

**Individual Rights Procedure**

Approved by: Nicola Short

Version: 1.1

Last Updated: 26/02/2025

Review date: 26/02/2026

**Contents**

1.[Document history 3](#_Toc134526257)

[1.1 Revision history 3](#_Toc134526258)

[1.2 Reviewers 3](#_Toc134526259)

[1.3 Authorisation 3](#_Toc134526260)

2. [Introduction 4](#_Toc134526261)

3. [Purpose 4](#_Toc134526262)

4. [Scope 4](#_Toc134526263)

[5 Roles and Responsibilities 4](#_Toc134526264)

[5.1 Senior Responsible Person 4](#_Toc134526265)

[5.2 Information Governance Lead 5](#_Toc134526266)

[5.3 Data Protection Officer 5](#_Toc134526267)

[5.4 Caldicott Guardian 5](#_Toc134526268)

[5.5 All Staff 5](#_Toc134526269)

[6 Procedure 6](#_Toc134526270)

[6.1 The Right to be Informed (Articles 13 and 14) 6](#_Toc134526271)

[6.2 Recognising a request and duty to respond 6](#_Toc134526272)

[6.3 Receiving and acknowledging a request 6](#_Toc134526273)

[6.4 Logging and retention of requests 7](#_Toc134526274)

[6.5 Processing requests 7](#_Toc134526275)

[*6.5.1 The Right of Access/Subject Access Requests (Article 15)* 8](#_Toc134526276)

[*6.5.2 The Right to Rectification (Article 16)* 9](#_Toc134526277)

[*6.5.3 The Right to Erasure (Article 17)* 10](#_Toc134526278)

[*6.5.4 The Right to Restrict Processing (Article 18)* 11](#_Toc134526279)

[*6.5.5 The Right to Data Portability (Article 20)* 13](#_Toc134526280)

[*6.5.6 The Right to Object (Article 21)* 13](#_Toc134526281)

[*6.5.7 Rights related to automated decision making and profiling (Article 22)* 15](#_Toc134526282)

[6.6 Additional Considerations - Requests received from Third Parties 15](#_Toc134526283)

[*6.6.1 Solicitor Requests* 16](#_Toc134526284)

[*6.6.2 Requests for access to Deceased Records* 16](#_Toc134526285)

[*6.6.3 Requests relating to individuals who lack mental capacity* 17](#_Toc134526286)

[*6.6.4 Requests for Children’s personal information* 18](#_Toc134526287)

*6.7 Refusing a request and complaints……………………………………………………………………………………..……*19

7 [Review 19](#_Toc134526288)

[Annex 1: Limited Rights 20](#_Toc134526289)

[Right to Erasure: 20](#_Toc134526290)

[Right to Restrict Processing: 20](#_Toc134526291)

[Right to Data Portability: 21](#_Toc134526292)

[Right to Object: 21](#_Toc134526293)

[Annex 2: Exemptions 21](#_Toc134526294)

# 1 Document history

## Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Revision Summary** |
| 30/01/2024 | 1.0 | Nicola Short | This procedure has been based upon Version V1 of the DPO Support Service Template |
| 26/02/2025 | 1.1 | Nicola Short |  |
|  |  |  |  |
|  |  |  |  |

## Reviewers

This document requires the following reviews:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Name** | **Position** |
|  |  |  |  |
|  |  |  |  |

## Authorisation

Signing of this document indicates acceptance of its contents.

|  |  |
| --- | --- |
| **Approver’s Name:** | Nicola Short |
| **Role:** | Practice Manager |
| **Signature:** | Nicola ShortPractice Manager26/02/2025 |

# 2 Introduction

The UK General Data Protection Regulation (UK GDPR) came into force on 25th May 2018 along with the updated Data Protection Act 2018. The UK GDPR applies to all ‘Data Controllers’ and ‘Data Processors’ who process personal data. It provides several ‘individual rights’ which provide individuals with more control over their personal data.

# 3 Purpose

The purpose of this procedure is to provide detailed guidance on how the practice meets individuals’ rights and to set out the process for responding to individual rights requests under the UK General Data Protection Regulation (UK GDPR) 2016 and Data Protection Act (DPA) 2018 (commonly referred to as the Data Protection Legislation).

Requests made under the above-named legislations only relate to living individuals. This procedure will also cover requests received under the Access to Health Records Act (AHRA) 1990 which specifically relates to deceased individuals.

This procedure has been adopted by Cathays Surgery to support the work associated in dealing with and managing individuals’ requests.

# 4 Scope

This procedure applies to all staff employed by Cathays Surgery.

The term ‘staff’ includes all health professionals, partners, staff members, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of Cathays Surgery.

This procedure is supplementary to the practice’s Information Governance Policy and sets out the arrangements in place to manage individuals’ rights as set out in the policy. It must be read in conjunction with the policy.

