Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

# Expectations Guidance Document

## 1.4 Individual Rights

# Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Individual Rights section of the Welsh Information Governance Toolkit (WIGTK).

You will need to consider your Organisation's procedures in regards to upholding individual rights, staff responsibilities and awareness, along with how the organisation provides privacy information to individuals.

You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.

The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

Please note, in this section of the WIGTK you will be required to upload copies of the relevant procedures if you have ticked that your organisation has them available.

# Minimum Expectations

**Processes for dealing with Individual Rights Requests**
Your organisation should have an individual rights policy or procedure in place which states that under UK GDPR individuals have the following rights regarding their data:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

You should be able to provide individuals with clear and relevant information about their rights and how to exercise them. Your organisations policies and procedures should clearly set out processes for how staff should process any requests.

Your procedures should account for the different types of personal data you process including, but not limited to, health records, staff records, emails and other communication methods and CCTV.

**Staff awareness and responsibilities**
All staff should receive training or guidance on what constitutes as an individual rights request. Staff should be able to recognise a range of requests, know they can be made in

writing or verbally and know who the request needs to be forwarded to, along with the importance of doing this without delay due to the strict timeframes that apply.

There must be a specific person or team who is responsible for managing and responding to requests. The chosen member of staff or team should receive specialised training to handle the requests, including regular refresher training.

It is also important to note that additional staff should be trained to carry out these requests and tasks in times of absence. The organisation should be aware of having sufficient resources to deal with these requests as these will need to be processed within a one-month window. This highlights the importance of all staff being able to recognise requests and be aware of the reporting processes.

The request should be dealt with in a timely manner, ideally as soon as possible when the request is first submitted and should be actioned within one month.

**Maintaining a log within the Organisation**

It is important that the organisation keeps a log of all written and verbal individual rights requests received.

This allows the organisation to record receipt of the request, track it's progress and the outcome. The log should include the following:

- A reference number for the request
- The date the request was received
- The right being exercised
- The date the response is due
- The date the response is provided
- If any information was disclosed/actions taken as a result
- If the request was refused or an exemption was applied, and the reason for this.

Keeping an accurate log will not only help with monitoring the outcome or progress of an individual rights request but also assist if there are any complaints in the future. The log will provide the organisation with accountability, and they can go back to the log and review the request and outcome efficiently.

A checklist records the key stages in the request handling process, such as which systems or departments have been searched. This can form part of the log or be recorded in a separate document.

**Privacy information**

The organisation is required to publish transparency information about their data processing activities under Article 13 of the UK GDPR. This helps to inform people about their rights under data protection legislation and how to exercise them. This is known as privacy information and should include the following:

- The organisation's contact details
- The Data Protection Officer's contact details (if your organisation has one)

- If your organisation is not the Controller, the details of the Controller and their Data Protection Officer
- What personal data you are processing
- The purpose of your processing
- The names or categories of organisations the data will be shared with
- The lawful basis for processing
- A list of rights and how they apply to the processing you are undertaking.
- The retention period for the data (in line with the Records Management Code of Practice for Health and Social Care 2022)
- That individuals have a right to complain to the ICO, and their contact details

Where applicable to the processing, the following details should also be included in the organisation's privacy information:

- What the legitimate interests are if this is your legal basis for processing
- Details of data transfers to countries outside the UK and what safeguards are in place to protect the data.
- Where consent is being used as a legal basis for processing, how consent can be withdrawn

All staff should be aware of where they can locate privacy information and front-line staff should be able to explain the necessary information to data subjects and provide guidance.

Children need to have the same level of transparency about how their data is used. The UK GDPR has specific provisions regarding the privacy information for both children and adults, this includes ensuring it is concise, easily accessible and written in clear, plain language. Where the organisation processes children's information, privacy information should be provided in an appropriate format to meet their needs.

Privacy information should be made freely available and communicated in a way that is effective to the target audience. It is best practice to utilise a layered approach, which includes providing high level information such as posters with QR codes and further links sign posting individuals to more detailed information.

Privacy information should inform individuals as to whether your organisation is transferring personal data to any third countries or is relying on legitimate interests as a lawful basis. Where this is the case, the legitimate interests pursued by the organisation should be explained. Additionally, if the organisation relies on consent as the lawful basis for any of its processing, privacy information should inform individuals of the right to withdraw consent.

**Maintaining Responses - HB/Trust/SHAs and Prison Healthcare only**
The organisation's responses to individual rights requests should be maintained in line with the Records Management Code of Practice. This outlines a minimum retention period of three years for subject access requests (SAR), when the SAR has been subject to an appeal, the minimum retention period increases to six years. It is good practice to retain both the information disclosed and any information withheld, as well as the justification for any decision making, along with any subsequent correspondence.

## Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

**Maintaining Responses – General Practices, Community Pharmacies, Optometrists, Dentistry and Urgent and Emergency Care only**

The organisation's responses to individual rights requests should be maintained in line with the Records Management Code of Practice. This outlines a minimum retention period of three years for subject access requests (SAR), when the SAR has been subject to an appeal, the minimum retention period increases to six years. It is good practice to retain both the information disclosed and any information withheld, as well as the justification for any decision making, along with any subsequent correspondence.

**Performance Reports – HB/Trust/SHAs and Prison Healthcare only**

Organisations should produce regular reports to monitor requests and ensure they are correctly dealt with under Data Protection legislation. Your report should contain the following information:

- Number of individual rights requests received
- Number responded to within the calendar month timeframe
- Number of cases where an extension was applied and the reasons for the extension
- Number of requests which exceeded the statutory deadlines and the reason for these
- Details of any complaints made about any response or the process itself
- Details of any requests that have been escalated to the Information Commissioner's Office by the applicant

Based on these reports the IG Committee/Group can monitor performance and agree on any necessary improvement plans or recommendations for improvements,

**Ensuring accuracy of records – HB/Trusts/SHAs, Prison Healthcare and Third Party Contractors only**

The Organisation is required to take reasonable steps to check the accuracy of the personal information it holds. Example evidence for this would be copies of data quality checks/reports or processes and procedures in place for routine checking.

High quality information is required to inform high quality patient care. If information held by organisations is inaccurate there could be consequences for care, treatment, and safety.

Checks on the accuracy of information should occur whenever individuals present or where their records are being updated, examples include:

- When attending appointments
- When receiving care or treatment as an hospital admission
- When referrals are received

- When individuals contact booking centres

**Reviewing privacy information**
The organisation should review its privacy information and update it whenever there is a new project, asset, or change to service or processing of data.

Privacy information should be regularly reviewed to ensure it remains accurate and up to date. It should explain in full what your organisation does with the personal data it is collecting and the reasons why to ensure individuals are appropriately informed.

**Communicating new purposes for processing to individuals – HB/Trusts/SHAs and Prison Healthcare only**
If the organisation has plans to use personal data for a new purpose, there should be up to date privacy information in place. This should also be communicated to all individuals before starting the new processing.

The organisation should make all staff aware of any updates to processing through the inclusion of a statement to the affect in the relevant policy or procedure.

The evidence required for this would be a copy or extract from a relevant policy or procedure.