Community Pharmacy
GDPR Working Party

The General Data Protection Regulation and associated legislation

Part 5: Getting to grips with GDPR (articles by PSNC's Gordon Hockey)

Published 18th May 2018

Community Pharmacy
GDPR Working Party

Contents

Introduction

This article has been written by Gordon Hockey, PSNC Director of Operations and Support, and is the first in a series of articles for contractors about the General Data Protection Regulation (GDPR) and the associated (currently draft) UK Data Protection Act 2018 (DPA 2018), which both come into force on 25th May 2018. The articles accompany the GDPR guidance and contractor workbook.

For more information and guidance on GDPR, please visit: psnc.org.uk/GDPR

1. Where do I start?

The bad news is that the GDPR has been described as one of the most complex pieces of regulation ever produced by the European Union; the good news is that the PSNC, NPA, CCA, AIMp, RPS, CPPE and CPW, along with various representatives from contractors, have already got together to sweat it out and prepare guidance and a workbook for you to complete. If you do, it will go a long way to helping you comply with the GDPR and associated legislation.

The GDPR and its associated legislation applies to the **processing** of personal data, e.g. names and addresses, including special category personal data, e.g. data concerning health. It concerns the personal data of living persons – we'll take that as read – primarily in filing systems. These are electronic or paper systems in which you can search people by set criteria, such as a name. Probably the single biggest consideration for community pharmacy is the processing of more than a billion prescription items annually and the associated electronic records held in Patient Medication Record (PMR) computer systems.

Before we go further, remember that while the GDPR is important, and it does change the way we consider data protection, it is **not** about pharmacy practice, life, the world and the universe!
There are two sets of rules that community pharmacies already comply with that I want to highlight because they interact with, but should not be confused with, the GDPR. These are:

1. consent or agreement to the activity in question – for example, patients must give consent to you administering a flu vaccination or agreement to you dispensing a prescription as a part of pharmacy practice; and
2. the common law duty of confidence (confidentiality) – patients can generally expect their health information not to be disclosed unless, for example, they consent to the disclosure (express or implied consent is acceptable here) or it is authorised or required by law or there is an overriding public interest.

There are some complexities around the interaction of these two with the GDPR work, but the key thing to remember is that while you generally won't be using patient consent as a lawful basis for processing their data under the GDPR, it will remain important in these two other areas so you must continue to seek consent for services and protect confidentiality as you do now.

It's sensible to appoint **one person to lead** on implementation of the GDPR. That person will bring it all together and make sure that not only is the Workbook completed, but that technical and procedural aspects of data protection are carried out in the community pharmacy and all relevant staff understand the GDPR to the extent required for their roles.

The bigger your business, the more likely it is that you'll need some help and guidance on the GDPR from somebody who has expert knowledge of it and understands your business. You may indeed be required to have such a person by the GDPR – a **Data Protection Officer (DPO)**. Guidance on the role of the DPO can be found here.

Whether all community pharmacy contractors will have to appoint a DPO is subject to debate, but if you do, you may need to share a DPO with other contractors, to keep costs to a minimum. The hope is that only **large-scale** community pharmacies will have to appoint a DPO. There is little guidance on what 'large-scale' means in practice, but what there is suggests that processing on the scale of a single

practitioner is not large-scale, but processing on the scale of a hospital is. It is not clear where community pharmacy fits into this and we are seeking to resolve this urgently.

2. Have a plan!

Once you've started to get to grips with GDPR (see *Part 1. Where do I start?*), it's important to have a plan and consider what needs to be done. The Community Pharmacy GDPR Working Party has developed a 13-step plan, followed by both the guidance and the workbook. The steps are set out in the form of a mnemonic – **DATAPROTECTED** – to help you to remember them, as follows:

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

If you follow this 13-step plan, this should assist you on your journey towards GDPR compliance.

Your plan you should also include **staff training**. Staff need to be trained appropriately to their roles and should understand the basics of data protection (knowledge they should have already) and be aware of the GDPR and some of its key issues for your pharmacy, for example:

- you have a lawful basis for processing data concerning health, a special category of personal data;
- you have a privacy notice and they need to bring this to the attention of new patients;
- data security is very important, and they are involved in this too (and exactly how);
- generally, subject access requests are dealt with without charge and within in one calendar month; and,
- there are new rules on dealing with data protection breaches and the Information Commissioner's Office (ICO) may need to be informed of a breach without undue delay and at least within 72 hours of you first becoming aware of it.

Your registration with the ICO also remains important and you will need to continue to pay a fee to the ICO after 25th May 2018 (there are some exemptions from this requirement).