The procedure will cover the following rights stipulated in data protection legislation:

• The right to be informed (Articles 13 and 14)

• The right of access (Article 15)

• The right to rectification (Article 16)

• The right to erasure (Article 17)

• The right to restrict processing (Article 18)

• The right to data portability (Article 20)

• The right to object (Article 21)

• Rights in relation to automated decision making and profiling (Article 22)

This procedure will also cover the rights of access to personal data for deceased individuals under the AHRA.

This procedure provides detailed guidance on when each of the rights apply and provides procedural guidance on how to process each type of request.

## **5 Roles and Responsibilities**

## 5.1 Senior Responsible Person

The Senior Responsible Person within the Practice is responsible for ensuring the highest level of organisational commitment to this procedure and the availability of resources to support its implementation. Where appropriate, the Senior Responsible Person may delegate specific tasks to other individuals who have responsibility for ensuring all individual rights requests are dealt with in line with this procedure.

## 5.2 Information Governance Lead

The Information Governance (IG) Lead will receive specialist training in relation to individuals’ rights and isresponsible for overseeing the day-to-day duties relating to individuals’ rights. Where appropriate, the IG Lead may delegate specific tasks to other individuals who have received appropriate training. The IG Lead is also responsible for ensuring all staff are familiar with the procedure by having suitable access to this document and monitoring compliance against this procedure.

## 5.3 Data Protection Officer

The Data Protection Officer (DPO) will provide independent risk-based advice to support the Practice in its decision making.

The DPO can provide advice on:

* Individual rights requests and under what context these apply
* Provision of privacy information
* Processing requests, timeframes, extensions, refusal and exemptions
* Complex responses
* Legitimate interests
* Erasure of data

The Data Protection Officer for Cathays Surgery is the Digital Health and Care Wales (DHCW) Data Protection Officer Support Service.

The DPO can be contacted by emailing DHCWGMPDPO@wales.nhs.uk.

## 5.4 Caldicott Guardian

The Caldicott Guardian has responsibility for assisting the IG Lead, or other nominated individual, in processing complex requests, particularly where there is an ethical or clinical consideration. This includes:

* Where redactions for serious harm are considered
* Where the accuracy of clinical information is called into question
* Requests relating to deceased individuals where appropriate authority is not in place
* Requests relating to individuals who lack mental capacity
* Requests relating to children where it is necessary to assess Gillick Competence
* Requests relating to children where the best interests of the child need to be assessed
* Where informing third parties of rectification, restriction or erasure of information would prove impossible or involve disproportionate effort

## 5.5 All Staff

All staff have a responsibility to familiarise themselves with the Practice’s Individual Rights procedure and ensure they comply with its obligations.

All staff are responsible for ensuring they are aware of the Practice’s privacy information in line with Section 6.1 of this procedure.

All staff are responsible for ensuring they can recognise individual rights requests and are able to act promptly should they receive such a request, in line with Sections 6.2 and 6.3 of this procedure.

## **6 Procedure**

## 6.1 The Right to be Informed (Articles 13 and 14)

Individuals have the right to be informed about the collection and use of their personal data under Articles 13 and 14 of the UK GDPR. This is a key transparency requirement under the UK GDPR and must be provided to individuals at the time personal data is collected from them. Cathays Surgery are obliged to provide individuals with the following information

* the purposes of processing an individual’s personal data
* the lawful basis for processing
* the retention periods for that personal data
* the details of any third parties that the information is shared with
* the categories of data being processed
* the details of the Data Protection Support Officer/Service
* the name and contact details of the practice’s representative
* the rights available to individuals in respect of the processing
* the right to lodge a complaint with the supervisory authority (ICO)
* the source of the personal data
* the right to withdraw consent where consent is used as the legal basis
* the details of whether individuals are under a statutory or contractual obligation to provide the personal data
* the details of the existence of automated decision-making, including profiling

The practice meets individuals’ right to be informed by the provision of privacy information. The practice utilises a layered approach and provides privacy information in a variety of formats, including:

All Wales Your Privacy, Your Rights posters and leaflets

Detailed privacy information via the practice website

Regular reviews are undertaken to check the privacy notice remains accurate and up to date. If personal data is used for any new purpose(s) or the way data is being processed is changed, the privacy notice will be updated as soon as possible. Any new use of personal data will be communicated and brought to the attention of all individuals involved before any processing has commenced.

## 6.2 Recognising a request and duty to respond

The UK GDPR does not specify how to make a valid request. Therefore, an individual (or a third party acting on the individual’s behalf) can make a request verbally or in writing and they do not have to use specific terminology. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point. Therefore, if a request is received by any staff member, this must be logged and actioned as soon as possible.

The practice has one calendar month to respond to a request. The timescale for responding may be extended by a further two months if the request is complex or if several requests from an individual have been made. However, the individual must be informed within one month of receiving the request of why the extension is necessary.

## 6.3 Receiving and acknowledging a request

**NOTE:** The process detailed below applies when an individual is requesting access to their own information. [Section 6.5 Additional Considerations](#_6.5_Additional_Considerations) should be read in conjunction with the below processes when responding to requests from third parties.

