Community Pharmacy Scotland

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

Part 1: 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

Situation

The GDPR and DPA 2017 will require community pharmacy owners and their teams to understand and comply with new rules in relation to the processing of personal data, which is part of daily practice. We have provided four documents to help you to do this:

- Part 1: An introduction to and **guidance** on the GDPR/DPA (This document)
- Part 2: **Summary guidance** for quick reference
- Part 3: A **Workbook** which can be used to check and demonstrate compliance – this should be completed before the 25th of May 2018 and reviewed at least annually
- Part 4: A set of **FAQs** which address common questions on this subject

Background

The General Data Protection Regulations (GDPR) are new EU laws which aim to unify and strengthen data protection for all individuals in the European Union and the UK. These come into effect on the 25th of May 2018.

The Data Protection Act 2017 replaces the DPA 1998 and describes how some parts of the GDPR are applied in the UK. It also covers some areas which the GDPR does not. For ease, in this document we will refer to both sets of legislation as the **GDPR**.

Together, these two pieces of legislation seek to modernise the way in which data should be handled to reflect the ways in which organisations now use personal information, which were unforeseen when previous data protection laws were written. The rights of data subjects (people whom data relates to) are also expanded and made clearer.

Data protection will still be regulated by the Information Commissioner's Office (ICO).

Assessment

GDPR has attracted a lot of media attention, in the main suggesting that the changes will be significant and difficult to achieve in time for the 25th of May. There has also been a great deal of publicity around the ICO's increased powers to fine organisations for non-compliance. However, the ICO have described the transition as an evolution, not a revolution – and compliance will be a journey which they will support organisations with. Financial penalties tend to be reserved for where there has been gross negligence, intentional misuse of data or failure to co-operate in investigations and the ICO have indicated that they wish fines to remain proportionate to the offence committed.

Data is generally handled in accordance with current data protection laws in community pharmacy. Although there is work to do, you are likely to be in a strong starting position.

As the legislation itself is complex, and the ICO's guidance, whilst excellent, is generalised for any organisation, there is a need for clear, sector-specific guidance which covers data processing activities common to all community pharmacies in Scotland. We have produced this with help from other UK pharmacy bodies. However, this guidance does not substitute the responsibility that the pharmacy business has for GDPR compliance, nor the responsibilities of its owners or directors to maintain this compliance. There may be areas of business practice out of the scope of this guidance which you will have to address individually, such as direct marketing.

Recommendation

In order to prepare for the GDPR, pharmacy contractors should familiarise themselves with the guidance provided and complete the actions in the workbook. This should be retained and reviewed on at least an annual basis such that they are satisfied with their ongoing compliance.

If you are concerned about getting everything done on time, the Information Commissioner Elizabeth Denholm has said in a recent blog that "GDPR compliance will be an ongoing journey"; and "… if you can demonstrate that you have the appropriate systems and thinking in place you will find the ICO to be a proactive and pragmatic regulator aware of business needs and the real world". This should hopefully reassure you as you work towards compliance.

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

The owner of the pharmacy business - the data controller - and the directors and officers (senior staff) of the business have responsibility for data protection in the pharmacy and the implementation of the GDPR.

The superintendent pharmacist, Information Governance (IG) lead, or other person employed or engaged by the pharmacy business may have specific responsibilities for data protection and implementation of the GDPR.

The pharmacy team must have training about the GDPR and IG, appropriate to their role.

The Data Protection Officer (DPO) is a formal role laid out in the legislation which some organisations will have to appoint. This role comes with specific responsibilities, for example, to have knowledge of the pharmacy business and expertise in data protection rules, so that they are able to give appropriate advice to the pharmacy business. Two or more pharmacy businesses can share a DPO. More information on the full role of the DPO can be found in our FAQs (Part 3 of this pack).

The draft Data Protection Act 2017 deems all community pharmacies to be public authorities, which means that they must have a DPO. We, amongst others, consider that this is inappropriate for many pharmacy businesses, where the costs of engaging a DPO are disproportionate to the benefits; and accordingly, pharmacy bodies across the UK are seeking an amendment to the draft legislation. We are also pursing an alternative approach, which is for the role of the DPO in smaller pharmacies to be applied pragmatically. However, as neither can be guaranteed, it is suggested that smaller pharmacy businesses start considering the appointment of a DPO who can fulfil the full role, although do not appoint this pack will be updated to reflect any changes from the current direction of travel.