This has the feeling of a revision plan, which is perhaps appropriate as we head towards the summer exams for many students.

3 and 4. Your lawful basis for processing personal data

Under the GDPR, anybody processing personal data must have a **lawful basis** for doing so. For special categories of personal data, including data concerning health, additional requirements are in place. The details of this are set out in Articles 6 and 9 of the GDPR.

Community pharmacies must be able to identify their lawful basis for processing personal data, and will need to follow two steps to do this:

Step 1 – Make sure you have a valid reason why you need to process personal data (relating to Article 6 of the GDPR); and,
Step 2 – If it is **data concerning health** (a special category of personal data), make sure that you are processing it only as permitted for the provision of healthcare or treatment (relating to Article 9 of the GDPR). Most of the personal data processed in community pharmacy will fall into this special category and, therefore, you will need to consider both Articles 6 and 9 of the GDPR.

The Community Pharmacy GDPR Working Party has done this for you and for data concerning health processed by community pharmacy it is fairly clear – Article 6(1)(e) and Article 9(1)(h).

For those interested in the detail, let's look at this more closely.

Step 1 – The basis or reason why you process the personal data is set out in Article 6(1) of the GDPR. There are several lawful reasons why you might be processing personal data and these can be condensed down to:

a. **Consent** (where explicit consent is given by the data subject)
b. **Contract** (where processing is necessary to fulfill a contractual obligation or as part of entering a contract)
c. **Legal Obligation** (where processing is necessary for compliance with a common law or statutory obligation)
d. **Vital interests** (where processing is necessary to protect someone's life)
e. **Public interest** (where processing is necessary to perform a specific task in the public interest that is set out in law)
f. **Legitimate interests** (where processing is necessary for the purpose of legitimate interests, but public authorities cannot rely on this)

The incoming Data Protection Act 2018 clarifies aspects of Article 6.

NHS Digital's Information Governance Alliance (IGA) advises that *'the most appropriate basis for lawful processing that is available to publicly funded and/or statutory health and social care organisations in the delivery for their function'* is 'public interest'.

There is an argument that the public interest lawful basis covers only the publicly funded functions of community pharmacy and not, for example, maintaining a list of patients for **home delivery purposes** (by a bricks and mortar pharmacy). However, I take a broader view that the overall purpose of community pharmacy is to perform a task in the public interest and that this has a sufficiently clear basis in law – meaning that all professional pharmacy activities are covered by the lawful basis of public interest (Article 6(1)(e)).

If that argument were accepted, an alternative would be to use legitimate interests as the lawful basis for such ancillary activites. This can be used by public authorities (which for these purposes community pharmacies are) when they are not carrying out official – NHS – activities. As a last resort you could use GDPR consent, but as the IGA observes: *'in many health and social care contexts obtaining GDPR-compliant consent (which is stricter than that required for confidentiality) may not be possible.'* (Remember, consent is important in other spheres, for example, confidentiality, see Part 1.)

Step 2 – The special categories of personal data include **data concerning health** (Article 9(1) of the GDPR), which is described as *'data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'*, for example, patients' prescription information.

The processing of special category data is prohibited unless one of the conditions listed in Article 9(2) applies. The four most relevant/quoted conditions are paraphrased below:

a. **Explicit consent** (where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes)
b. **Employment** (where processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the data controller's duties as an employer)
h. **Provision of health or social care treatment** (where processing is necessary as part of the data controller's role as part of a healthcare organisation, e.g. the provision of health or social care or treatment or the management of health or social care systems and services)
i. **Public health** (where processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices)

Article 9(2)(h) is the most relevant to the healthcare sector, and is likely to be the basis for pharmacies processing special categories of data. If processing is under this provision, an additional requirement that must be met. This is included in Paragraph 6 (Article 9 (3)) of the GDPR (and clarified by the incoming data protection act) and requires that a healthcare professional (such as a pharmacist or a pharmacy technician subject to registration and regulatory oversight e.g. as per the Pharmacy Order 2010), social work professional or a person with a duty of confidentiality under a legal provision, must be responsible for the processing of personal data for these purposes.

You may note that, rather confusingly, 'consent' is included in the first set of conditions and 'explicit consent' in the second. We will look at this in a later article (or see Step 7 in the guidance). Generally, GDPR consent is not applicable to the provision of healthcare, including pharmacy practice.

In conclusion, identifying your lawful basis for processing personal data can be complicated, but for data concerning health processed by community pharmacy it is fairly clear – Article 6(1)(e) and Article 9(1)(h).

5. Process according to data protection principles

Community pharmacy contractors, as data Controllers, must process personal data in accordance with the principles of the GDPR (Article 5 (1)), which, in brief, are:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. 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; and
6. 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.