Requests may be received by any member of staff. If received in writing, these must be forwarded to the Senior administrator immediately, as the timeframe to respond is calculated from the date the request was received into the practice. If the request is made verbally, the staff member receiving the request should transcribe, gather as much information as possible, and forward to the Senior administrator immediately.

On receipt of the request the Senior administrator must log the request on the practice’s request register and confirm the identity of the individual making the request.

If identification to verify the individual’s identity has not already been provided with the request, the Senior administrator, must request this prior to processing the request. The timeframe for providing a response pauses and resumes once the requester’s identity has been confirmed.

Examples of forms of ID which is acceptable include, but are not limited to:

• UK passport / other country passport

• Driving Licence

• National ID card

• Adoption certificate

Cathays Surgery may utilise a standard individual rights request form for individuals to complete when submitting a SAR. Using a form can provide more structure to a request, prompt individuals to provide necessary details and supporting documents and provide the necessary contact details. However, the individual should be informed that they are not obliged to complete the form, but it will help the practice process their request and locate the required information more efficiently.

If more information is required to clarify the request this must be requested without undue delay, ideally at the time of requesting proof of identity. The period for responding to the request pauses until the additional information and identification is received. However, if an individual refuses to provide any additional information, the practice must still endeavour to comply with the request i.e., by making reasonable searches for the information covered by the request.

On receipt, the Senior administrator will acknowledge the request and provide the date in which the requester can expect to receive a response by (one calendar month). Where the practice intends to apply an extension (of up to two calendar months) or a fee where the threshold is met, the Senior administrator will inform the requester within the first calendar month.

## 6.4 Logging and retention of requests

On receipt of a request, the Senior administrator will log the request on the Practice’s SAR/Individual Rights log, allocating the request a reference number.

The Senior administrator will then create a folder named in line with the reference number within the Individual Rights folder for the applicable year on Global drive.

All documentation relating to the request and response, including communication with the requester will be stored within the allocated folder.

The folder will be retained in line with the Practice’s retention schedule.

## 6.5 Processing requests

Following receipt of a request and subsequent acknowledgement, each request will be processed in line with the applicable individual right:

## 6.5.1 The Right of Access/Subject Access Requests (Article 15)

The right of access, commonly referred to as subject access request (SAR), gives individuals the right to obtain a copy of and/or to view their personal data and other supplementary information that is held by the practice. This provides individuals with an understanding of how and why Cathays Surgery uses their data and provides reassurances that processing is done lawfully. The supplementary information includes:

* the purposes of the processing;
* the categories of personal data concerned;
* the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
* where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
* the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
* the right to lodge a complaint with the Information Commissioner;
* where the personal data are not collected from the data subject, any available information as to their source;
* the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

**Step 1: Conducting Searches**

Utilising the information provided by the individual the senior administrator will refer to the Practice’s Information Asset Register to identify systems/databases which may contain information within the remit of the request to be searched. For example, a request for medical records may require the following searches:

* [Patient Medical Record (PMR) Storage and Scan on Demand Service]
* [Lloyd George Notes]
* [Practice clinical system]
* [Docman]

**Step 2: Compiling the Response**

Following completion of the searches, the senior administrator will collate all located information within the remit of the request. The senior administrator will review all collated information to ensure all data is that of the correct individual.

Information should be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

**Step 3: Redaction**

The GP will review the collated response and apply the necessary redactions to the response, referring to the Guide to Redaction.

All identifiable third-party data will be redacted unless consent has been received from that individual to release the information.

Any information deemed 'likely to cause serious harm to the physical or mental health of the data subject or another individual' will also be redacted. To establish this the IG lead, will consult with the clinician responsible for the patient’s care or the Practice’s Caldicott Guardian to conduct the ‘Serious Harm Test’. The outcome of this assessment will be recorded.

Where information has been redacted or withheld, the reasons for this should be provided in the response to the data subject, for example:

 “Third-party information has been redacted”.

**Step 4: Review and Sign Off**

Following redaction, the response will be reviewed by the Caldicott Guardian for sign off.

Particular care will be taken to ensure:

* All data is that of the correct individual
* All appropriate redactions have been made

Following approval, a final response will be saved in the patient record, where it will be retained in line with the Practice’s retention schedule.

Details of the sign off and location of the final response will be recorded on the Practice’s individual rights log.

**Step 5: Disclosure**

Responses to requests made electronically will be provided in a commonly used electronic format unless requested otherwise. All disclosures provided electronically will be done so with additional security measures such as the Secure File Sharing Portal. If providing in paper form, the practice will use secure methods such as recorded delivery or offering the individual the opportunity to collect the response by attending the practice in person with ID.

The IG lead will record the date of disclosure on the Practice’s individual rights log.

## 6.5.2 The Right to Rectification (Article 16)

Individuals have the right to have inaccurate or incomplete personal data rectified under Article 16 of the UK GDPR. When a request for rectification is received, all checks will be made to ensure the data is accurate and rectify the data if necessary; considering all arguments and evidence provided by the individual.