NB: If you process personal data concerning health on a ‘large scale’ you must have a DPO, regardless of whether you are deemed to be a public authority. There is little guidance on what amounts to large scale but processing by an individual practitioner is unlikely to be large scale, whereas processing by (for example) a hospital is likely to be large scale.

Action

You should record in **Template A** of your workbook the name of the pharmacy/pharmacy business and, as appropriate, the directors and officers (senior staff) who have agreed, or been given, specific responsibilities for data protection and implementing GDPR. You can also record the name of the person who will be your DPO.

2. Action Plan

Once you have decided who is responsible for GDPR compliance (may be more than one individual), it is a good idea to create a live action plan which will help to split up the tasks which must be undertaken into manageable projects. These can then be assigned to individuals, deadlines set and progress tracked using the template.

Remember – The GDPR comes into effect on the 25th of May 2018 so you should aim to have completed your workbook by then.

Action

Use **Template B** of your workbook to create your action plan for GDPR compliance. This can also be used for future reviews/audit, which we would recommend is done on at least an annual basis and in the event of a data protection breach. Staff will need to be trained as appropriate on the GDPR.

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

In order to comply with the GDPR, one thing you must be able to demonstrate is that you continually review and record the types of personal data you process and justify why you have a legal right to process it. This will need to be done before the 25th of May, and we recommend on at least an annual basis thereafter. You must be able to provide this information to the ICO if requested, which is likely if you ever encounter an information governance problem or report a breach of data protection.

Recording what data you process is only possible if you know what to look for, so we suggest that you familiarise yourself with some key definitions below before you start:

- The **Data Subject** is the person whom the data you hold relates to (e.g. a patient)
- **Personal Data** is any information relating to a data subject who can be identified directly or indirectly by that data. For example, a CHI number, name or address relates to a specific individual, and could be used to identify them. Likewise, a CCTV recording of a person would be classed as data which identifies an individual.
- **Special Category Data** is data about an individual which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, **information about health**, sex life, sexual orientation or trade union membership. This category also includes any biometric data e.g. fingerprints or DNA information. Paper prescriptions and the health records you store on your PMR therefore contain special category data, which demands stricter controls tat “standard” personal data. Again, CCTV recordings could be classified as special category data if, for example, they revealed an individual’s ethnic origin.
- **Information about health** covers almost everything we do in community pharmacies. Data which reveals anything about a person’s physical or mental health becomes special category data and may include information about services provided, medication history or diagnoses.
- **Processing** data can mean a number of things – collecting, recording, organising, adapting, structuring, storing, using and sharing/disclosure of personal data. So, when you take in a prescription you are processing data. When you use the information to dispense a medication, you are processing. When you discuss a patient with another healthcare professional, you are processing. If an email containing personal data arrives in your inbox you are already processing that data, as you are storing it within your system – even before you have read it.
- A **Data Controller** of personal data is the organisation which determines the purposes and means of processing personal data. All community pharmacy businesses are data controllers, processing personal data.
- A **Data Processor** is an external organisation which processes data on the behalf of a data controller, where the data controller dictates exactly how the data should be processed and for which reasons. For example, if you contract with a company who takes care of your payroll, they are a data processor.

You will need to consider all the places (filing systems) where you might have personal data, whether electronic or otherwise. For pharmacies, the main filing system will undoubtedly be your PMR, followed by paper prescription filing systems. You may also keep personal data in cloud storage services, on website servers or in hard-copy files for services that you provide amongst other locations. Remember to ask others in your business about where they hold data – there may be processing which you do not carry out yourself or are unaware of.

You must consider and record when and how you collect the personal data you use, how you store it and for how long and to whom you provide this information. Transfer of data overseas should also be recorded as well as details of your processors, and your security measures. Your findings must be recorded, for example in the workbook we have provided.

