Community Pharmacy Scotland

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

Part 4: Frequently Asked Questions

Version 2: May 2018

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

Community Pharmacy GDPR Working Party

Contents

Introduction

1. What is the GDPR and why is 25 May 2018 important?

The General Data Protection Regulation (GDPR) is European legislation that will be directly effective in the UK from 25 May 2018. It will be accompanied by UK-specific legislation, a new Data Protection Act, which will complement and clarify aspects of the GDPR. It will continue to apply after Brexit.

While the GDPR will bring changes to the way in which data protection is managed, it is more **evolution than revolution,** and is designed to both protect the rights of individuals and make clear the responsibilities of those who process data. It makes mandatory what up until now has been considered good or best practice. The basic principles of processing personal data remain broadly the same as our previous Data Protection Act, although the meaning of personal data is broadened, which may mean that some information that was previously not considered to be personal data now is.

Pharmacies must comply with information governance requirements already so no-one will be starting from scratch, though some will have more to do than others to be ready for the 25th of May.

2. What is personal data and what are the main terms I need to know?

Key aspects of the GDPR to understand are:

Personal data – includes any information relating to a person (the data subject) who can be identified directly or indirectly (for example, by a CHI number).

The GDPR applies to the processing of **personal data** (which may be by automated means) which forms part of a **filing system** or is intended to form a part of a filing system.

A **filing system** means anywhere you store data – this could be on paper or electronic in nature. So, a pharmacy company's main filing system for patients will be its PMR, which may be in each pharmacy or one system spread across many pharmacies.

Processing is any action related to personal data – right from collecting and storing to analysing and passing on to someone else.

The **controller** of the personal data makes decisions about what data is used, the purposes for using data and how processing of personal data is undertaken. There can be joint controllers for certain purposes. The pharmacy company is a controller, processing personal data.

A **processor** is somebody external to the pharmacy who processes personal data on your behalf, who you instruct exactly how to process the personal data. One example might be a payroll processing company.

The meaning of personal data is now broader and includes data from which people 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) to identify a natural person, it is personal data even though you cannot see to whom it relates. The GDPR refers to this data as **pseudonymised data** – personal data that can no longer be linked to a person without the use of additional information. **Pseudonymisation** of personal data is encouraged in appropriate circumstances where those processing some of the data do not to see all of it, for example, removing patient details for pharmacy accounting purposes.

3. Does the GDPR apply to all personal data?

No. The GDPR applies to the processing of **personal data** (which may be by automated means) which forms part of a **filing system** or is intended to form a part of a filing system. (see the means of these terms in the answer to question 2).

However, for the average community pharmacy, the GDPR will apply to all the personal data you come across in the course of your work.

The GDPR does not apply to the processing of personal data in the course of purely personal or household activities.

4. Who's responsible for GDPR and what needs to be done?

Generally, the legal owner of the pharmacy – e.g. the contractor – will be the person responsible for the organisation's compliance with the GDPR. Responsibility for compliance with GDPR cannot be delegated to any one person in the organisation, but one or more persons may be asked to lead one or more projects associated with GDPR and each person will be accountable for their actions. In GDPR terms this person is the data controller. The data controller also has some responsibility for any other person processing personal data on its behalf (a data processor).

The term 'accountability' is used in the GDPR to indicate that organisations must be accountable – must demonstrate – that they comply with the principles of data protection when processing personal data. Completing the GDPR Workbook (Part 2 of this pack) will help you to demonstrate GDPR compliance.

Processing personal data

5. What does 'accountability' mean in the GDPR?

The GDPR requires active and demonstrable compliance with data protection principles. Under the Data Protection Act 1998, which is being replaced, compliance was required but did not need to be demonstrated until perhaps a problem, for example, data breach occurred. The GDPR requires a pro-active, quality assurance approach to data protection and recognition that you must take steps to protect personal data and keep it secure.

For pharmacies, this will mean that records must be kept of the activities on an ongoing basis. This is not a record of everything undertaken, rather a record of classes of processing demonstrating adherence to the principles relating to the processing of personal data.

6. What records of processing activity do I need to keep?

You must be able to demonstrate that you are processing personal data in accordance with these principles. This will require you to keep records of the activities you undertake and show that you have considered whether the activity complies with each of the requirements.