**Step 1: Locate the disputed data**

Using the information provided by the individual, the practice will locate the disputed data. If the practice is unable to locate the disputed data, the IG lead will contact the individual and request further details to assist in locating the data. Individuals have the right, under Article 18, to request restriction of the processing of their personal data. As a matter of good practice, processing of the data in question will be restricted whilst the accuracy of the data is verified.

**Step 2: Confirm the accuracy of the data**

All reasonable steps will be taken to confirm that the personal data is accurate, this may include reviewing the data alongside other data held for the individual and consulting with the recording clinician. The practice may also consider any steps already taken to verify the accuracy of the data prior to the request.

Where opinions are recorded, these are subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. Therefore, providing the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, the Practice will not consider the data to be inaccurate.

Where the data refers to a mistake that has subsequently been resolved and an update has been added to show the accurate information, the Practice will not consider the data to be inaccurate, so long as the record correctly reflects the actual sequence of events as this may reflect or have impacted upon the treatment the patient received. For example, if a diagnosis for a condition is recorded on a patient’s record which later is proven not to be the case, it is likely that their medical records will record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is considered as an accurate record of the patient's medical treatment at that point in time.

**Step 3: Establish if rectification is appropriate**

Where the disputed information is found to be accurate, the Practice will not rectify the data.

Where the information is found to be inaccurate, the IG lead will consult with the clinician responsible for the patient’s care or the Practice’s Caldicott Guardian to establish the most appropriate way of rectifying the record.

Inaccurate information will not be removed from the individual’s record unless the clinician is confident that the inaccurate information has had no impact on the patient’s care and has not influenced any clinical decision making. For example, the inaccurate entry was made on the patients record two days prior and the patient has not received any care from a health professional in that time.

Where inaccurate information has been present on an individual’s record for a prolonged period of time, has impacted the individual’s care or influenced clinical decision making, the inaccurate information is to remain on the record with an addendum added to the entry that the data has since been found to be inaccurate and the correct noted.

**Step 4: Update the record**

Where it is agreed that information is inaccurate and this has been verified by a clinician, amendments can then be made to an individual’s record.

The clinician will rectify the record in line with the agreed appropriate method identified in Step 3.

For accurate information, a note may be added noting that the individual disputes the entry.

The IG lead will record details of the rectification on the Practice’s individual rights log.

**Step 5: Inform 3rd Parties**

Where inaccurate data has been previously shared or is subject to ongoing sharing to other organisations, the IG lead will contact each recipient to inform them of the rectification of inaccurate data unless this proves impossible or involves disproportionate effort.

If the IG lead suspects this would prove impossible or involve disproportionate effort, the Practice’s Caldicott Guardian will be consulted, and an assessment made. Details of this assessment will be documented.

**Step 6: Providing a response**

If the practice is satisfied that the personal data is accurate, then the IG lead will inform the individual without undue delay of the decision and that no amendments will be made. The practice will also provide the reasons for their decision and provide the individual with the option of adding a note to their record stating that they dispute the entry.

Where data has been confirmed as inaccurate, the IG lead will inform the individual without undue delay. The practice will provide details of the rectification and the reasons for this, along with details of any third parties informed of the rectification.

The IG lead will record the date of the response on the Practice’s individual rights log.

## 6.5.3 The Right to Erasure (Article 17)

The right to erasure under Article 17 of the UK GDPR stipulates that individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right only applies to data held at the time the request is received, it does not apply to data that may be created in the future.

This is not an absolute right and only applies in certain circumstances, see [Annex 1: Limited Rights](#_Annex_1:_Limited).

**Step 1: Establishing if the right applies**

The IG lead will refer to [Annex 1: Limited Rights](#_Annex_1:_Limited) and consider if the request meets the criteria to have the right upheld.

The Practice acknowledges that there are limited circumstances in which the right will apply to the processing it conducts. For example, the collection of patient email addresses to distribute the Practice newsletter.

**Step 2: Erase the relevant data**

If it is established that the right to erasure does apply, the Practice will erase the requested data without undue delay.

Where the Practice has any uncertainty, the IG lead will contact the DPO Support Service for advice prior to erasing any data.

The IG lead will record details of the erasure on the Practice’s individual rights log.

**Step 3: Informing 3rd Parties**

Where individual’s right to erasure applies and the applicable data has been previously shared or is subject to ongoing sharing to other organisations, the IG lead will contact each recipient to inform them of the erasure unless this proves impossible or involves disproportionate effort.

If the IG lead suspects this would this prove impossible or involve disproportionate effort, the Practice’s Caldicott Guardian will be consulted, and an assessment made. Details of this assessment will be documented.

**Step 4: Providing a response**

If it is established that the right to erasure does not apply, the IG lead will inform the individual without undue delay of the decision, noting that their request cannot be fulfilled and provide the reasons and an explanation for the decision.

In instances where the request meets the criteria to exercise the right to erasure, the IG lead will inform the individual without undue delay of the outcome and confirm that their request has been completed and actioned.

