The General Data Protection Regulation and associated legislation

Part 1: Guidance for Community Pharmacy

Version 1: 25th March 2018

Community Pharmacy
GDPR Working Party

Introduction

The General Data Protection Regulation and, when enacted, the Data Protection Act 2018 (we refer to the two together as the 'GDPR'), will bring in a new approach to data protection. The two pieces of legislation are intended to provide an improved and more comprehensive framework for protecting living individuals' personal data; and you will need to take steps before the 25th May 2018 to comply with the new requirements.

This may sound worrying, but the GDPR brings evolution rather than revolution and much of what becomes mandatory for the first time has been good practice for many years. This is particularly so for community pharmacy: patient confidentiality is a professional obligation and NHS pharmacies are already subject to Information Governance (IG) requirements. We have explained what this all means for you and provided guidance on how to comply with the new requirements in our four information booklets: **Guidance for Community Pharmacy** (Part 1), **Guidance for Community Pharmacy (shorter version)** (Part 2), **Workbook for Community Pharmacy** (Part 3) and **FAQs for Community Pharmacy** (Part 4).

We suggest you read the **Guidance for Community Pharmacy** and then complete the **Workbook for Community Pharmacy**, adding relevant information about your pharmacy and amending it, as appropriate. There are 13 steps to follow to assist you to comply with the GDPR, which we have listed under the mnemonic **DATAPROTECTED**. The **Guide for the Community Pharmacy (short version)** may be used for staff training.

Everybody is getting to grips with the GDPR and there is much to be clarified both before and after the 25th May 2018. Therefore, this guidance should be considered a starting point and we will update it as issues are clarified. We are also happy to accept questions, which may be sent to any of the working party's member organisations and selected questions with answers will be added to the **FAQs for Community Pharmacy**. If you are worried about getting everything done in time, two quotes from the Information Commissioner Elizabeth Denham's blog may reassure you:

"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".

Community Pharmacy GDPR Working Party

Organisations involved

DATA PROTECTED – this mnemonic will help you to remember the 13 steps, which will assist you in 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.

You, as the owner of the pharmacy business - in practical terms this is likely to mean the directors and officers (senior staff) of the business - have overall responsibility for data protection in your pharmacy or pharmacies and we suggest you consider who will lead your work to comply with the GDPR and whether you need to appoint a DPO.

The person who leads your efforts to comply with the GDPR could be you as an individual owner, a director of the business, your superintendent pharmacist (if applicable), your IG lead (or Senior Information Risk Owner (SIRO)), or another appropriate person employed or engaged by the pharmacy business who understands pharmacy, the business and associated professional and legal responsibilities. In smaller pharmacy businesses, one person may fulfil all these roles or descriptions.

You may also need to appoint a DPO. The DPO is a formal role for somebody with expertise in data protection law and the GDPR, who can give you advice and monitor your compliance. The Information Commissioner's Office (ICO) confirms that the DPO can be an existing employee provided the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interest. Two or more pharmacy businesses can share a DPO. More information on the full role of the DPO can be found in '*Guidance on the role of the Data Protection Officer*' by NHS Digital's Information Governance Alliance (IGA) and in our FAQs.

The draft Data Protection Act deems all community pharmacies to be "public authorities", which means that they must have a DPO. We consider that this would be inappropriate for **smaller** pharmacy businesses, where the costs of engaging a DPO are likely to be disproportionate to the benefits; and accordingly, we are lobbying for an amendment to the draft legislation to exempt smaller pharmacies from this requirement; **smaller** is not yet defined. 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 what there is suggests that processing by an individual practitioner is not large-scale, whereas processing by a hospital is large-scale.

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.

We suggest you use the 13 steps – **DATA PROTECTED** – outlined in these information booklets and complete the **Workbook for Community Pharmacy** (Part 3) as your action plan, to assist your compliance with the GDPR – by 25th May 2018. The Workbook is partially completed for you and should build on your existing IG work. Your action plan also needs to include continuing to pay an annual fee to the ICO. The fee will depend on the number of staff you have if you are deemed to be a public authority; and the number of staff you have and your annual turnover if not. It's anticipated that the fee should be no more than £60.