Broadly, these are the same as the current data protection principles. What is different is the 'accountability principle' – that the data *'Controller shall be responsible for and be able to demonstrate compliance'* with these principles (Article 5(2)). This is the one of the fundamental shifts with the new legislation, **you must not only comply but show that you are complying**. Showing you comply has been good practice for a while; after 25th May 2018, it will be mandatory.

Completion of the GDPR Workbook is part of what you need to do to demonstrate compliance with the data protection principles. Equally important is that the Workbook is used to record data breaches and subject rights, or subject access requests and that data protection and security is a part of your ongoing work, as is compliance with any other legal requirement.

We said in the Guidance for Community Pharmacies: Completing the **Workbook for Community Pharmacy** will help you demonstrate you are complying with the data protection principles. This is referred to as the accountability principle and is part of the GDPR's shift from a reactive to proactive approach to data protection.

Having appropriate procedures, including the Workbook, is important. It will even more important if somebody complains about you. In the past, often a data Controller's response to a compliant was to apologise and assure the Information Commissioner's Office (ICO) that they would put in place data protection procedures to avoid a repeat. After 25th May 2018, simply offering to introduce procedures will be too late. They should have been there already, for you to demonstrate compliance with the accountability principle.

6. Review and check with your processors

The GDPR requires data Controllers to be more conscious and careful about giving personal data to others to process – their processors – and community pharmacy is no exception.

What is a Processor?

Processors are those who do exactly what you ask them to do with the personal data you send to them. They are not other data Controllers to which you pass information. So, for example, if you send payroll information to a third party which pays your staff, the third party is a processor of your information. If you send information to, for example, your bank, HMRC, NHS England or the NHS Business Services Authority (NHS BSA), these organisations are generally data Controllers. (Generally, you as a pharmacy are a data controller because you make the decisions about what, when and whether to process patient data.)

Who are my main Processors?

The main Processors for community pharmacies will be:

- your PMR supplier and the aggregator (usually by the PMR supplier) which together transfer prescription data from the community pharmacy to the NHS; and
- any organisation that provides data capture and reporting systems (such as PharmOutcomes, Sonar Informatics, Healthi or Webstar Health).

Reviewing arrangements with your Processors

Having identified your Processors, the question is whether the necessary GDPR safeguards are included in the relevant contract (or sometimes legal provision), which include:

1. Details of the processing that will be carried out on your behalf;
2. The Processor will ensure the security of the personal data;
3. The Processor will only act on the written instructions of the Controller; and
4. The Processor will assist you as the Controller to fulfil your obligations, for example, in relation to the security of the data and data breaches.

Points 1 and 2 may be clear already in your contractual arrangements; points 3 and 4 may be clarified in the standard terms of business or require clarification in a revised contract.

A good starting point is to see what information the Processor has on its website. You must be realistic with the extent to which you can influence larger businesses that process personal data for you. Generally, you will be subject to their terms and conditions including the GDPR assurances you need, which should be updated before 25th May 2018 or soon afterwards.

7. Consent

Consent is a particular problem area given the number of questions we have had about it, so let's try to clarify the position.

Perhaps the three things to remember are that (1) generally, for the professional activities of a community pharmacy you will **not** be using GDPR consent, (2) consent remains important to pharmacy practice, and that (3) GDPR consent will be important to any direct marketing. Exploring each one:

Why is GDPR consent generally not relevant to professional activities of community pharmacy?
There are three main reasons why GDPR consent is not usually relevant to pharmacy professional practice:

1. There are other options for lawful processing such as contract, legal obligation, legitimate interests or vital interests, and one lawful basis should cover almost everything – performance of a duty in the public interest.
2. GDPR consent may not be appropriate to the processing of healthcare information where consent to processing cannot always be withdrawn and where some patients may not be able to give consent.
3. Processing of health data (a special category of personal data) is more appropriately processed for the purposes of treatment and care, public health or the management of the health service, under the responsibility of an appropriate person such as a pharmacist.

The table below describes pharmacy services and the applicable lawful basis (as previously described in part 3 of this series).

Pharmacy services	**Lawful basis (Article 6)**	**Lawful basis / Condition for processing special category personal data (Article 9)**
Dispensing prescriptions	Performance of a duty in the public interest	Treatment of patients and management of a healthcare system
Flu vaccination service	Performance of a duty in the public interest	Treatment of patients and management of a healthcare system
Home delivery service (free or paid)	Performance of a duty in the public interest (you could argue this comes under legitimate interests)	Treatment of patients
Summary Care Records	Performance of a duty in the public interest	Treatment of patients and management of a healthcare system
Patient nominations	Performance of a duty in the public interest;	Treatment of patients and management of a healthcare system

What do you mean by consent remains important to pharmacy practice?
Consent remains important in terms of the **activity** or **confidentiality**.