Although data needs to identify a data subject to be considered personal and therefore be covered by the GDPR, it does not have to do this directly. So, even if the data you process is partially anonymised (pseudonymised) but could identify a person if matched with other information at a later stage, it will still be in the scope of the GDPR and you should include this when recording the data which you process. The GDPR does not apply to completely anonymised data.

Action

Use **Template C** in your workbook to record the types of personal data, processing and filing systems you identify in your practice. We have pre-populated this template with types of personal data and processing activities which are common to all community pharmacy businesses, but you may have to make additional entries based upon your individual business practices (e.g. data collection from a website/app, direct marketing etc).

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

You must be able to demonstrate that your business has a legal basis for **each processing activity** that you undertake with personal data. The GDPR defines a number of reasons (legal bases) why an organisation might be "allowed" to process personal data, and your activities must satisfy one or more of these.

If you process special category data (as most pharmacies do), you must also satisfy one or more of a second set of conditions to demonstrate that you have a legal basis to undertake this processing. This is because special category data is by nature more sensitive information with a greater potential to cause harm if it is misused.

You can read more about this in our FAQ section (Part 3 of this pack) and on the ICO website to help you determine your legal basis for activities which we have not pre-populated.

Community Pharmacies' legal basis for most of our processing activities is that we have a **Legal Obligation** to process the data, or that it is processed for the performance of a **Contract** with the data subject. Much of what we process is special category data, and the condition that we satisfy to allow us to do so is that the processing is **necessary for the provision of health or social care treatment**, or the **management of health care systems and services**. We have attached these legal bases to the common processing activities we have pre-populated for you in Template C. However, these may not be the appropriate legal bases and conditions for all of your processing activities and you must ensure that you identify and record an appropriate justification for each type of processing activity.

Consent as a legal basis for processing personal data is often misunderstood, and therefore used inappropriately. If you make consent to data being processed as a precondition of a service it is probably not the correct legal basis for you. Consent should offer the data subject real choice and control – we will discuss this in more detail in the Consent section.

Action

We have identified the legal basis for all of the common datasets and processing activities and described these in **Template C** of your workbook. If you have identified any processing activities that your business undertakes, you should identify the legal basis (and conditions for special categories of data) for these activities and record it.

5. Make sure you process data in accordance with data protection principles

To comply with the GDPR, pharmacies must consistently process all data in accordance with the following principles:

- Data must be processed lawfully, fairly and in a transparent manner;
- Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." processed lawfully, fairly and in a transparent manner

Broadly, community pharmacies will be processing data in a manner which satisfies most of these principles. However, you are now legally obligated to demonstrate and document how you are doing this. This shows a move from a reactive duty to a proactive one, and will demonstrate accountability to the ICO if required.

Action

Template D of your workbook is designed to assist you as far as possible in recording the relevant information to demonstrate your compliance with these principles. Complete this in full and review on at least an annual basis or in the event of a data protection incident.

6. Review your agreements with Data Processors

You will need to identify any organisation that you engage to process data on your behalf (Data Processors). You must be satisfied that you are sending them only as much personal data as they need to carry out the processing that you have asked them to. You must also gain assurance that they will process that data you share with them in accordance with the GDPR, and will only keep that data for as long as it is needed before destroying it or returning it to you.

Processing by a processor must be underpinned by a contract or legislation, and will document the instructions from the Controller to the Processor about how the data may be used, thus helping both parties in demonstrating their GDPR compliance.

As a community pharmacy, you may well process data on behalf of another controller, so do not be surprised if you are asked to provide similar assurances to them in the near future. If you do act as a Data Processor, you must not engage another processor to help you (i.e. sub-contract) without prior approval/consent of the Data Controller for whom you process.

By carrying out these checks as a part of GDPR compliance, you are ensuring as far as possible that the rights of data subjects about whom you hold personal data are protected, and you will therefore minimise the risk of a data protection incident.

You may need to rely on the technical expertise of your suppliers, for example, your PMR supplier for assurances about the security of systems.

Action

Your existing contractual terms may already be sufficient to comply with GDPR requirements.

Template E of your workbook allows you to record your processors and provides a standard letter which you may wish to adapt and send to them to ask them to agree or confirm whether your contractual relationship includes what is necessary for compliance.