The IG lead will record the date of the response on the Practice’s individual rights log.

## 6.5.4 The Right to Restrict Processing (Article 18)

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that the practice uses their data. This is an alternative to requesting the erasure of their data and usually exercised where there are concerns about the accuracy of the information or how it’s being processed. In most cases, the restriction will only be in place for a period of time as opposed to having the processing restricted indefinitely.

This is not an absolute right and only applies in certain circumstances, see [Annex 1: Limited Rights](#_Annex_1:_Limited).

**Step 1: Establishing if the right applies**

The IG lead will refer to [Annex 1: Limited Rights](#_Annex_1:_Limited) and consider if the request meets the criteria to have the right upheld.

The Practice acknowledges that there are limited circumstances in which the right will apply to the processing it conducts. For example, whilst the accuracy of disputed data is verified.

**Step 2: Temporarily restrict processing**

When a request is received, as good practice, the practice will stop all processing of the data whilst the accuracy or the legitimate grounds for processing the personal data in question is considered. This may mean opting the individual out of any data sharing agreements that the practice is involved in until there is confidence that the practice is sharing the accurate information*.*

Processing includes a broad range of operations including collection, structuring, storing, dissemination, and erasure of data. Therefore, the practice will consider the following methods to restrict data:

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

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

* the individual has disputed the accuracy of the personal data and you are investigating this; or
* the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

**Step 3: Establishing if the processing of the data should continue to be restricted**

Once the practice has established the accuracy of the data, or whether the organisation’s legitimate grounds override those of the individual, the practice may decide to lift the restriction.

For requests where the accuracy of the information is disputed, the IG lead will follow the process outlined in [Section 6.4.2 The Right to Rectification](#_6.4.2_The_Right).

The practice recognises that there will be limited circumstances in which it relies upon Article 6(1)(f) Legitimate Interests as the legal basis for the processing it conducts. Therefore, for any request in which the legitimate interests is disputed, the IG lead will seek the advice of the DPO Support Service, and provide a copy of the Legitimate Interest Assessment in order for the legitimate interests of the practice and the individual to be considered.

 **Step 3: Informing 3rd Parties**

Where the restriction of the processing of the data is upheld and the applicable data has been previously shared or is subject to ongoing sharing to other organisations, the IG lead will contact each recipient to inform them of the restriction unless this proves impossible or involves disproportionate effort.

If the IG lead suspects this would this prove impossible or involve disproportionate effort, the Practice’s Caldicott Guardian will be consulted, and an assessment made. Details of this assessment will be documented.

**Step 4: Providing a response**

Following consideration of a request, the IG lead will inform the individual without undue delay of the Practice’s decision. Where processing is ceased individuals will be made aware of any potential impact this may have on their ongoing care or future treatment.

Where the restriction of the processing is to be lifted, the Practice must inform the individual **before** the restriction is lifted.

The IG lead will record the date of the response on the Practice’s individual rights log.

**Step 5: Lifting the restriction of processing**

Where it is decided the temporary restriction of the processing of the data is to be lifted, the IG lead will undertake the necessary steps to reverse any actions taken in Step 2 to lift the temporary restriction of processing.

## 6.5.5 The Right to Data Portability (Article 20)

The right to data portability allows individuals to obtain and reuse personal data they have provided to a data controller. This will be done in a structured, commonly used and machine-readable format.

This is not an absolute right and only applies in certain circumstances, see [Annex 1: Limited Rights](#_Annex_1:_Limited).

**Step 1: Establishing if the right applies**

The IG lead will refer to [Annex 1: Limited Rights](#_Annex_1:_Limited) and consider if the request meets the criteria to have the right upheld.

The Practice acknowledges that there are limited circumstances in which the right will apply to the processing it conducts.

**Step 2: Collating the data**

If it is established that the right applies, the IG lead will collate the applicable data in a format that is:

* structured;
* commonly used; and
* machine-readable

For example, CSV, XML or JSON format.

Only personal data which has been provided to the Practice by the individual will be within the remit of the request.

 **Step 3: Providing a response**

If it is established that the right to data portability does not apply, the IG lead will inform the individual without undue delay of the decision, noting that their request cannot be fulfilled and provide the reasons and an explanation for the decision. Where a request meets the criteria to exercise this right, a response will be provided to the individual without undue delay of the decision made and confirmation of the actions taken by the practice. Where data is transmitted electronically, the IG lead will take steps to ensure this is done securely, for example, utilising the Secure File Sharing Portal.

The Practice will not retain responsibility for further processing of the data following its transmission.

The IG lead will record the date of the response on the Practice’s individual rights log.

## 6.5.6 The Right to Object (Article 21)

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data. An objection may be in relation to all the personal data the practice holds about an individual or only to certain information. It may also only relate to a particular purpose that the practice is processing the data for and the legal basis for processing.

This is not an absolute right and only applies in certain circumstances, see [Annex 1: Limited Rights](#_Annex_1:_Limited).