Data protection and confidentiality of patient data are the responsibility of the pharmacy team, not just the business, so your plan will also need to include the provision of training on the GDPR to members of the pharmacy team, appropriate to their roles and responsibilities. This will help your staff respond to questions and queries from patients about the GDPR. The **Guidance for Community Pharmacy (shorter form)** may assist your staff training.

Before you get started you also need to understand some of the terms used in the GDPR, so you know what you are looking for when you assess your pharmacy's use of personal data. In brief, this is as follows: The GDPR applies to the **processing** (obtaining, storing or passing on) of information (**personal data** such as names, addresses, NHS number and health information) that relates to identified or identifiable living individuals (a **data subject**) by manual or automated means, which forms part of a paper or electronic **filing system** (searchable according to certain criteria e.g. a name) and in some cases manual unstructured files (see Step 4, note 2). The pharmacy business is generally the **data controller** (the person who has overall responsibility for the processing) and may have **processors** that process its data on its behalf (e.g. the patient medication record (PMR) supplier). Most of the data processed by a pharmacy is of a **special category, data concerning health** (which includes prescription and other health information), so additional controls apply. The GDPR does not apply to anonymous data.

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.

You should consider all the filing systems you have that include personal data and include these in your consideration of GDPR; this includes paper and electronic filing systems. Lists, spreadsheets, databases or folders could all be filing systems. The most significant filing system is your PMR computer system. Ask others in your pharmacy business if they hold systems. All these systems (and any other manual unstructured personal data – see Step 4, note 2) need to be included. You also need to consider 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.

Remember that the meaning of personal data under the GDPR includes data from which natural persons (i.e. individuals) can be identified indirectly. This means that if the information you process can be matched at a later stage with other information (that you hold or somebody else holds) or linked to other data to identify someone, it is personal data, even though you cannot currently see to whom it relates. An example would be if someone were to hold health data about people identifiable only by their NHS number; this could be matched to individuals with other data (i.e. a list of NHS numbers and names). The GDPR refers to this data as **pseudonymised** data.

You then need to keep a record of your processing activity and review what you do on an ongoing basis - we suggest annually when you complete the IG Toolkit. This is not a record of everything you process, but of the types of personal data you process and other relevant information. You must provide this record to the ICO, if requested, and are likely to be asked to provide it if there is a personal data breach (see step 10).

The IG Toolkit is being updated to include the GDPR requirements and by 31st March 2019, you will have to complete the updated Toolkit. The work you do now will help.

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.

To comply with the GDPR, you must have a lawful basis for processing personal data, for example, when you dispense prescriptions, and this must be recorded. Each type of processing must be recorded separately, and we have included several suggestions in **Template C.**

In addition to having a lawful basis for any processing of personal data, there are safeguards in place for the processing of special categories of personal data, such as data concerning health. This means that in practice, for much of the data processed in pharmacies, there will be a **two-stage** process: the first stage giving the lawful basis as applied to all personal data (Article 6 of the GDPR), and the second because you are processing a special category of personal data, data concerning health (Article 9).

First stage: Generally, pharmacies have a lawful basis for processing personal data because it is necessary '**for the performance of a task carried out in the public interest**'. In some circumstances, pharmacies could also say that the processing is necessary for 'compliance with a legal obligation' (NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013 – the Terms of Service), or 'for the performance of a contract' (locally commissioned services) or 'to protect the vital interests of the data subject' (emergencies). The lawful basis for processing must be recorded.

Second stage: Special categories of personal data, including data concerning health, may be processed only for reasons specified in Article 9 of the GDPR. In the case of pharmacy, the reasons are generally for '**the provision of health care or treatment**' or '**the management of health care systems or services or social care systems or services**' or '**necessary for reasons**

of public health in the area of public health'. When processed for these reasons, 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.

