The General Data Protection Regulation and associated legislation

Part 2: Guidance for Community Pharmacy (shorter version)

Version 1: 25th March 2018

Community Pharmacy
GDPR Working Party

DATA PROTECTED – this mnemonic will help you to remember the 13 steps to assist you implementing and complying with the GDPR.

Contents

Step 1. Decide who is responsible

Summary:

- You as the owner of the pharmacy business are responsible for data protection and security, and compliance with the GDPR.
- It is sensible to appoint one person to lead efforts to comply with the GDPR. This could be the Information Governance (IG) lead.
- You may also need to appoint a Data Protection Officer (DPO).

Action: Complete **Template A** (Part 3), listing the names of relevant people involved with IG, including who will lead your efforts to comply with the GDPR.
Action: Large-scale pharmacy businesses should appoint a DPO; smaller businesses should await further information on this from us.

Step 2. Action plan

Summary:

- Data protection and confidentiality of patient data are the responsibility of the pharmacy team, not just the business, so all staff will need training.
- You can use the 13 steps in these information booklets to understand the framework of the GDPR.
- You will also need to continue to pay an annual fee to the ICO.

Action: Work through the action plan for pharmacy businesses set out in **Template B** (Part 3), adding the date when you completed each part of the plan. This will involve updating some of your existing procedures.
Action: Continue to pay an annual fee to the ICO.
Action: Train staff as appropriate on the GDPR.

Step 3. Think about and record the personal data you process

Summary:

- Any system, whether paper or electronic e.g. on a database, containing searchable personal data is a 'filing system' and should be considered.
- Pseudonymised data is data that could be attributed to a specific individual person if combined with additional data, the GDPR also applies to such data.
- You will need to have a record of all the filing systems that your pharmacy holds, and of how you collect, store and use all personal data. This will need to be reviewed on an ongoing basis – we suggest annually.
- The IG Toolkit is being updated to reflect the GDPR, so this work will help towards completion of the updated Toolkit in due course.

Action: Complete **Template C** (Part 3), in which we have identified various categories of personal data processed by community pharmacies, to confirm what processing is undertaken by your pharmacy and to add any other processing you do.

Step 4. Assure your lawful basis for processing

Summary:

- The GDPR requires all organisations to have a lawful basis for processing personal data. For much data in pharmacies this will be '**for the performance of a task carried out in the public interest**'.
- Personal data concerning health is further protected and pharmacies must have one of the stated reasons for processing it. These include: 'the provision of healthcare or treatment'.
- You will also need to consider personal data about employees.
- You will need to decide and record your lawful basis for processing.
- You must provide people with information about how you process their data: the Privacy Notice.

Action: Your lawful basis for processing personal data, and additional details for processing special categories of personal data, must be recorded. This is described in **Template C** (Part 3) for various pharmacy activities and you must confirm this applies to you or amend details as appropriate.

Step 5. Process according to data protection principles

Summary:

- All personal data must be processed in accordance with data protection principles, and you must be able to document this through your policies and records.
- Pharmacies should already be broadly compliant with the data protection principles, as part of their ongoing IG requirements, but must check that they can document this.
- Completing the **Workbook for Community Pharmacy** will further help to demonstrate compliance.

Action: Complete the **Workbook** to assist compliance**,** and **refer to Template D** (Part 3), which is a reminder of other relevant information that you should have in place for IG purposes already.

Step 6. Review and check with your processors

Summary:

- You must have data protection guarantees from anyone who processes personal data for you, such as your PMR supplier.
- Your existing contracts may confirm GDPR compliance, but if not, you will need to seek guarantees.
- You may also need to give guarantees if you are asked for them by other data controllers.

Action: Identify and list your processors in **Template E** (Part 3).
Action: Liaise with your processors to check and record whether your existing contractual terms are sufficient to confirm GDPR compliance. Template E includes details of what your contractual relationship should include for GDPR compliance.
Action: Respond to any requests that you receive from those for whom you process information, or commissioners, asking for you to confirm compliance with GDPR.

Step 7. Obtain consent if you need to

Summary:

- Consent or explicit consent is a lawful basis for processing personal data.
- Pharmacies already have a lawful basis for much of their data processing (as described in step 4), so are unlikely to need to seek consent for data processing.
- Note that consent for data processing is not the same as consent for service provision, which will still be needed.
- Certain functions, such as direct marketing, may require consent, in which case you need to ensure the consent is GDPR compliant and that you have a record of it.