**Step 1: Establishing if the right applies**

The IG lead will refer to [Annex 1: Limited Rights](#_Annex_1:_Limited) and consider if the request meets the criteria to have the right upheld.

**Step 2: Assessing legitimate grounds**

When a request meets the criteria to exercise the right, the IG lead and Caldicott Guardian and will review the specific reasons for the objection against the Practice’s legitimate grounds for processing:

Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority:

The Practice can refuse to comply if there are compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual or the processing is for the establishment, exercise, or defence of legal claims. On deciding whether the practice has compelling legitimate grounds which override the interests of an individual, the practice will consider the individual’s reasons for the objection in the first instance and balance the individual’s interests, rights, and freedoms with the practice’s own legitimate grounds.

Should the decision be to override the individual’s reasons, it will be the practice’s responsibility to demonstrate this.

Processing for the purposes of scientific/historical research and statistics:

Individuals must have “grounds relating to his or her particular situation” to exercise their right to object to processing for research purposes. If the practice is conducting research where the processing of personal data is necessary for the performance of a public interest task, the practice is not required to comply with an objection to the processing.

Direct Marketing:

The Practice will stop processing personal data for direct marketing purposes as soon as an objection is received.

The IG lead will document all decision making.

**Step 3: Actioning the objection**

Where the objection of the processing of the data is upheld, the IG lead will take steps to stop the processing of the data.

Depending on the circumstances of the request, appropriate action may include:

* Suppressing the data
* Erasing the data

Prior to erasing any data, the IG lead will seek advice from the DPO Support Service.

**Step 3: Informing 3rd Parties**

Where the objection of the processing of the data is upheld and the applicable data has been previously shared or is subject to ongoing sharing to other organisations, the IG lead will contact each recipient to inform them of the objection unless this proves impossible or involves disproportionate effort.

If the IG lead suspects this would this prove impossible or involve disproportionate effort, the Practice’s Caldicott Guardian will be consulted, and an assessment made. Details of this assessment will be documented.

**Step 4: Providing a response**

If it is established that that the right to erasure does not apply, the IG lead will inform the individual without undue delay of the decision, noting that their request cannot be fulfilled and provide the reasons and an explanation for the decision.

Where a request meets the criteria to exercise the right to erasure, the practice will inform the individual without undue delay of the outcome and confirm that their request has been completed and actioned.

The IG lead will record the date of the response on the Practice’s individual rights log.

## 6.5.7 Rights related to automated decision making and profiling (Article 22)

Automated individual decision-making and profiling is a decision made by automated means without any human involvement. Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. Automated individual decision-making does not have to involve profiling, although it often will do. One example of this includes using set criteria to assess individual’s priority to receive preventative vaccinations, i.e., Covid – 19 vaccination programmes.

Article 22(1) of the UK GDPR provides individuals with additional rules to protect them when organisations perform automated decision making that could potentially affect their legal rights or have similarly significant effects on them. Cathays Surgery will only carry this type of processing if the decision is:

* necessary for entering into or performance of a contract between an organisation and the individual.
* authorised by law (for example, for the purposes of fraud or tax evasion); or
* based on the individual’s explicit consent.

**Step 1: Processing a request**

The practice recognises that the right will only apply in certain circumstances and acknowledges that due to the nature of the processing the practice conducts, the number of requests the practice will receive will be limited. Therefore, should any requests regarding rights related to automated decision making and profiling be received, the IG lead will seek further assistance and guidance from the DPO Support Service.

**Step 2: Providing a response**

If it is established that the rights relating to automated decision making and profiling do not apply, the IG lead will inform the individual without undue delay of the decision, noting that their request cannot be fulfilled and provide the reasons and an explanation for the decision.

Where a request meets the criteria to exercise the right, the practice will inform the individual without undue delay of the outcome and confirm that their request has been completed and actioned.

The IG lead will record the date of the response on the Practice’s individual rights log.

## 6.6 Additional Considerations - Requests received from Third Parties

Under UK GDPR third parties can make individual rights requests on behalf of another individual if consent has been provided, or if they have the appropriate authority to act on the individual’s behalf. When responding to third party individual rights requests, Cathays Surgery will process the request in line with the process detailed in the applicable right above, along with the additional considerations detailed below.

## 6.6.1 Solicitor Requests

Often, a solicitor acting on behalf of a client will request access to information on behalf of an individual. In addition to the standard process outlined in the applicable right above, the additional considerations will be undertaken:

**Consideration 1: Has consent been received?**

The IG lead must be satisfied that the solicitor making the request is entitled to act on behalf of the individual. This may be in the form of a written consent or a completed authority form evidencing that the solicitor has consent from the individual to access their personal data.

It is the solicitor’s responsibility to provide evidence of this entitlement.

As good practice there may be occasions where the practice will verify consent with the individual.

**Consideration 2: Is the request excessive?**

There may be instances where a whole medical record has been requested when the case is specific to a certain timeframe, illness, or injuries. In these situations, the IG lead will review the amount of information that has been requested and if this is considered to be excessive, the IG lead will contact the individual and clarify the extent of the request and information to be disclosed to the solicitor.