7. Obtain consent if you need to

If the only lawful basis which you can identify for a processing activity is the consent of the data subject, then you must make sure that your mechanisms for obtaining consent meet the GDPR requirements and you must also have a record of that individual's consent, even if it was given before GDPR comes into force on the 25th of May 2018.

Consent will not be the most appropriate legal basis for most processing undertaken in community pharmacies. However, if you are currently using systems or paperwork which collect consent, these can still be used until they are redesigned to reflect GDPR changes.

The most likely processing activity to require consent of the data subject is direct marketing.

Remember, consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. If the processing activity which you need consent for uses special category data (e.g. using health information to target marketing), you will need to obtain **Explicit Consent**, which is even more specific than standard consent. This must be confirmed in clear wording (e.g. I consent to <insert company> using my healthcare information to make automated decisions to target and send emails about their products and special offers).

If you do collect personal data for marketing purposes, we would strongly recommend that you read the ICO's *Guidance on consent* document.

Action

Template F of your workbook can be used to list any personal data for which you have identified Consent as being the legal basis for collecting and processing. It will also help you to ensure that you have GDPR-compliant consent mechanisms and that these are recorded and version controlled.

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

The first data protection principle requires that data must be processed lawfully, fairly and in a transparent manner. By identifying your legal basis for each processing activity you will satisfy the “lawfully” part of this sentence, but it is equally important that you demonstrate fairness and transparency.

In effect, you can do this by creating a clear, concise explanation of the types of processing you undertake and making it available to all potential data subjects. This should also include some information about the data subjects’ rights and is sometimes known as a **fair processing** or **privacy notice**.

When you collect information from a data subject you must provide the data subject with relevant information. This should be available on the pharmacy premises, for example, in a poster or the practice leaflet. You may wish to use a mixture of methods such as a simple sign which directs people to the practice leaflet. If appropriate, there should also be a privacy notice on the pharmacy’s website – but this is likely to contain different information relating to the data you capture from data subjects online.

You should bring your fair processing notice (Online or in pharmacy) to the attention of new customers, but the information in the notice need only be provided once to the data subject until it is changed.

If you begin a new processing activity with data which you originally collected for other purposes, you must provide further information about this activity to the data subjects.

The **fair processing notice** should include:

a) The pharmacy business’s name and contact details;
b) The DPO’s name and contact details; purposes and legal basis for processing (and state if the processing is based on ‘legitimate interests’, a legal/statutory requirement, or a contractual requirement);
c) If the information was obtained by consent, that consent may be withdrawn at any time;
d) For how long the data will be stored or how this time is calculated;
e) The right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject, as well as the right to data portability;
f) The right to object to processing – this must be brought to the data subject’s attention explicitly and separate to other information in certain cases (generally this will apply for pharmacy);
g) Whether there is any automated decision making and its significance (generally this will not apply to pharmacy);
h) The recipients or categories of recipients of the personal data;
i) Any relevant information relating to transfer to third countries; and
j) The right to lodge a complaint with the ICO

Action

Template G of your workbook is a draft fair processing notice which is likely to be appropriate for community pharmacies undertaking core NHS business activities. You should read this and if you undertake additional processing of data add information about this to the notice before using it. If you capture personal data on your website you will need to modify the fair processing notice as appropriate before using it online.

9. Ensure security but be ready for unintended data breaches

One of your most important duties as a data controller is to take appropriate technical and organisational measures to ensure that personal data is processed securely. This will include, as appropriate: encryption of data; adoption of data protection policies; timeous system backups; and reviewing both the physical and electronic security of your data. You should also make sure there is a process for regularly testing the effectiveness of the measures you have put in place.

Physical security measures may include (but are not limited to) ensuring that PMR screens are not visible to the public, access to areas of the premises where personal data is stored being restricted and privacy screens for mobile devices. Electronic security measures may include (but are not limited to) installation of robust anti-virus software, password protection of systems and encryption of devices.

Pharmacies will need to rely on appropriate experts to provide the relevant technical assurances, for example, their PMR suppliers and other system providers. In most cases, such systems will have an appropriate level of security already and you simply need to confirm this, and that your installation and use of the systems is appropriate.

