General Data Protection Regulation (GDPR): consent – brief overview

(November 2017)

***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.

A brief overview of the GDPR can be found in the NPA resource "*General Data Protection Regulation (GDPR): brief overview*". This resource provides a brief overview on **consent** - one of the six lawful bases for processing personal data under the GDPR.

Lawful basis for processing personal data

Organisations must identify and document their lawful basis for processing personal data and sensitive personal data, as well as determining the necessity for the processing. There are six lawful bases to allow an organisation to process personal data, as outlined below:

GDPR "*Lawfulness of processing*"

*(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)... shall not apply to processing carried out by public authorities in the performance of their tasks.

REF:- 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): Chapter II, Article 6: Lawfulness of processing

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

General Data Protection Regulation (GDPR): consent – brief overview

(November 2017)

Consent

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. The GDPR defines consent as:

GDPR definition of consent

*'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.*

REF:- 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): Chapter I, Article 4: Definitions

In order for consent to be valid, it must meet the GDPR's Chapter II, Article 7, "*Conditions for consent*". Table 1 below summarises these conditions.

Table 1: Summary of conditions for consent

In order for consent to be **valid**, it should be:	Consent should **not** be:
✓ 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 ✓ 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	× Presented to the individual in a vague, difficult to understand, or unintelligible manner × Obtained by default by lack of affirmative action from the individual × Obtained by default by using pre-ticked opt-in boxes × Obtained by using opt-out boxes × Part of the terms and conditions of a service; consent must be separate

The Information Commissioner's Office (ICO) also recommends:

- Regularly reviewing and updating consent and associated procedures (as necessary)
    - The GDPR does **not** stipulate a set time limit or expiry date for the validity of consent; this would depend on the context in which it is being obtained
- Keeping records of evidence; including the name of individual providing consent, the date of consent, how consent was provided, and the purpose for consent

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

General Data Protection Regulation (GDPR): consent – brief overview

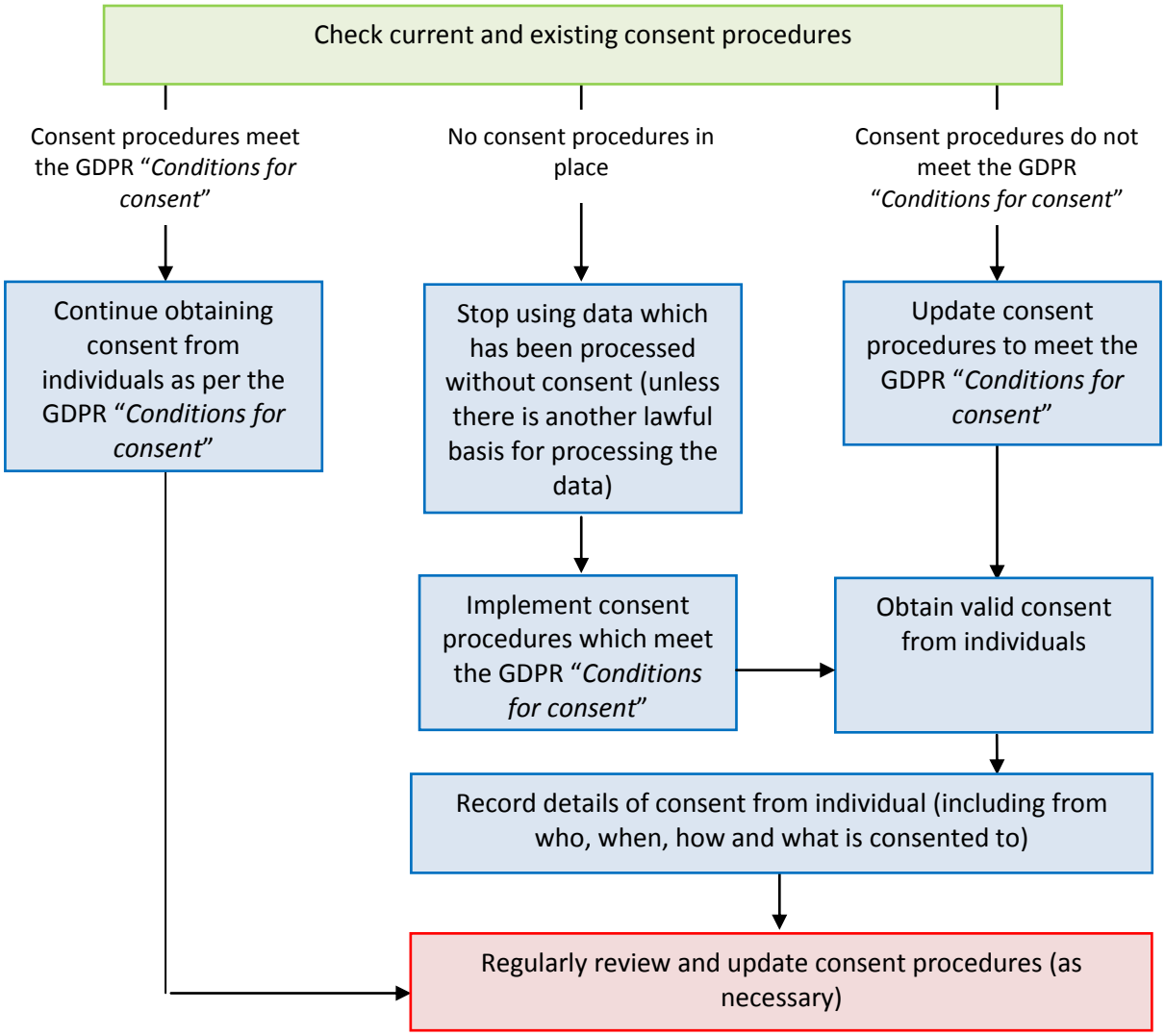
(November 2017)

Top tips: valid consent under the GDPR

In order to prepare for the implementation of the GDPR, pharmacy teams should:

- ✓ Familiarise themselves with, and be aware of, the six lawful bases for processing personal data
- ✓ Check current and existing procedures for obtaining/updating consent in the organisation – this includes how consent is sought, recorded and managed
    - Appendix 1 has a flowchart to help check if an organisation has the appropriate procedures in place, with the aim of highlighting potential areas of improvement, as necessary
- ✓ Consider the services offered by the organisation which require consent to process data
    - Services include providing a prescription delivery service or a repeat prescription management service, sending emails/text messages, nominating patients for the Electronic Prescription Service (EPS) and accessing Summary Care Records (SCR)
- × Be aware that inappropriate or invalid consent is **not** a lawful basis for processing personal data
    - Inappropriate/invalid consent may potentially result in substantial fines for the organisation

Appendix 1: Flowchart to check if there is an appropriate consent procedure in place



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

Reference, 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/
- ICO GDPR consent guidance: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/

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