Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Frequently Asked Questions

Community Pharmacies

Do Community Pharmacies require a Data Protection Officer (DPO)?

Yes, all Community Pharmacies (CPs) are required to appoint a Data Protection Officer. Under the UK GDPR, you must appoint a DPO if you are a public authority or body. CPs operates on a contractor model similar to other primary care providers, such as general practices. This means CPs are usually independent businesses, contracted by the NHS to provide certain services for local populations. The services provided under contract with the NHS are subject to the provisions of the UK GDPR, meaning that a DPO is required for pharmacies processing health data for NHS services, as they undertake large scale processing of special categories of data (health data is an example of a type of special category of data). CPs should ensure that a DPO takes responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. CPs can appoint their own DPO or utilise a DPO organisation/service.

The Information Commissioner's Office (ICO) is sympathetic to the position of small CPs, their advice is when a Pharmacy Manager (or staff member) becomes a DPO, the decision and reasons behind it should be documented and retained as part of the 'accountability' that the UK GDPR requires. Furthermore, they suggest that where possible, any conflicts of interest between a person's current role and that of DPO should be recorded, along with mitigating measures to reduce or eliminate such conflicts.

Are Community Pharmacies subject to the Freedom of Information Act (FOIA) 2000?

The Freedom of Information Act 2000 (FOIA) is designed to ensure that individuals and organisations can gain access to information about publicly-funded services. CPs, like other NHS bodies, are recognised as public authorities under the FOIA. Therefore, CPs are subject to FOIA and are required to respond to requests, providing information relating to the provision of NHS pharmaceutical services.

Are Community Pharmacies required to have a Publication Scheme?

The Freedom of Information Act 2000 (FOIA) requires all public authorities to adopt and maintain a publication scheme. Those providing pharmaceutical services under contract to the NHS in England, Wales and Northern Ireland are public authorities specifically in respect of information relating to those services. The publication scheme is only for information held by a pharmacy business as a public authority, and not for its wider business. A public authority would be in breach of FOIA if it has not adopted a publication scheme or is not publishing in accordance with it.

What is a Record of Processing Activities (ROPA)?

Record of Processing Activities (ROPA) is a legal requirement under Article 30 of the UK GDPR to keep a record of your processing activities, every piece of data processing you do needs to be recorded. The documentation of your processing activities must be in writing; this can be in paper or electronic form. Generally, organisations will benefit from maintaining their documentation electronically so they can easily add to, remove, and amend it as necessary. A good way to start is by doing an information audit or data-mapping exercise to clarify what personal data your organisation holds and where it is stored. A record of processing activities should include as a minimum, the following:

- Contact details of all parties including their DPOs
- The purpose and lawful basis for processing.
- Whose data is collected such as patients, staff and service users.
- The categories of the personal data collected.

- Transfer details, particularly when data moves across countries, and any safety measures that are put in place to protect the data.
- Retention schedules, such as short-term and long-term storage timelines and protection plans.
- An overview of the security measures, both technical and otherwise, that safeguard the data.

Keeping a record of your processing activities is not a one-off exercise; the information flows you've documented must reflect how processing activities have changed overtime. You should treat the record as a live document that you update as and when necessary. This means conducting regular reviews to ensure your documentation remains accurate and up to date.

What is a Data Protection Impact Assessment (DPIA)?

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 enforces a legal requirement to conduct a DPIA for types of processing likely to result in a high risk to the rights and freedoms of individuals. A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve. DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising. Under UK GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to £8.7 million, or 2% global annual turnover if higher. By considering the risks related to your intended processing before you begin, you also support compliance with another general obligation under UK GDPR: data protection by design and default.