**Consideration 3: Who should the response be disclosed to?**

If the individual has consented to the release of information to the solicitor, the practice may provide the response directly to the solicitor.

If the individual requests to receive the response, the individual’s wishes will be upheld and the response will be provided to the individual.

All disclosures will be made by secure means, as outlined within the standard process.

## 6.6.2 Requests for access to Deceased Records

The UK GDPR does not apply to deceased individuals, however, the ethical obligation to respect a patient’s confidentiality extends beyond death. Requests for access to deceased records should be made under the Access to Health Records Act 1990 (AHRA) which provides a small cohort of individuals with a statutory right to apply for access to information contained within a deceased person’s health record.

In addition to the standard process outlined in the right of access above, the additional considerations will be undertaken**:**

**Consideration 1: Is the record still held by the Practice?**

On becoming aware of an individual’s death, the Practice will transfer the record to NHS Wales Shared Services Partnership (NWSSP). If a request for access to a deceased individual’s record is received prior to the record being transferred to NWSSP, the Practice will process and respond to the request.

If the record has transferred to NWSSP, the IG lead will inform the applicant of this and provide the appropriate contact details:

[Health Records Request - NHS Wales Shared Services Partnership](https://nwssp.nhs.wales/ourservices/primary-care-services/general-information/health-records-request/)

**Consideration 2: Does the requester have authority to access?**

If the record is still held by the practice, the IG lead will review the request to establish if the third party meets the requirements defined under section 3(1)(f) of the AHRA. These being:

* “‘the patient’s personal representative” and
* “any person who may have a claim arising out of the patient’s death”.

Where evidence of authority has not been received, the IG lead will request this prior to processing the request.

A personal representative is the executor or administrator of the deceased person’s estate. The personal representative is the only person who has an unqualified right of access to a deceased patient’s record and does not need to give a reason for applying for access to a record.

Where the applicant is a person who may have a claim arising out of the patient’s death and is not a personal representative of the deceased, only information relating to that claim will be disclosed.

In the absence of appropriate authority, the IG lead will consult with the Practice’s Caldicott Guardian to consider if a limited disclosure in line with BMA guidance is appropriate. Disclosures in this area are complex and the Caldicott Guardian will ensure all decision making is documented.

[bma-confidentiality-and-health-records-toolkit-july-2021.pdf](https://www.bma.org.uk/media/4283/bma-confidentiality-and-health-records-toolkit-july-2021.pdf)

**Consideration 3: What were the individual’s wishes or expectations?**

The IG lead will consult with the Practice’s Caldicott Guardian to consider any preferences expressed by the deceased prior to death for any information to remain confidential, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. If the deceased individual expressed a wish for information to remain confidential this will be upheld regardless of who is making the request unless there is an overriding public interest in disclosing.

**Consideration 4: When do we have to respond?**

Requests for deceased records will be processed and a response provided within 40 calendar days, no charge will be applied.

All disclosures will be made by secure means, as outlined within the standard process.

## 6.6.3 Requests relating to individuals who lack mental capacity

Access requests made relating to individuals who lack mental capacity have no specific provisions under the UK GDPR or Mental Capacity Act 2005. Therefore, the Practice position is that an attorney with authority to manage the affairs of an individual (or under a deputyship order) will have the appropriate authority to exercise an individual’s rights on their behalf.

The Lasting Power of Attorney (LPA) gives the attorney authority to make decisions on behalf of the person who has requested the LPA (known as the Donor) and the attorney has a duty to act or make decisions in the best interests of the person who has made the LPA. There are two different types of LPA:

1. A personal welfare LPA is for decisions about both health and personal Welfare.

2. A property and affairs LPA is for decisions about financial matters.

In addition to the standard process outlined in the applicable right above, the additional considerations will be undertaken**:**

**Consideration 1: Does the individual have capacity?**

Prior to processing the request, the IG lead will review the patient’s record to ascertain if a statement of the individual’s capacity is recorded.

If there is any uncertainty regarding the individual’s capacity the IG lead will consult the Practice’s Caldicott Guardian, and if necessary, the patient will be invited into the Practice for a clinician to make an assessment on the individual’s capacity.

**Consideration 2: Does the requester have authority to act?**

The practice will need to satisfy that the attorney is acting within the powers given within the LPA, that they are entitled to ask for this information in the same way the individual would have done if they had the capacity to do so. The IG lead will request formal evidence that the individual holds the necessary LPA.

Where no appropriate authority is in place the IG lead will inform the requester that unfortunately, Next of Kin has no formal legal status. There are no rights given to Next of Kin to access a person’s medical records or make decisions on behalf of them. However, where there are no nominated individuals, they may wish to apply to be a deputy through the court of protection.

Where the IG lead in consultation with the Practice’s Caldicott Guardian establish that disclosure is in the individual’s best interests, a limited disclosure which is limited to information relevant to the purpose may be considered.

