Senior Executive Team

It is the role of the Senior Executive Team to define NHS Devon policy in respect of Information Governance, taking into account legislative and NHS requirements. The Executive Management Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Audit and Risk Committee

The Audit and Risk Committee is responsible for oversight of the Information Governance agenda, ensuring that NHS Devon complies with their statutory responsibilities and fulfils the requirements of administrative law, Data Protection Act 2018, UK General Data Protection Regulation, the Common Law Duty of Confidentiality and the Records Management Code of Practice 2021: A guide to the management of health and care records.

Data Protection Steering Group

The Data Protection Steering Group (DPSG) is responsible for overseeing day to day Information Governance issues; implementing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in NHS Devon and raising awareness of Information Governance.

Data Protection Team and Data Protection Officer

The Data Protection team and Data Protection Officer (DPO) are responsible for processing all Individual Rights requests in accordance with Data Protection Legislation.

Information Asset Owners

Information Asset Owners (IAOs) are responsible for ensuring that Individual Rights requests are processed by their team when a request is received for records from the Data Protection Team.



Information Asset Administrators

Information Asset Administrators (IAA) are responsible assisting the IAO to ensure that Individual Rights requests are processed by their team when a request for records is received by the Data Protection Team.

NHS Devon Staff

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. Equality Analysis

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 B.

6. Training

All staff are required to complete annual Data Security and Awareness training via ESR.

7. Dissemination/publication

This policy will be made available to staff via the NHS Devon intranet and will also be published on the NHS Devon website.

8. Monitoring compliance and effectiveness

The application of this policy and the accompanying standard operating procedures will be monitored by NHS Devon through updates to DPSG and quarterly reports to the Audit and Risk Committee.

9. Review

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 annually.

11. References and associated documents

Legislation

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



- the UK General Data Protection Regulation (GDPR),
- the Data Protection Act (DPA) 2018,
- any applicable national Laws implementing them as amended from time to time

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

Consideration must also be given to the

- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990

Guidance

- NHS Devon 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](#)
- [NHS England Confidentiality Policy](#)
- [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](#)



APPENDIX A: The Individual Rights in more detail

The Right to be Informed (UK GDPR Articles 12, 13 and 14)

NHS Devon 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 NHS Devon:

- 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?

The 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 within 40 calendar days instead of one calendar month. The request must still be logged and actioned without undue delay.

The Right to Rectification (UK GDPR Article 16 and 19)

The 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)

The 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.



APPENDIX B: Equality Impact Assessment

Equality Impact Analysis (SCWCSU template) on the

Individual Rights Policy

1 What is it about?	<i>Refer to the Equality Act 2010</i>
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Individuals Rights Policy details how NHD Devon 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?	<i>Consider all equality groups</i>
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	<i>Consider how it affects different dimensions of equality and equality groups</i>
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 can't be changed, how can this impact be mitigated or justified?

NHS Devon 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.

Sign-off (to be completed on approval of the policy)

Name of person leading this EIA:

Date completed:

Proposed EIA review date:

Name of director/decision-maker