Community Pharmacy Scotland

The General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2017

Part 2: Summary Guidance for Community Pharmacies

Version 1: April 2018

With thanks to the Community Pharmacy GDPR Working Party for sharing resources

Community Pharmacy GDPR Working Party

Contents

There are 12 key considerations which should be regularly reviewed to ensure consistent GDPR compliance. These are laid out in chapters below and will give you some background information to help you complete your GDPR workbook.

1. Decide who is responsible

Summary

- The owner of the pharmacy business is responsible for GDPR compliance including data protection and security.
- It would be sensible to appoint one person to co-ordinate your work on GDPR.
- You may also need to appoint a Data Protection Officer.

Action

- Complete Template A of the Workbook with details of the people in your business who are responsible for Information Governance.
- Large-scale pharmacy businesses should appoint a DPO; smaller businesses should consider this whilst awaiting the outcome of the DPA Bill's progress for potential exemption.

2. Action Plan

Summary

- Data protection and confidentiality is the whole team's responsibility in day-to-day operations, so all staff will need training.
- Use these information resources to understand the framework of the GDPR
- You will need to continue to pay an annual fee to the ICO.

Action

- Work through the Action Plan in Template B to create a live action plan, updating as you make progress towards compliance.
- Continue to pay the annual ICO fee
- Train staff as appropriate

Action

- Work through the Action Plan in Template B to create a live action plan, updating as you make progress towards compliance.
- Continue to pay the annual ICO fee
- Train staff as appropriate

3. Record all the types of personal data which you process

Summary

- Any personal data, whether in paper or electronic form, should be considered as part of your review.
- Pseudonymised data is also covered by the GDPR. This is where the data you hold could be attributed to a person using additional data.
- You will need to make a record of all the places your pharmacy business holds personal data, and how it is collected, stored and used. This will need to be regularly – we would suggest on at least an annual basis.

Action

Complete Template C in the Workbook – we have identified various categories of personal data which most community pharmacies will process. You will need to confirm that these apply to you, and add any additional processing that you undertake.

4. Determine your legal basis for processing the personal data you have identified

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', or as part of a 'legal obligation'.
- 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 of the workbook for various pharmacy activities and you must confirm this applies to you or amend details as appropriate.

5. Make sure you process data in accordance with 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.
- Most Pharmacies will already be broadly compliant with the data protection principles, 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, completing Template D.

6. Review your agreements with Data 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

- Use Template E of the workbook to identify and list your processors
- 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.
- Respond to any requests that you receive from those for whom you process information, asking for you to confirm compliance with GDPR.

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 of the Workbook to list any personal data you have 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.

8. Inform people how you use their data and what your legal basis for doing so is

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 Privacy notice examples in Template G of the workbook, amending or adding as appropriate for your business. (Please note – there are certain details which MUST appear on a privacy notice – see the full guidance in Part 1 for details)
- 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

9. Ensure security but be ready for unintended data breaches

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.
- 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 H of the Workbook using your existing internal policies to assure security within the pharmacy.
- If necessary, carry out training specifically on data security with your staff
- If necessary, seek assurances from your providers about data security

10. Be ready for Data Subject rights requests

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 I of the Workbook 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.

11. Design your processes with privacy in mind

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 J of the workbook to record the activities you have considered.

12. Carry out a Data Protection Impact Assessment where necessary

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

A draft data protection impact assessment is included in your workbook as **Template J**.

Acknowledgements

We would like to thank the Community Pharmacy GDPR Working Party for sharing the structure and content of their guidance with CPS.