Consent for activity is common sense. You need a patient's consent to administer a flu vaccination. It is patients who chooses or should choose which pharmacy dispenses their prescriptions. A patient must agree for you to delivery medicines to their home. A patient must nominate a pharmacy for EPS in accordance with current rules and guidance.

Confidentiality (the common law duty of confidence) is integral to pharmacy practice. Generally, you must not disclose confidential information, but you may do so with the express or implied consent of the patient, or as required by law, or because of an overriding public interest. It is these provisions which might allow you to disclose information to a GP or hospital in an emergency (you do not have to have your lawful basis of processing under GDPR as 'vital interests' to do so); or allow you to provide information to the police if they are investigating a serious crime and wish to identify a person who visited your pharmacy at a particular time; or call out the name of a patient waiting to collect a dispensed medicine (on the basis of implied consent).

When might GDPR consent be relevant?
This could be for direct marketing or a pharmacy store card and you will need to seek your own advice on this aspect of your business. There is some information on GDPR consent in the guidance and perhaps key points to remember are that:

1. Pre-ticked boxes will **not** provide GDPR consent;
2. GDPR consent must be freely given, unbundled with other acceptances and recorded;
3. If you do not have GDPR consent and require it, this must be obtained before 25th May 2018;
4. If you are processing health data under GDPR consent that consent must be explicit – see the ICO information for more detail; and
5. You **must not** use information provided for NHS or healthcare purposes to seek to obtain GDPR consent for other purposes such as direct marketing.

8 and 11. Privacy Notice and data subject rights

The Privacy Notice and the array of data subject rights in the GDPR seek to address the power imbalance between all of us as private citizens and those, including community pharmacy, which hold our personal data.

Community pharmacy should embrace these provisions. The way in which community pharmacy uses personal data is already transparent and data subjects' rights, while potentially onerous, generally are exercised rarely when patients or other data subjects have confidence in your handling of their data. The Privacy Notice is important to building that confidence.

Key points about the Privacy Notice are:

- Ensure the Privacy Notice includes all the necessary information and make it clear and simple.
- The name and contact details of your Data Protection Officer must be included in the Privacy Notice.
- A model Privacy Notice is included in the Community Pharmacy GDPR Workbook.
- While it is the contractor (as the data Controller) that must have a Privacy Notice, this should be available at each community pharmacy.
- The Privacy Notice should be displayed in each community pharmacy and/or in the practice leaflet and/or on the pharmacy website.
- You should make new patients aware of the Privacy Notice (recognising that a patient who is new to your community pharmacy may well have seen a similar Privacy Notice at another one).
- Be ready and willing to revise and reissue your Privacy Notice if necessary to improve it for your patients and other data subjects.

Generally, community pharmacy receives personal data direct from the data subject, for example, when a patient 'presents' a prescription (hard copy or electronic prescription) or nominates a pharmacy (electronic prescription). The obligation is then to provide the Privacy Notice at the time you collect a patient's personal data – i.e. when you receive or download the prescription.

If you obtain personal data from other sources, you must provide the patient or other data subject with your privacy information within a reasonable period of obtaining the data and no later than one month after.

The two data subject rights of particular relevance to community pharmacy are the **right of access** or **subject access** (this was the subject access request) and the **right to object**. Relevant staff should be aware of both. Key points on the subject access request are:

- The request can be verbally or in writing and to any member of staff.
- You may need to ask the person making the request for ID or establish to your satisfaction that the person has the authority to make the request on behalf of another person.
- You have one calendar month to respond (but in my experience try to do it as quickly as practicable) which can be extended in certain cases.
- In most circumstances you may not charge a fee (but you can charge a fee if the request is manifestly unfound or excessive or reasonable administrative fee if additional copies of the information are requested).
- You are providing information not actual or original documents (although in some cases it is just easier to provide a copy of a document).
- You must confirm if you process (whether you have) the data and if you do, provide it.

- Data subjects have a right of access to the information provided in your Privacy Notice, so if for example, there is a request for your lawful basis of processing, it may be more helpful to provide a copy of the Notice.
- If a data subject makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.
- You should not provide the personal data of another person in response to a right of access.
- In the case of a child's data, the child's request may be made by a parent or guardian or, if the child understands his or her rights and how to interpret the information, may be accepted from the child. There is additional guidance on children and the GDPR provided by the Information Commissioner's Office (ICO).
- The information requested must be provided in concise and intelligible form, using clear and plain language, which means you may need to explain any coded or abbreviated information.
- The right to object must be stated on the Privacy Notice if the lawful processing (see *Stage 1 – Where do I start?*) is 'performance of a duty in the public interest'. If someone objects, you will need to demonstrate 'compelling, legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject'. In most cases you will need to retain the data in accordance with your retention policy. The National Data Opt-Out Programme is an example of the right to object and the extent to which you can accept an objection – if you use patients data for research and planning purposes (see our webpage for more information).

9 and 10. Data security and data breaches

Data security was important before the GDPR and it remains important after its introduction. Perhaps the key difference is that you need to think about this and demonstrate compliance proactively before any problems occur. Up until now, you might have 'got away' with just doing what you've done for a while and promising to improve if there was a problem.

In the GDPR Workbook, we list many of the existing templates you may have, or you may have equivalent practices / documents through which you will seek to ensure the physical, electronic and human security of personal data.

An example of each might be:

Security type	Practical example in community pharmacy
Physical	Preventing unauthorised access to the pharmacy premises by ensuring that it is locked as required.
Electronic	Seeking appropriate advice to ensure that your PMR database and use of the Electronic Prescription Service (EPS) is secure and has the necessary ongoing support from your PMR supplier or others. Pharmacy teams should also only be using NHSmail accounts to send health data about a patient to another healthcare professional.
Human	Training staff in confidentiality requirements and ensuring they are bound by them (either professionally or by contract).

The GDPR is making everybody think about how they process personal data, including how they transfer personal data to others and this should not stop after 25th May 2018.

As regards personal data breaches, the first point is to seek to avoid them through good practice, procedure and the right culture in the organisation; and if they happen deal with them quickly and sensibly. In terms of the GDPR, there are three levels:

1. Any personal data breach – record all data breaches in the Workbook, however minor (and learn from them).
2. When it is 'likely to result in a risk to the rights and freedoms of the patient or other data subject – record the data breach and notify the Information Commissioner's Office (ICO). What needs to be reported may change over time. Everybody will probably be cautious at the start and over report data breaches, the real danger here being that the ICO becomes overloaded with information and misses the real problems.
3. Record the data breach, notify the ICO and tell the patient or other data subject (although as pharmacists are subject to a duty of candour, they may decide to tell the patient about something before this stage).

As a rough guide, because each data breach must be considered against its own facts, the health data disclosed or potentially disclose, where and when:

Level of data breach	Practical example in community pharmacy
1. Record the breach	If you send a patient's health data to the wrong GP or similar controlled environment when confidentiality can be assured as part of professional requirements; or if a patient's dispensed medicine has another patient's repeat slip but the error is corrected quickly in the pharmacy or soon

	afterwards (subject always to the circumstances and not, for example, if particularly sensitive patient data has been disclosed to somebody who knows the patient).
2. Record the breach and notify the ICO	If the prescription bundle is lost on route to the NHS Business Services Authority (NHS BSA) and it is not thought to be lost in the courier's warehouse.
3. Record the breach, notify the ICO and tell the patient about the breach	If a prescription collected at the GP practice has been lost on the way back to the pharmacy and could be picked up by anybody locally.

12 and 13. Data protection by privacy and design and the Impact Assessment

Data protection by design and default is all about processing personal data more safely and more securely, with the minimum risk to the individuals concerned, as well as about making sure this is the thinking for any new project.

Let's take pseudonymisation as case in point. Pseudonymisation is suggested as an appropriate technical measure to reduce the risks for data subjects and it is likely that you are already doing this to some extent. For example, those dealing with your accounts may not see patient details. Also, if you capture and submit records through a Local Pharmaceutical Committee (LPC) to a Local Authority or other commissioner, it is likely that the patient records are pseudonymised as they are processed by the LPC.

That's all about improvement, but what about your current processing? The GDPR requires that organisations undertake a Data Protection Impact Assessment (DPIA) where their processing presents a high risk to the rights and freedoms of individuals. **Template M of the GDPR Workbook** helps you consider which pharmacy activities may require a DPIA, and any assessment should be carried out with the help of your Data Protection Officer (DPO). In some cases, you must carry out a DPIA and examples of such scenarios are highlighted in Template M.

Community pharmacies processing data concerning health on a large-scale must carry out a DPIA. However, the interpretation of large-scale is unclear. Accordingly, we recommend that **all** contractors complete a DPIA as part of their preparations for GDPR compliance and a model DPIA is attached below to be used in addition to the GDPR Workbook.

PSNC's model Data Protection Impact Assessment (DPIA) for community pharmacy contractors