Action: Use **Template F** (Part 3) to list any personal data held in filing systems where consent is the basis for obtaining the data, and for each of these confirm you have GDPR compliant consent and that you have a record of this.

Step 8. Tell people about your processes: the Privacy Notice

Summary:

- A key principle of the GDPR is the provision of clear information to people about how their data is being used (or 'processed').
- This could be provided in the form of a Privacy Notice.
- Pharmacies will need to have this notice available on their premises and should draw it to the attention of new customers.
- If personal data is to be used for any purpose other than that which it was collected for, further information must be provided to the person to whom the data relates (the data subject).

Action: Review the two versions of the privacy notice provided in **Template G** (Part 3) to decide what will be an appropriate Privacy Notice for your pharmacy. You may have to add to this if you undertake additional processing of personal data.
Action: Ensure that your notice is available in the pharmacy premises and online, and that staff know how to access this and when it should be shown to patients.

Step 9. Ensure data security

Summary:

- The GDPR requires anyone processing personal data to take steps to ensure data security.
- Pharmacies should already have policies on data security, but you may need to seek assurances e.g. from PMR suppliers that all processed data will be secure.
- You may need to train staff on security of personal data.

Action: Work through **Template H** (Part 3) to ensure that you have all the required policies in place already to assure security within the pharmacy.
Action: If necessary, seek assurances from your providers about data security.

Step 10. Consider personal data breaches

Summary:

- Pharmacies must have policies and procedures in place to cover any data breaches.
- Breaches likely to affect people's rights and freedom, for instance, the loss of a prescription bundle in a public place, must be reported to the ICO, and sometimes to the people affected.
- Reports to the ICO must include relevant information and be made without undue delay.
- You must record all data breaches, even if they are not reported to the ICO.
- You should be able to show that you have learnt from and responded to any data breach.

Action: Work through **Template I** (Part 3), which provides an updated *Information Security Incident Management Procedures* (currently Template 11 in the IG templates provided by PSNC for pharmacy contractors) and a table to record any personal data breaches, and, if appropriate, put these in place for your pharmacy.
Action: Keep a copy of **Template J** (Part 3) for use if a data breach occurs.

Step 11. Think about data subject rights

Summary:

- The GDPR gives people a number of rights about how they can access and seek to control processing of their personal data.
- Your pharmacy must be aware of these and ready to respond to requests.

Action: Ensure you are familiar with all the key rights of patients and customers whose data you hold as set out in **Template K** (Part 3) and that you are ready to respond to these and other requests from data subjects. Note that request may come from people seeking information about your processing or seeking to exercise their rights.

Step 12. Ensure privacy by design and default

Summary:

- Privacy and data protection should be key considerations in the early stages of any project, such as installing a new IT system.
- The GDPR makes considering data protection by design and default a legal requirement.
- Pseudonymisation of data is likely to be a useful data protection measure in many scenarios.

Action: Ensure that your IG Lead and others involved in IG, including your DPO (if applicable) consider privacy by design and default. Use **Template L** (Part 3) to record the activities you have considered.

Step 13. Data protection impact assessment

Summary:

- The GDPR requires that a Data Protection Impact Assessment (DPIA) be carried out for certain data processing activities where there is a high risk to the rights and freedoms of individuals. This includes all processing of healthcare data, but exemptions apply where data is processed to meet legal requirements or in the performance of a task in the public interest, or where an assessment was previously carried out.
- We are awaiting ICO guidance, but, in our view, most smaller pharmacies will not need to carry out a DPIA for normal dispensing practices.
- All pharmacies will need a DPIA when introducing any new technologies.

Action: Use **Template M** (Part 3) to help you consider which pharmacy activities may require a DPIA, then carry any necessary assessments out with the help of your DPO.

Mapping the steps to the workbook templates

Part 3 of this guide is the **Workbook for Community Pharmacy**, which contains templates relating to each of the 13 steps. The templates correspond to the steps as follows.

1. **D**ecide who is responsible	Template A
2. **A**ction plan	Template B
3. **T**hink about and record the personal data you process	Template C (joint)
4. **A**ssure your lawful basis for processing	Template C (joint)
5. **P**rocess according to data protection principles	Template D
6. **R**eview and check with your processors	Template E
7. **O**btain consent if you need to	Template F
8. **T**ell people about your Privacy Notice	Template G
9. **E**nsure data security	Template H
10. **C**onsider personal data breaches	Template I Template J
11. **T**hink about data subject rights	Template K
12. **E**nsure privacy by design and default	Template L
13. **D**ata protection impact assessment	Template M