The Information Governance Alliance recommend that the lawful basis for employers processing employee data is '**for the performance of a task carried out in the public interest**'. It could also be argued that employee information may be processed for the performance of the employment contract or to comply with legal obligations. Employee consent to processing the data is not required as the employer must comply with tax and National Insurance obligations.

Note 1: Although consent (under the GDPR) is not needed to process patient data for health purposes, patients still need to consent (as part of pharmacy practice and service specifications) to any treatment provided, such as a flu vaccination, or any other pharmaceutical service, such as a Medicines Use Review (MUR). Patients also need to agree to having prescriptions dispensed, for example, by nominating the pharmacy for electronic prescriptions or presenting a paper prescription.

Note 2: (relating to Step 2 and Step 3) Manual unstructured data includes paper records that are not structured according to specific criteria, such as a data subject's name. These are subject to limited aspects of the GDPR, for example, they should be accurate and kept up to date, and data subjects have a right of access if they can describe the data and the data controller can comply with the request within the cost limits set by the Freedom of Information Act. Manual unstructured data might include notes of telephone messages from General Practitioners that relate to patients, recorded in a diary against the date of the call.

Note 3: The common law duty of confidence (confidentiality) continues to apply to healthcare practice and the courts have recognised three broad circumstances under which confidential information may be disclosed: consent – whether express or implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected); authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings; and overriding public interest, for example where a patient is contagious or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality.

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.

All personal data must be processed in accordance with the data protection principles, which are, in brief:

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."

You should be processing personal data in accordance with these principles already, but now you must be able to demonstrate and document this. You can do this through your policies, procedures and practices, and by recording appropriate information about your processing activities and data retention policies. 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.

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.

As a data controller for personal data that you obtain and store (e.g. PMR system records) you must identify your processors – those who process personal data for you (in this case, the PMR supplier) – and ensure that they provide you with sufficient assurances, as required under the GDPR. Other processors you have may be systems such as PharmOutcomes, payroll systems or any third party transferring prescription bundles to the NHS Business Services Authority (NHS BSA).

These assurances are usually in your contract and include, for example, the documented instructions from you, as the data controller, about how the personal data may be processed and how the processor will assist you to comply with your responsibilities under the GDPR.

You should be able to rely on your processors to ensure they give you appropriate assurances, in your contracts, but you need to check this.

Processors must not engage another person to process personal data without your prior specific approval or general written authorisation. In the event of a data breach, processors must notify you without undue delay upon becoming aware of the breach.

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.

'Consent' of the data subject under the GDPR means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent gained by pre-ticked consent boxes is not valid consent under the GDPR.

If you process data based on consent, you must ensure that the consent given is compliant with the GDPR and that you have a record of the consent. If you are missing either you must obtain such GDPR compliant consent before 25th May 2018. If you carry out direct marketing, this is likely to be by consent and you should read the *ICO's guidance on consent*.

If you want to use data concerning health for purposes that are not described in step 4, you must obtain the **explicit consent** of the patient, or have another reason for processing it listed in Article 9 of the GDPR, because such data is a special category of data.

Explicit consent is intended to be more specific than 'consent', and must be confirmed in words, rather than by any other positive action i.e. the person giving consent must signal agreement to an explicit statement in words such as 'I consent to emails about your products and special offers' (followed by a tick box to be completed, or not, as the case may be).

Current NHS systems sometimes use consent as the lawful means of processing and this is likely to continue until they are redesigned or otherwise updated.

Generally, community pharmacies will not need to seek consent or explicit consent to process personal data, because they already have a lawful basis for processing the data, although the concept of consent in terms of pharmacy practice will remain important (see step 4).

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.

A key principle of the GDPR is the provision of concise, transparent and intelligible information to data subjects about the processing of their personal information and their rights – sometimes called the **privacy notice**.