A **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data for which you are responsible. In the case of a personal data breach, you must notify the ICO if it is likely to result in a risk to the rights and freedoms of a data subject. The ICO must be notified without undue delay, and no later than 72 hours after you first become aware of the breach. You must record all breaches internally, even if a breach is unlikely to risk the rights and freedoms of a data subject. The ICO can inspect these records at any point.

When notifying the ICO of a breach, you must describe: the nature and size of the breach, the likely consequences of the breach and; any measures you have taken to mitigate the consequences of the breach. If you become aware of any further information in relation to the breach once it has been reported, you must contact the ICO to update them.

Action

Insert into your workbook any communications with your system suppliers that will help you demonstrate technical security (e.g. PMR supplier's AVG specification).

Template H of your workbook includes some steps you may wish to take to assist you in assuring security and a table to keep a record of any personal data breaches.

10. Be ready for Data Subject rights requests

The GDPR strengthens and expands the rights of data subjects in relation to the data you hold about them. You will need to know when you might be required, for example, to delete a person's personal data and when this might be inappropriate.

The GDPR provides the following rights to data subjects, which you can read about in more depth on the ICO website:

- 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

Not every right will apply to all who process personal data, and some rights may only be exercised if processing has not been carried out in accordance with the law and GDPR principles. The right to be informed can be covered with an appropriate fair processing notice and associated procedures. The right of access (previously subject access requests) are now without charge to the data subject and the information must be provided within one calendar month.

You need to be able to provide a copy of any information you hold on a data subject, for example, in your PMR record, or be asked to correct, or add a note correcting, relevant information, whichever is more appropriate. Some information you must retain even if it is incorrect, if, for example, it records what was written on a prescription or what was dispensed. There will also be other laws which prevent rights being exercised – for example, the legal requirement to keep a CD register for two years past the last entry would overrule a data subject's wish to have a CD register entry deleted.

Generally, any personal data you collect by consent must be deleted if consent is subsequently withdrawn, with various exceptions including potential legal proceedings. You should seek advice if you receive a data subject request with which you are unfamiliar.

Action

In **Template I** of your workbook**,** we have set out some of the key rights of patients and customers whose personal details you hold. You should be ready to respond to these and other requests from data subjects where they seek to exercise their rights.

11. Design your processes with privacy in mind

The GDPR makes data protection by design a legal requirement. This means giving due regard to the data protection principles when you look at how you do things. For example, it may be possible and appropriate for your business to redact personal information when carrying out accounting activity to remove the risk of a data breach. This has been good practice for some time.

Individuals who you have identified as being responsible should advise on any new filing system (Electronic or otherwise) you intend to introduce or if you are making amendments to an existing system.

Action
Involve your Data Protection leads if you are designing a new filing system or making amendments to an existing system.

12. Carry out a Data Protection Impact Assessment where necessary

If you process special category (e.g. Health) data on a large scale, and are introducing or changing new technologies, practices or procedures, you should carry out a data protection impact assessment (DPIA).

As discussed earlier with regards to whether a DPO is required, it is not yet clear what “large scale” is intended to mean. However, it may be wise to complete an assessment if you are introducing significant changes as described above. This is likely to be helpful to the pharmacy, should assist patient confidence and avoids any possible argument about the legal technicalities.

This assessment should include a description of the processing activities and the purposes; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the privacy and related risks; and, the measures in place to address those risks, including security, to demonstrate that you comply. Where appropriate, the views of data subjects should be sought. If the risk of processing is high and you cannot identify measures to mitigate that risk, you must contact the ICO for guidance before initiating processing.

Action
A draft data protection impact assessment is included in your workbook as **Template J** for those who would require it.

Summary

Preparing for the new regulations may seem like an overwhelming task, but community pharmacy businesses are not starting from scratch. By doing the following, you should be able to demonstrate ongoing GDPR compliance:

- Read and understand this guidance
- Familiarise yourself with the ICO website
- Cascade relevant information to your team members as appropriate
- Complete the workbook which we have provided in full, identifying any actions which need to be taken and assigning them appropriate deadlines.
- Review the workbook regularly – we would suggest on an annual basis and in the event of a data protection breach.

Acknowledgements

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