General Data Protection Regulation (GDPR): FAQs (March 2018)

Disclaimer: ***As the information on the General Data Protection Regulation (GDPR) is constantly being updated, the contents of relevant superintendent updates and resources may be subject to change. The information published is, to the best of our knowledge, correct at the time of publication. However, no responsibility will be accepted for any consequences of decisions made using this information.***

Introduction

The General Data Protection Regulation (GDPR) will come into effect in the UK from 25 May 2018. Many concepts and principles setting out the main responsibilities for organisations will be similar to the existing UK Data Protection Act 1998 (DPA); however, the GDPR will introduce new elements and significantly enhanced requirements regarding data protection. If an organisation needs to be compliant with the current DPA, it also needs to be compliant with the GDPR.

NPA support

- In preparation for the GDPR, the NPA has published a number of resources which can be downloaded from the NPA website.
- Furthermore, a GDPR webinar was held in March 2018 which provides practical guidance and examples to help understand the GDPR requirements.

! PLEASE NOTE – this FAQ document will continue to be updated as required.

General questions

FAQ	Answer
1) Where can I find further information regarding the GDPR?	Further information on the GDPR can be obtained from the: • NPA website • Information Commissioner's Office (ICO) website • NHS Digital website
2) What is changing regarding data protection?	Data protection laws are changing within the European Union and the UK: • European Union: currently, the requirements for processing personal data is set by the Data Protection Directive; however, this will be replaced by the GDPR from 25 May 2018 • UK: currently, the requirements for processing personal data in the UK is governed by the Data Protection Act 1998 (DPA), which implements the EU directive. The DPA will be replaced by the updated Data Protection Act which will **accompany** the GDPR ○ The Data Protection Bill (the proposal to change the UK's existing data protection law) is currently passing through the UK Parliament ○ The updated Data Protection Act will establish rules for processing personal data which is outside of the GDPR such as law enforcement
3) Is Brexit going to affect the implementation of the GDPR?	No. The GDPR applies to all European Union member states and will occur regardless of Brexit negotiations. The GDPR applies from 25 May 2018; Brexit is currently set for 29 March 2019.

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

4) Do all members of the pharmacy team need to be aware of the GDPR?	Yes. A fundamental requirement for the implementation of the GDPR is its awareness by all within an organisation; this includes having an understanding about the GDPR, its principles, and the roles, responsibilities and processes of organisations. The NPA GDPR Staff Training Manual and accompanying multiple choice question (MCQ) assessment can be used to demonstrate compliance with this requirement of the GDPR.
5) What is the difference between a data controller and a data processor?	A **data controller** determines how and why personal data is processed. Under the GDPR, the pharmacy organisation is a data controller. The superintendent pharmacist/members of the pharmacy team working within the pharmacy organisation help to fulfil the role of the data controller. A **data processor** carries out processing on behalf of the data controller. All individuals within a pharmacy organisation are acting as data controllers and not data processors. Examples of a data processor would include an externally appointed pharmacy organisation's payroll company or a courier company used for the purpose of submitting an end of month prescription bundle.
6) What are the six data protection principles identified under the GDPR?	The **six data protection principles** identified under the GDPR state that personal data must be: 1. *Processed lawfully, fairly and in a transparent manner* 2. *Collected for specified, explicit and legitimate purposes* 3. *Adequate, relevant and limited to what is necessary in relation to the purposes of processing* 4. *Accurate and where necessary, kept up to date* 5. *Kept in a form which allows the identification of a data subject for no longer than is necessary* 6. *Processed in a manner that ensures appropriate security*

7) What is the purpose of the accountability principle under the GDPR?	The accountability principle is a new addition under the GDPR which requires organisations to demonstrate compliance with the data principles of the GDPR. The accountability principle aims to minimise the risk of data breaches and promote protection of personal data. It is the organisation's responsibility to ensure they are able to demonstrate compliance with the GDPR requirements.
	