## 6.6.4 Requests for Children’s personal information

A child has the same rights as any adult under the UK GDPR regardless of their age, however some children will not be competent to understand and exercise their rights themselves and therefore will likely have their rights exercised by those who have parental responsibility for them.

In addition to the standard process outlined in the applicable right above, the additional considerations will be undertaken**:**

**Consideration 1: Is the child competent?**

Children aged over 16 years are presumed to be competent and have equal rights as an adult. Children who are aged 12 or over are also generally expected to have the competence to give or withhold their consent to the release of information from their health records.

In cases where a child is 12 years or older, they would generally be expected to exercise their own rights or provide consent for their parents or guardian to exercise those rights on their behalf.

There may be some instances where a child may present the ability to understand their rights at a younger age. In these cases, the IG lead in consultation with the Practice’s Caldicott Guardian will determine if the child can understand what it means to give their consent by utilising the Gillick Competence test.

**Consideration 2: Does the requester have parental responsibility?**

Where a child is not competent to exercise their own rights, a person with parental responsibility may exercise the child’s rights on their behalf. The IG lead will request evidence of parental responsibility from the requester, such as a copy of the birth certificate along with photo ID.

Where the IG lead has reason to believe parental responsibility has been removed, additional checks will be undertaken.

**Consideration 3: Is the request in the child’s best interest?**

As the parent is exercising the right on behalf of the child, the Practice will consider if the request is in the best interests of the child.

Considerations include:

* the nature of the personal data
* 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.

6.7 Refusing a request and complaints

The Practice can refuse a request should it be deemed to be manifestly unfounded, excessive in nature or if an [exemption applies](#_Annex_2:_Exemptions). Deciding whether a request qualifies for refusal should be based on the context and needs to be justified.

If it is decided to refuse an individual’s request to exercise their right(s), the IG lead will inform the individual without undue delay and within one month of receipt of the request. The response will outline:

* the decision made by the Practice
* an explanation for the decision to refuse and on what grounds
* a point of contact for the Practice, who will be the IG lead
* the right to make a complaint to the Information Commissioner’s Office, including contact details.

The IG lead will maintain a record of the decision demonstrating the reason for the refusal should the Information Commissioner’s Office (ICO) request evidence of this.

Under the UK GDPR, in most cases a fee cannot be charged. However, where the request is manifestly unfounded or excessive, the practice may charge a “reasonable fee” for the administrative costs of complying with the request.

The Practice may also charge a reasonable fee if an individual requests further copies of their data. The fee must be based on the administrative costs of providing further copies.

The IG lead will record the date of the response on the Practice’s individual rights log.

## **7 Review**

This procedure will be reviewed every one year or more frequently where the contents are affected by major internal or external changes such as:

* Changes in legislation;
* Practice change or change in system/technology; or
* Changing methodology.

# Annex 1: Limited Rights

## **Right to Erasure:**

Source: [Right to erasure | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/)

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 must do it to comply with a legal obligation; or
* we have processed the personal data to offer information society services to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation;
* for the performance of a task carried out in the public interest or in the exercise of official authority;
* for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
* for the establishment, exercise or defence of legal claims.
* If you are required by law to process individuals’ personal data, then the right to erasure will not apply.

The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

* if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
* if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

## **Right to Restrict Processing:**

Source: [Right to Restrict Processing | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/)

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

* The individual contests the accuracy of their personal data and the practice are verifying the accuracy of the data.
* The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead.
* The practice no longer needs the personal data, but the individual needs the practice to keep it in order to establish, exercise or defend a legal claim; or
* The individual has objected to the practice processing their data under Article 21(1) (the right to object), and the practice is considering whether their legitimate grounds override those of the individual.

## **Right to Data Portability:**

Source: [Right to data portability | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/)

The right to data portability only applies when:

* your lawful basis for processing this information is consent **or** for the performance of a contract; and
* you are carrying out the processing by automated means (ie excluding paper files).

## **Right to Object:**

Source: [Right to object | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/)

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

Individuals can also object if the processing is for:

* a task carried out in the public interest;
* the exercise of official authority vested in you; or
* your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

An individual can also object where you are relying on one of the following lawful bases:

* ‘public task’ (for the performance of a task carried out in the public interest),
* ‘public task’ (for the exercise of official authority vested in you), or
* legitimate interests.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

In these circumstances this is not an absolute right, and you can refuse to comply if:

* you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
* the processing is for the establishment, exercise or defence of legal claims.

# Annex 2: Exemptions

The Data Protection Act 2018 provides several exemptions from specific UK GDPR provisions. Where an exemption applies, the Practice is not required to comply with individuals’ rights. The most relevant exemptions to the Practice are:

* Information required to be disclosed by law or in connection with legal proceedings
* Legal professional privilege
* Disclosure prohibited or restricted by an enactment
* Health data – an individual’s expectations and wishes
* Health data – serious harm

A full guide to exemptions is available on the ICO website - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>