When you collect personal data from a data subject, you should provide them with a privacy notice. This should be available on the pharmacy premises which patients access, for example, in a poster or the practice leaflet, and, if appropriate, on the pharmacy website (this is likely to be different to the privacy notice relating to the website only) and you should draw the attention of new customers to the Privacy Notice.

The information in the privacy notice needs to be provided only once to the data subject.

In brief, the **privacy notice** should include:

a) the pharmacy business's name and contact details;
b) the DPO's name and contact details (if applicable);
c) purposes and legal basis for processing;
d) if the information was obtained by consent, that consent may be withdrawn at any time;
e) for how long the data will be stored or how this time is calculated;
f) the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject (where applicable);
g) the right to object to processing – this must be brought to the data subject's attention explicitly and separately to other information in certain cases (generally this will apply for pharmacy);

h) whether there is any automated decision-making and its significance (generally this will not apply to pharmacy);
i) the recipients or categories of recipients of the personal data;
j) any relevant information relating to transfer to third countries; and
k) the right to make a complaint to the ICO.

You may wish to have a layered approach to Privacy Notices so that increasing amounts of information are available about the way you process personal data.

It may be helpful to refer to the National Data Opt-Out in your Privacy Notice (see step 11).

There are further requirements if information is processed without the knowledge of the data subject; and if there is any further processing by the data controller, other than that for which the personal data was collected, further information must be provided to the data subjects, as appropriate.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) set out additional obligations in relation to electronic communications, for example, the use of cookies or similar technologies by any website you have.

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.

The GDPR requires data controllers to take appropriate technical and organisational measures, and adopt appropriate policies, to ensure personal data is processed securely. Such steps should include as appropriate: encryption of data; confidentiality and integrity of the systems used; backups made in a timely manner; and a process for regularly testing and evaluating the effectiveness of the security.

You may wish to consider such risks in relation to physical security (for example, the security of the pharmacy premises), electronic security (for example, computer systems and e-mails) and human security (including, for example, staff and security of Smartcards).

You should have existing policies on data security. However, you should check these to ensure that you have sufficient assurances from experts or suppliers, particularly on electronic security, to ensure your connection to and use of the internet and electronic NHS systems, does not compromise the security of personal data you process.

Additional staff training may be required to ensure the security of personal data and patient confidentiality in the pharmacy.

You may find that data you previously considered to be 'anonymised' and, therefore, not personal data (because the patient's name is removed), is now considered to be personal data and subject to the GDPR, because a patient can be identified using a separate key held by you or somebody else. A key system could be a patient's NHS number, or part of the NHS number. Such data is called pseudonymised personal data.

You may also want to consider whether personal data you process should be pseudonymised, to avoid unnecessary disclosure of personal data.

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.

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 transmitted, stored or otherwise processed.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The pharmacy business should have policies or procedures in place for personal data breaches.

If a personal data breach is **unlikely** to result in a risk to the **rights and freedoms** of a living person, for instance, if the data has been misplaced in a controlled environment such as the pharmacy premises, you do **not** need to notify the ICO. If a personal data breach is **likely** to result in a risk to the rights and freedoms of a natural person, for instance loss of a prescription bundle in a public place, you do need **to notify** the ICO. Notifying the ICO must be done without undue delay, and no later than 72 hours after you first **become aware** of the breach.

When you can be said to have **become aware** of a data breach is sometimes straightforward, for example, if somebody contacts you to say he or she has accidentally received a patient's personal data. In other cases, it will be less clear until you have started to investigate the incident. Any notifiable breach should be reported to the ICO when there is a reasonable degree of certainty that a breach has occurred.

Any notification to the ICO must describe the nature of the breach, such as numbers of data subjects or records and what was lost e.g. a prescription bundle; the name and contact details of the DPO; the likely consequences of the breach and measures you have taken to mitigate it. Where you cannot provide the information immediately, you may provide it later, again without undue delay.

You must document any data breaches, even if they are not reported to the ICO. The ICO may inspect your records to verify you are keeping such records.

If there is a **high risk** to the rights and freedoms of the data subject, you must inform them of the breach without delay, the likely consequences of the breach, the measures you are taking to address the breach and mitigate possible adverse effects, and the name and contact details of your DPO. This threshold is higher than the threshold for notifying the ICO, so there may be times when you notify the ICO but do not notify the data subject. If the ICO considers you should inform the data subject of the breach it can compel you to do so.

As with any security incident, you should reflect and learn from it and revise procedures and practices accordingly, to reduce the likelihood of repetition in future.

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.

The GDPR gives data subjects a number of rights of access and control over their personal data, so you will need to know when they might apply, for example, when to delete a person's personal data and when this would be inappropriate.

The GDPR provides the following rights for individuals: the right to be informed (Privacy Notice); the right of access; the right to rectification; the right to erasure (not usually applicable); the right to restrict processing; the right to data portability (not usually applicable); the right to object; and rights in relation to automated decision-making and profiling (not usually applicable).

The right of access (previously subject access requests) is now without charge to the data subject and the information must be provided within one calendar month of receiving the request for access. Generally, the right to rectification – correction - will not mean changing the record of medicines dispensed or other health data, but may, for example, mean correcting a name or address or adding a note of explanation to the record. You should identify those members of staff who may correct a record if requested to do so by a patient.

The right to object is particularly relevant to pharmacy where lawful processing is based on the 'public interest' provision. If someone objects to you processing his or her data, you will need to demonstrate 'compelling, legitimate grounds for [either] the processing which overrides the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims'. The National Data Opt-Out Programme will be an example of the right to object and is being introduced so that patients can ensure their personal data is not used for research and planning purposes.

You are also subject to professional obligations concerning confidentiality that are broader than the GDPR, for example, generally, patient information remains confidential even when the patient is deceased. Generally, any personal data you collect by consent must not be processed if consent is subsequently withdrawn, with various exceptions including potential legal proceedings. You should seek advice if you receive a request with which you are unfamiliar.

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.

The ICO already encourages organisations to ensure that privacy and data protection are key considerations in the early stages of any project, and then throughout its lifecycle. For example, when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

The GDPR makes data protection by design and default a legal requirement, indicating that you need to implement technical and organisational measures to ensure you only process personal data necessary for the task. Decisions about what is necessary should take into account what you are doing with the data, how long it is being stored, the accessibility required, and the risks involved given the nature and scope of the data.

Pseudonymisation (see step 3) is suggested as an appropriate technical and organisational 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 collected and submitted by the LPC.

Your DPO (if applicable) and others involved in IG should advise and consider privacy by design and default on an ongoing basis and with any new filing system you intend to introduce, such as your PMR system.

When NHS services are developed, for example, phase 4 of the Electronic Prescription Service (EPS), we would expect the NHS to consider privacy by design and default and carry out a Data Protection Impact Assessment (see step 13).

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.

Data controllers introducing new technologies or where processing is likely to result in a **high risk** to the 'rights and freedoms of individuals' must carry out a DPIA.

High risk processing includes large-scale processing of special categories of personal data, such as healthcare data, and so includes larger community pharmacy businesses. The ICO will be introducing updated guidance on DPIAs soon, but it is suggested that for smaller community pharmacies, a DPIA is not required for current routine provision of NHS pharmaceutical services.

The introduction of new technologies is high-risk, so any pharmacy introducing, for example, a dispensing robot, is likely to have to carry out a DPIA. In certain circumstances, data controllers must consult with the ICO about the DPIA.

Data controllers do not have to complete a DPIA where the processing is the result of legal obligations (for example, the NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013) or the performance of a task in the public interest and a DPIA was carried out (or its equivalent before 25th May 2018). Arguably this applies to the processing of prescriptions for the NHS.

A DPIA should include a description of the processing operations 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. If you have a DPO, his or her advice should be sought on a DPIA. Where appropriate, the views of data subjects, including patients, should be sought.

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 processes: the 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