	Organisations can demonstrate compliance through:
	• Implementation of comprehensive governance measures, which must be proportionate to their processing
	• Maintenance of records of data processing activities – these records must include the:
	  ○ *Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer)*
	  ○ *Purposes of the processing*
	  ○ *Description of the categories of individuals and categories of personal data*
	  ○ *Categories of recipients of personal data*
	  ○ *Details of transfers to third countries including documentation of*

	the transfer mechanism safeguards in place ○ *Retention schedules* ○ *Description of technical and organisational security measures* • Putting into practice appropriate security measures to protect personal data
8) What is the fine imposed on an organisation if they fail to comply with the GDPR requirements?	The fine is determined by the type of infringement. The GDPR have outlined the following fine structure: • A fine up to €10million or 2 per cent of the organisation's global turnover (whichever is higher) for infringements including those relating to the failure to notify the ICO of a data breach and the failure to follow data controller or processor obligations • A fine of up to €20million or 4 per cent of the organisation's global turnover (whichever is higher) for infringements including those relating to non-compliance of orders from the ICO, failure to follow the basic principles for processing including consent, and individual rights Fines can be imposed solely, or in addition to certain measures including warnings issued by the ICO to the data controller or processor of a GDPR infringement. The decision of whether to impose a fine, and the amount, will be assessed on a case-by-case basis depending on factors such as: • The duration, gravity and nature of the infringement • Whether the infringement was intentional or due to neglect • Action taken by the data controller or processor to mitigate any damages caused • The categories of personal data involved

Data breaches

FAQ	Answer
9) What types of data breaches need to be reported and to whom?	There will be a **duty for all organisations to report certain data breaches to the ICO**, and in some cases, report the date breaches to the affected individual(s). Examples of data breaches which must be reported include: • Damage to reputation • Discrimination • Financial loss • Loss of confidentiality • Other economic/social disadvantage **You must notify the ICO:** • If the data breach is likely to result in a risk to the rights and freedoms of an individual **You must notify the affected individual(s):** • If the data breaches is likely to result in a 'high risk' to the individual's rights and freedoms of individuals ○ The ICO considers 'high risk' when "*the threshold for informing individuals is higher than for notifying the ICO*" – a pharmacy will need to assess "*both the severity of the*

	potential or actual impact on individuals as a result of a breach and the likelihood of this occurring"; furthermore, the ICO can actually compel a pharmacy to report the breach to the affected individual(s) if this has not already been undertaken
	
	Other parties requiring notification:
	• NHS England, where required
	  ○ The NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013 (NHS Terms of Service) require NHS contracted pharmacists to ensure compliance with NHS England's (formerly NHSCB) requirements regarding data security and investigate the cause of the breach and evaluate the response to it – this include updating SOPs and providing staff training to prevent reoccurrence
	  ○ Currently, to ensure compliance, the Information Governance (IG) Toolkit must be completed by each NHS pharmacy contractor annually – this covers data breaches
	  ○ Any patient identifiable data (PID) which has been incorrectly submitted, is breaching the NHS Terms of Service
	• **Patient safety incident**
	  ○ If the data breach constitutes to a patient safety incident, this should be recorded and reported:
	  ▪ England: via the NPA Patient Safety Incident Report Form
	  ▪ Northern Ireland: anonymously to the Health and Social Care Board Medicines Governance
	  ▪ Scotland: advised to use the NPA Patient Safety Incident Report Form and contact the local NHS Board.
	  ▪ Wales: via the National Reporting and Learning System
	• Regulatory bodies such as the General Pharmaceutical Council (GPhC), where required
	• The police, where required

10) What fines can be imposed as a result of failure to report a data breach?	**Failure to report** certain personal data breaches to the ICO (and, in some instances, failure to report breaches to the affected individual(s)) upon identification can result in a fine of up to €10million or 2 per cent of the organisation's global turnover.
11) Can asking a patient/ representative to confirm the address verbally when handing out dispensed prescription items be seen as a data breach if others can hear this?	Yes. Asking a patient/representative to confirm the address verbally when handing out dispensed prescription items can be deemed a data breach if others can hear this. It is prudent to ensure the standard operating procedures consider patient confidentiality, not just to comply with the GDPR, but also to abide by the professional standards set by the GPhC and the Pharmaceutical Society of Northern Ireland (PSNI). You may wish to consider displaying a patient notice informing patients of the procedure undertaken when handing out dispensed prescription items and this can state the patient is able to provide proof of identification instead of verbally confirming their identity. Additionally, the patient notice can highlight that this process can take place in a consultation room.