The data protection principles are largely the same as those under the existing legislation, but under the GDPR, you must now show that you are complying with these them. You also need to be able to show that you are processing data lawfully.

7. What are the data protection principles to follow when processing personal data?

The GDPR requires you to follow certain data protection principles which, briefly, are:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected for specified, explicit and legitimate purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date;
e) 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
f) 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.

8. What are the lawful bases for processing the personal data?

Article 6 of the GDPR sets out how personal data may be processed lawfully:

> *'Article 6 Lawfulness of processing*
> ***1. Processing shall be lawful only if and to the extent that at least one of the following applies:***
> ***(a)*** *The data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
> ***(b)*** *Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
> ***(c)*** *Processing is necessary for compliance with a legal obligation to which the controller is subject;*
> ***(d)*** *Processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
> ***(e)*** *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
> ***(f)*** *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*
> *Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*
>
> *……..'*

Category 1(b) (c) (d) and (e) are all likely to apply in certain circumstances, but the most appropriate is likely to be 1(c) – the terms of service for NHS pharmacies and 1(e) – for all pharmacies. The provision of pharmaceutical services by pharmacy businesses is carried out in the public interest, both within the NHS and in the private sector.

By a quirk of legislation (unless this is reversed in the UK legislation accompanying the GDPR) pharmacy contractors with the NHS are considered to be public authorities and, therefore, cannot use lawful processing category 1(f) for the provision of pharmaceutical services.

Please note there is another hurdle or consideration if you want to process special categories of personal data lawfully.

9. What is special category data and what does this mean?

Special categories of personal data – those described in Article 9 of the GDPR – may not be processed except for specified purposes also set out in Article 9 and sometimes subject to special conditions.

Special categories of personal data that may not be processed unless there is a specific exception are:

> *… personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation…*

Therefore, as may be expected data concerning health is a special category of data. It has a specific meaning as follows.

> *'data concerning health' means personal 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;*

Data concerning health and other special categories of data may be processed where:

> ***(h)** Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, **the provision of health or social care or treatment or the management of health or social care systems** and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

Paragraph 3 requires a person who is subject to a professional obligation of confidentiality to be responsible for the processing of the data concerning health. Our understanding is that such a person must be a registered professional to practise and subject to removal from the register if unfit to practise; this could be a pharmacist or pharmacy technician.

10. How do the two hurdles of lawful processing and special category data fit together for data concerning health?

The GDPR has a two-stage process for you to confirm that you have a lawful basis for any personal data you process.

First stage

The first stage is to identify which of several broad categories applies to the personal data you process. These are listed in Article 6 of the GDPR, which is

above in the answer to question 7. Data concerning health may be processed because it is necessary for a task carried out in the public interest (Article 6(e)).

If the personal data is not special category data (see Article 9 of the GDPR and the answer to question 8 above), the data may be processed lawfully, and the second hurdle or stage is not relevant. If the personal data is a special category of data, for example, data concerning health, you must consider the second stage.

Second stage
If the personal data is a special category of personal data and, it may not be processed unless permitted by the GDPR and subject to any conditions in the GDPR.

Data concerning health may be processed – according to Article 9 (h) but the condition is that a professional subject to the obligation of confidentiality, such as pharmacist or pharmacy technician, must be responsible for a pharmacy company's processing of that data concerning health.

11. Must all personal data be processed lawfully under one of the provisions in Article 6 of the GDPR and, if a special category of personal data, the processing be permitted in Article 9 of the GDPR?

Yes.

Consent

12. Is consent still important?

Yes, but its use for the processing of data is not encouraged unless it is meaningful. Seeking consent for processing data associated with a prescription is not meaningful, as if it was refused then the prescription could not be dispensed. Prescription data must be processed for a variety of reasons including patient safety, professional responsibilities, pharmacy payment and anti-fraud checks. Patient consent to the action of the pharmacy dispensing the prescription (and, for example, consent to other services like MAS and CMS) remains as meaningful and important as ever, but once a patient has consented to this, generally records must be kept and often may be used by others caring for the patient. This is part of healthcare practice.

While consent for processing the personal data is not required, fair processing notices explaining to patients what personal data is processed and for what purpose are necessary.

13. If I want to collect personal data by consent or I do already, how do I comply with the GDPR?

If you want to collect data by consent, there are stricter rules on the meaning of consent and how it should be obtained. The GDPR seeks to make any consent sufficiently specific to be meaningful and introduces an additional concept of explicit consent for consent related to special category personal data.

By 25 May 2018, all consent must comply with the new meaning of consent set out in the GDPR and for a record of that GDPR compliant consent to be retained by the data controller. If you have this already, you do not need to renew the consents you have, for implementation of the GDPR. **If you do not have GDPR compliant consent, or do not have a record of this, you will have to renew the consent given before 25 May 2018 so that you have both.**

So, if the pharmacy has a separate marketing list for a specific purpose, to which those persons listed have given their consent, you may have to renew each person's consent before 25 May 2018 so that the consent is GDPR compliant and you have a record of it. It is also a good idea to version control your consent statements so that, if asked, you can show exactly the wording that an individual agreed to when giving their consent for data processing.

14. What is GDPR compliant consent?

The key point here is that generally you will not be processing personal data on the basis of 'consent' in GDPR terms, but if you do, the data subject's **consent** is required for processing of personal data; and the data subject's **explicit consent** is required for processing special categories of personal data, such as data concerning health.

'Consent' of the data subject 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 so if your website or any of your forms use this then you will need to review your processes.

Explicit consent is intended to be more specific 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'.

Broadly if personal data is collected by consent a data subject should be able to withdraw his or her consent at any time. Also, it should be as easy to withdraw consent as it was to give it.

Whether consent was freely given will depend on whether the data subject could give or refuse consent to the processing of data and still continue with the rest of the service or contract. If the data subject can do so, it is more likely that consent was freely given. If not, the data is processed, for example, by virtue of the contract only and should only be processed to the extent required by the contract.

If you collect personal data for marketing purposes, we advise you to read the guidance on consent by the Information Commissioner's Office.

15. Can I dispense and processes prescriptions without consent?

Generally, you need the consent of the patient **for the action of dispensing** that patient's prescription.

Generally, you do **not** need that patient's consent to **process the data associated with the prescription** – for example to make a record of the supply on your PMR or in your CD register.

Children's data

16. What about processing children's data?

For pharmacies dealing with prescriptions for children normal professional rules and legal principles apply, not the GDPR, because prescription data is not processed under explicit consent.

The GDPR sets out additional requirements in relation to children giving consent for the processing of their personal data particularly where this relates to 'information society services' which are broadly services provided at a distance, often via the internet and may involve buying and selling.

In Scotland, for the purposes of data protection, "Children" includes anybody below the age of 12. So, if you are using consent or explicit consent as a legal basis for processing, you must obtain parental consent for those under 12 (or those who are over 12 but you feel do not understand what they are agreeing to).

A child may wish to exercise their rights under the GDPR (see "Data Subject Rights"), so you must take any request from a child seriously, and make reasonable efforts to obtain parental consent if this is required.

Where services are offered direct to a child, you must ensure your fair processing notice is written in a clear, plain way that a child will understand.

Data Protection Impact Assessments

17. Do I need to do a data protection impact assessment (DPIA)?

You may need to undertake a data protection impact assessment under the GDPR if there is a significant change in a processing operation. You may wish to undertake a DPIA for your current activities to satisfy yourself that the need for processing is greater than the risks in relation to the purpose of your processing.

18. What information should data protection impact assessment (DPIA) include?

A DPIA should include:

a) A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
b) An assessment of the necessity and proportionality of the processing in relation to the purpose.
c) An assessment of the risks to individuals.
d) The measures in place to address risk, including security and to demonstrate that you comply.
e) A DPIA can address more than one project.

(Question and answer is taken from the ICO website)

19. What must I do if the data protection impact assessment indicates there is a high risk to the processing of personal data?

If there are high risks that personal data may not be protected – a high risk to the rights and freedoms of individuals – the supervisory authority, for the UK, the Information Commissioner's Office, should be consulted.

Pseudonymised personal data

20. What if I process pseudonymised personal data – personal data that does not identify the data subject?

If you process s pseudonymised personal data – personal data that does not identify the data subject but where the data subject could be identified later when the information is matched up with other information – you are still obliged to process this in accordance with the data protection principles, and to ensure the security of this data. However, you are **not** required to acquire or process additional information in order to identify the data subject and the data subject does **not** have most of the rights to access or rectify data etc.

Security and personal data breaches

21. What must I do to process personal data securely?

To process personal data securely you must consider:

- **a)** Pseudonymisation and encryption of personal data (for some time it has been necessary to encrypt personal data held on lap tops and memory sticks – but you may wish to speak to your PMR supplier about further measures);
- **b)** Be able to ensure the confidentiality, integrity, availability and resilience of the processing systems and services;
- **c)** Able to restore the personal data in a timely manner in the event of physical or technical problems; and,
- **d)** Have a system for regularly testing, assessing and evaluating the effectiveness of the security, technical and organizational; recognizing the risks involved in processing the personal data, including the risk of unauthorized disclosure.

Any natural person processing personal data – for the data controller or the processor – does so under instructions from the data controller; the pharmacy.

22. What is a data breach?

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 within your control.

23. What do I do if there is a data breach?

You must document any personal data breaches, including the facts of the breach, the effects of the breach and any remedial action taken. The Information Commissioner's Office may use these reports to assess compliance with the GDPR.

24. When must I notify a personal data breach?

Any personal data breach must be notified to the Information Commissioners Office (ICO) within 72 hours of the data controller having become aware of it, **unless** the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons.

If the breach is reported later, the reason for the delay must be explained at the same time the breach is notified late.

25. What must I do to notify a personal data breach?

Breach notifications to the Information Commissioner's Office must include:

a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) Describe the likely consequences of the personal data breach;
d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

26. Will I be fined if there is a data breach?

The Information Commissioner has other enforcement powers such as warnings and reprimands and powers to ensure appropriate standards are met, and it will use these to help support organisations to comply with the GDPR and DPA.
It does also have the power to fine and the fines under the GDPR are higher than before, up to £10 million Euros or 2% of global turnover. The maximum fine for non-compliance with an order by the supervisory authority, the ICO is double these amounts to £20 million Euros or 4% of total worldwide. The ICO has described these fines as last resort and for where a breach has been a result of gross negligence or criminal intent. Organisations may also face fines if they do not co-operate with the ICO in any investigation.

The Data Protection Officer

27. Who is the Data Protection Officer (DPO) and do I need one?

The Data Protection Officer (DPO) is a designated role under the GDPR which is intended to be given to somebody with expertise in data protection and who is both independent in decision-making – such as a professional – and senior in the organisation, who advises the organisation on data protection and GDPR issues.

28. Do I need a DPO?

There are two reasons why you are required to have a DPO. The first is because NHS pharmacies are subject to the Freedom of Information Act and any organisation that is subject to this act is automatically deemed to be a public authority by the proposed data protection legislation accompanying the introduction of the GDPR. The second is because you may be considered to be a data controller '*processing on a large scale .. special categories of data pursuant to Article 9* (which includes data concerning health).
Together, these make it clear that a DPO is required for community pharmacy businesses.

Recital 91 in the GDPR, albeit talking about data protection impact assessments (DPIAs) states:

> *….The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.*

Although, it is clear that 'processing of patient data in the regular course of business by a hospital is considered to be large-scale (Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, last Revised and Adopted on 5 April 2017).

29. What is the position and role of the DPO?

The Data Protection Officer (DPO) is somebody who:

a) Is appointed on the basis of professional qualities and knowledge of data protection law;
b) May be a staff member or somebody external may be contracted to undertake the role;
c) Has a role liaising with the supervisory authority, the Information Commissioner – the DPO's details shall be published and communicated to the ICO;

The data controller and the processor need to:

a) Ensure the DPO is involved properly and in a timely manner in all issues which relate to the protection of personal data;
b) Support the DPO with the resources necessary to carry out the role and access to processing operations and so the DPO can maintain his or her expert knowledge;
c) Ensure the DPO has the necessary protection, freedom and protection to carry out the role without fear or favour;
d) Ensure the DPO reports to the highest management level;
e) Provide that data subjects may contact the DPO relating to issues on processing their personal data ad their rights under GDPR;
f) Centrally bind the DPO to confidentiality; and,
g) Allow the DPO to carry out other duties and tasks (as appropriate) where there is no conflict of interest.

The DPO must have at least the following tasks:

a) Inform and advise the controller or the processor and the employees who carry out processing obligations under the GDPR or other data protection provisions;
b) Monitor compliance with the GDPR, considering data controller's policies, assignment of responsibilities, awareness-raising and training of staff involved in processing and related audits;
c) Provide advice where requested on the data protection impact assessment and monitor its performance;
d) Cooperate with, and act as a contact point for, the supervisory authority, the Information Commissioners Office;
e) Have due regard to the risks associated with processing operations in the performance of his role, taking into account the nature, scope, context and purposes of processing.

Fair Processing or Privacy Notices – information to be provided to data subjects

30. What is a fair processing Notice?

The GDPR requires data controllers to provide to data subjects information about their processing and related matters and the rights of the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

31. What information must I provide to data subjects? (Fair processing notices)

Where the personal data is provided by the data subject, for example, when a prescription is presented to a pharmacy in hard copy or following nomination of that pharmacy, the following information must be provided to the data subject, the patient:

a) The name and address of the data controller, the pharmacy company;
b) The contact details of the Data Protection Officer (DPO)
c) the purposes for which the personal data is processed and the legal basis for this;
d) The recipients or categories of the recipients of the personal data, if any;
e) Any relevant information about transfers to a third country or international organization
f) The period or criteria that will determine, how long the personal data is stored;
g) The relevant rights the data subject has in this case;
h) If the processing is based on consent, the right to withdraw that consent at any time;
i) The right to lodge a complaint with the supervisory authority, the Information Commissioners Office;
j) If the provision of personal data is a statutory requirement, the possible consequences of failure to provide it;
k) Relevant information on automated decision-making; and,
l) Any processing of the information subsequently for a different purpose.

You do not need to provide this information if it has been provided to the data subject already.

32. How must this information be provided?

The information may be provided in writing or, at the request of the data subject orally. Providing information may be by means of a notice in the pharmacy or on the website, whichever is more appropriate and may make use of standardized icons (which must be machine readable if provided electronically), to make the fair processing notice easily visible, intelligible and the information clearer.

33. When shall I provide the information - the fair processing notice – to a patient?

Ideally, the information in the fair processing notice should be provided to a patient at the time the patient nominates the pharmacy for the dispensing of its prescriptions, but could be provided when the first prescription is dispensed.

The information could be provided by way of an information notice on the wall of the pharmacy that is visible to patients and it is suggested that a patient's attention is drawn to the fair processing notice when the pharmacy dispenses the patient's first prescription, or subsequently when the notice is first displayed.

The notice could be handed out to the patient or included in the bag of dispensed medicines, when a patient's first prescription at the pharmacy is dispensed, or included in the pharmacy leaflet required for NHS pharmacies.

Health and Employment data

34. Can I process health data and employment data without consent?

Yes. Health data may be processed by a pharmacy on the basis, for example, that it is necessary for the performance of a task carried out in the public interest (Article 6, 1(e)); or processing is necessary for compliance with a legal obligation (the Terms of Service in the NHS Scotland Pharmaceutical Services Regulations) (Article 6(c)). There will also be many occasions when health data in a pharmacy is processed to protect the vital interests of the patient (Article 6(d)). As health data is a special category of personal data, the second stage of lawful processing must also be considered.

Employment data may be processed lawfully under one or more of the broad categories in Article 6, for example, as necessary for the performance of a contract and, for tax and national insurance purpose, for compliance with a legal obligation.

Processors

35. What are processors, and can I send my staff's data to a third party for the payroll?

Processors are those people to whom you send personal data for a specific task, who you instruct exactly what to do with the personal data, for example, when you send information to a third party organisation for your payroll. You can use processors, but you must include in your fair processing notice the types of organisation which you may share data with and why.

36. What must I agree with my processors?

You must have a contract or other legal provision which ensures they are GDPR compliant and if they are not in the UK, additional requirements may apply.

In brief, the contract must include or stipulate:

a) Documented instructions from the data controller, which includes transfers to a third country or international organisation;
b) Ensure that persons authorised to process the personal data have committed themselves to confidentiality or under a statutory obligation of confidentiality, for example, pharmacists and pharmacy technicians;
c) Ensure the processor takes all the GDPR measures necessary for processing personal data securely;
d) The processor must agree not to pass personal data to another processor except with the prior written authorisation of the data controller and if given, apply the same data protection requirements to the contract with the additional processor;
e) The processor must assist the data controller in complying with data subject rights.
f) The processor assists the controller in complying with obligations relating to security and data breaches.
g) At the choice of the data controller, the processor will delete or return all personal data at the end of the contract/provision of services, unless required by las to keep them;
h) The processor will make available to the controlled all information necessary to demonstrate obligation such as audit and inspection conducted by the data controller or somebody mandated by the controller.

Processors may not pass the personal information to a third party – another processor – without prior written authorisation from the data controller; and if this is permitted the contract with the additional processor must include the same data protection requirements as the original contract

37. If I am a processor of personal data what must I record?

Processors are required to keep certain records which you as the data controller may be asked to make available to the Information Commissioners Office. More information is available on the ICO website. Processors must also be able to demonstrate that they either return or destroy personal data once the processing that they have been instructed to, or as per your contract with them.

Data subject rights

38. What do I have to provide or do at the request of the data subject?

Data subjects had various rights under the Data Protection Act 1998 and broadly, these rights remain and are developed and clarified under the GDPR. Some rights only apply to personal data which is collected by consent, on the basis that if you consent to the collection of data you ought to be able to retract that consent. The key rights that data subject have are:

a) Right of access – the data subject has a right to obtain from you a copy of the personal data you hold on the person (e.g. from the PMR), free of charge on the first occasion, and the following information
   i) Purpose of the processing
   ii) Categories of personal data concerned
   iii) To whom you disclose the data
   iv) How long the data is stored or how this is calculated
   v) The existence of the right to rectification or reassure (not erasure for health data)
   vi) Right to lodge a complaint with the ICO
   vii) If not collected from the data subject, where the personal information came from
   viii) Additional information related to automated decision-making and transfer of personal data overseas)

b) Right to rectification – the data subject may ask for incorrect or inaccurate information to be corrected, which may be more appropriate by way of a supplementary statement, because, for example, the record of what was prescribed or dispensed my need to be retained for professional or legal reasons.

c) Right to erasure – particularly relevant if the only ground for processing personal data is consent (or explicit consent if the information is special category personal data). The right to erasure does not apply to data concerning health.

d) Right to restrict processing – in some cases the data subject may restrict your normal processing and may, for example, not to delete data you would otherwise delete because the data subject needs the data for a legal case.

e) Right to have others notified of any rectification, erasure or restriction - any rectification, erasure or restriction must be notified to each person to whom the data has been disclosed unless this proves impossible or would involve a disproportionate effort.

f) Right to data portability – this applies only where the processing is based on consent or a contract (and therefore in most cases should not apply to data concerning health)

g) Right to object – which could apply to pharmacies – in which case the pharmacy should provide a copy of the fair processing notice and will need to show in the specific case that it has compelling legitimate grounds for processing the personal data that overrides the interest, rights and

freedoms of the data subject; or the pharmacy may retain the data for the establishment, exercise or defence of legal claims.

39. When do I have to provide relevant information to data subjects?

You must provide relevant information to the data controller without undue delay and in any event within one month of receipt of the request. If you need more time you need to tell the data subject and explain why. If you have not taken the action requested you should provide the details of the supervisory authority, the Information Commissioners Office so the data subject may lodge a complaint.

40. How should I provide the information?

The information requested if requested electronically should be provided electronically if possible, unless otherwise requested by the data subject. Otherwise the information may be provided in hard copy form.

41. Can I charge a fee for providing information to data subjects in response to these requests?

No. Unless the request is manifestly unfounded or excessive, for example because they are repetitive, in which case you can charge a reasonable fee or refuse to act on the request.

42. Can I refuse these requests from data subjects?

Yes, but only in certain cases, see the answer to the question above.

43. May I check the identity of the data subject?

You may, and you should, to ensure that you do not disclose confidential information to the wrong person.

Data protection by Design

44. Do I have to think about data protection by design and default?

Yes. Designing systems and procedures with recognition of data protection principle has long been important and it is now a requirement of the GDPR. The introduction of any new activity or technology should involve your DPO so that they are able to give advice.

Cooperating with the Supervisory Authority – the Information Commissioners Office

45. Do I need to cooperate with the Information Commissioner's Office and NHS Scotland?

Yes, the Information Commissioners Office (ICO) is the relevant supervisory authority for the UK and enforces data protection rules, regulations and legislation. Data controllers and processors must cooperate with the ICO.

The ICO also provides extensive guidance on data protection and the GDPR.

Acknowledgements

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

Version Control

Version 1: April 2018

Version 2: May 2018 – change in advice re: DPO