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

Lawful basis for processing

FAQ	Answer
12) What are the six lawful bases identified for processing data under the GDPR?	The **six lawful bases** for processing data outlined under the GDPR are: 1. *The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes* 2. *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* 3. *Processing is necessary for **compliance with a legal obligation** to which the controller is subject* 4. *Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person* 5. *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* 6. *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** **shall not apply to processing carried out by public authorities in the performance of their tasks*
13) Is consent always required when processing personal data in a pharmacy?	Consent must be obtained where no other lawful basis for processing personal data is applicable. As there are five other lawful bases to process personal data, consent may not always be required from an individual. Wherever possible and appropriate, the organisation should try to use other lawful bases permitting the processing of an individual's personal data. For consent to be valid, it must meet the GDPR's *'conditions for consent'.* Where consent is used as the lawful basis for processing personal data, the individual must be given an actual choice and control on how the organisation is to use their data. Examples of where consent would be necessary in pharmacy include: a prescription delivery service, a repeat prescription management service, sending emails/text messages, nominating patients for the Electronic Prescription Service (EPS) and accessing Electronic Care Records in Northern Ireland or Summary Care Records (SCR) in England. When a patient presents a prescription for dispensing in a pharmacy, the patient effectively implies consent to enable the pharmacy to process their personal data for the purpose of prescription dispensing. In this scenario, the pharmacy's lawful basis for processing the personal data under the GDPR is: *"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**"*. Further information can be found in "*General Data Protection Regulation (GDPR): consent – brief overview*"

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

Privacy notice

FAQ	Answer
14) Is there a template privacy notice for pharmacies?	A template privacy notice will be available from the sector-specific resources published by the Community Pharmacy GDPR Working Party.
15) What needs to be included in a privacy notice?	The ICO has provided guidance, a privacy notice checklist and examples of privacy notices in practice regarding how a privacy notice should be written which outlines the following elements to be considered: • What information is being collected? • Who is collecting it? • How is it collected? • Why is it being collected? • How will it be used? • Who will it be shared with? • What will be the effect of this on the individuals concerned? • Is the intended use likely to cause individuals to object or complain?

Consent

FAQ	Answer
16) What is meant by 'consent' under the GDPR?	'Consent' 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. Further information on consent can be found in "*General Data Protection Regulation (GDPR): consent – brief overview*"

17) What does GDPR compliant consent mean?	In order for consent to be valid, it must meet the GDPR's Chapter II, Article 7, "*Conditions for consent*" as summarised:
	• Freely given by the individual
	• Obtained by clear affirmative action from the individual who must have positively opted-in
	• Specific and unambiguous as to what the individual is consenting to
	  ○ For example, a statement can be added to a consent form confirming that the information provided, such as an email address/telephone number, will only be used for the purpose of the prescription collection/delivery service, and information will not be passed on to third parties
	• Easily accessible to the individual, and be presented in clear and plain language
	• Simple and straightforward and allow for the individual to withdraw at any time; individuals should be aware of how to withdraw consent prior to providing consent
	  ○ For example, a consent form may include information on **how** the individual is able to withdraw consent, such as via email/telephone

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

18) Does consent need to be obtained from each patient who presents a prescription for dispensing?	No. Consent under the GDPR does not need to be obtained from each patient presenting a prescription for dispensing because consent **is not** the lawful basis for processing: • A patient provides implied consent to enable the pharmacy to process their personal data for the purpose of dispensing a prescription • The pharmacy's lawful basis for processing the personal data present on the prescription: "*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*"
19) Is the dispensing of electronic prescriptions expressed consent or implied consent from the patient?	Dispensing electronic prescriptions is **implied consent** as the patient/representative nominates the pharmacy before the electronic prescription is retrieved by the pharmacy.
20) What examples of pharmacy services require records of consent?	Examples of services which require consent to process data include: • Providing a prescription delivery service • Providing a repeat prescription management service • Sending emails/text messages to patients • Nominating patients for the Electronic Prescription Service (EPS) • Accessing Summary Care Records (SCR)
21) If a surgery asks for a prescription to be delivered urgently to a patient and the pharmacy do not have consent from the patient – should the pharmacy get consent once the medicines have been delivered?	A pharmacy cannot deliver prescription items to a particular patient and obtain consent afterwards. ICO guidance states that if you are able to process a particular personal data without consent, then asking for consent will be *"misleading and inherently unfair"*. In this scenario, it needs to highlighted that consent is **not** the lawful basis for processing: • The requirement to urgently deliver medication is coming from the patient's surgery and not the patient themselves • The lawful basis for processing the patients personal data for the purpose of urgent delivery in this case is: "*processing is necessary in order to **protect the vital interests** of the data subject or of another natural person"* In this situation, it is advisable that the pharmacy clearly documents the lawful basis of this processing on the patient's medication record (PMR). If the patient wishes to receive future deliveries of prescription items following this initial urgent delivery, the pharmacy would need to obtain GDPR compliant consent as further deliveries would fall require consent as a lawful basis.
22) Can a representative give consent on behalf of a patient?	**An adult unable to give valid consent** If an adult patient **lacks** capacity, understanding or is unable to make their own decisions, they cannot give valid consent and no-one else can do so on their behalf unless their representative has a Lasting Power of Attorney (or Enduring Power of Attorney in Northern Ireland), or are appointed as a deputy by the Court with authorisation to make service or treatment decisions on behalf of the patient. Further information can be found in the NPA service user consent suite of resources. **An adult able to give valid consent**

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

	In a scenario where personal health data is to be processed for an adult **with** capacity to give consent, and consent cannot be obtained, for example, in the event a patient has a physical disability and cannot sign the form, the organisation will be required to choose another lawful basis. The ICO suggests that where possible, if consent cannot be gained as per the GDPR requirements, another lawful basis should be chosen. Another lawful basis could be: • *"Processing is necessary in order to* ***protect the vital interests of the data subject or of another natural person"*** as "*processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent"* • *"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"*** Under the Equality Act 2010, a pharmacist is required to make reasonable adjustments within the pharmacy to overcome obstacles which prevent a person with a disability from receiving goods and services. This could mean liaising with appropriate healthcare professionals involved with the patient's care, for example, the prescriber, and making clear records of any decisions made without written consent for a clear audit trial.

Data protection officer (DPO)

FAQ	Answer
23) Do all pharmacies need a Data Protection Officer (DPO)?	Yes. All pharmacies process personal health data and under the GDPR, a data protection officer (DPO) is required if an organisation carries out '***large scale processing of special categories of data***'. Health data is an example of a special category of data.
24) Who can be the DPO?	The ICO has stated • The DPO can be an **existing employee of an organisation** or the role can be **contracted out externally** to another organisation • Professional duties should be compatible with DPO duties **and** there must be no conflicts of interests If the DPO is a General Pharmaceutical Council (GPhC) registrant, they must additionally abide by the standards for pharmacy professionals; Standard 6 states "*pharmacy professionals must behave in a professional manner*"... and "*act with honesty and integrity*". This further re-emphasises the possibility of an existing pharmacy professional (such as the superintendent pharmacist) potentially acting as the DPO even if they are in charge of setting pharmacy procedures or complying with GPhC registered pharmacy premises standards. In England and Wales, the pharmacy's Information Governance (IG) Lead can potentially act as the DPO **as long as** the criteria above are fulfilled. This concept is similar to how the IG Lead can presently be

	the pharmacy superintendent pharmacist whilst acting independently – the professional duties of the DPO will require the DPO to have no conflicts of interests.
25) Does the DPO need to undertake any training?	No training is required for the role of a DPO; however, the ICO have stated that the DPO must be an expert in data protection. The DPO is therefore, expected to have adequate knowledge of data protection law.
26) Can pharmacies of different legal entities share one DPO?	Yes. The ICO has stated that one DPO can be appointed for a group of companies or public authorities as long as the appointed individual effectively performs the DPO tasks taking the size and structure of each organisation into consideration. The organisations should ensure the DPO has the necessary resources in place to undertake their role and be supported as appropriate. Furthermore, the DPO must be easily contactable – the DPO's contact details should be available by the employees of each organisation, the ICO and the individuals whose personal data is processed.

References, further reading and information

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- ICO "*Guide to the General Data Protection Regulation (GDPR)*": https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr