General Data Protection Regulations

What you need to know

The GDPR and Data Protection Act 2018 replace the Data Protection Act 1998 which is an updated and strengthened data protection framework, however, the key principles of the original Act remain unchanged.

The most relevant changes for GPs in their role as data controllers are:

- Compliance must be actively demonstrated, for example it will be necessary to:
    - Keep and maintain up-to-date records of the data flows from the Practice and the legal basis for these flows; and
    - Have data protection policies and procedures in place.

- More information is required in 'Privacy Notices' for patients.
- Practices will not be able to charge patients for access to medical records (save in exceptional circumstances)
- Designation of Data Protection Officers.

Consent

Consent is defined as:

"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 must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

Active opt-in: Pre-ticked opt-in boxes are invalid, use unticked opt-in boxes or similar active opt-in methods with equal prominence.

Documented: Keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

You must keep clear records to demonstrate consent. The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanism. The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Access

Subject Access Requests: The GDPR makes two important changes to individuals' rights of access to data about them. Firstly, the time period for complying with such requests has been reduced from 40 days to one calendar month. Secondly, except for repeated requests. Controller will not be able to charge individuals for responding to these requests.

Withdraw consent

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time. Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent. You need to review existing consents and you consent mechanism to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be easy to withdraw as it was to give consent.

Rights

The GDPR provides the following rights for individuals:

1. **The right to be informed.** Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

2. **The right of access.** Individuals have the right to access their personal data and supplementary information.

3. **The right to rectification.** Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete.

4. **The right to erasure.** GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten.'

5. **The right to restrict processing.** Individuals have the right to request the restriction or suppression of their personal data. This is not an

absolute right and only applies in certain circumstances.

6. **The right to data portability.** This allows individuals to obtain and reuse their personal data for their own purposes across different services, it allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. **The right to object to processing.**

8. **Rights in relation to automated decision making and profiling.** The GDPR has provisions on: automated individual decision – making (making a decision solely by automated means without profiling can be part of an automated decision-making process).

Privacy Policy

The Privacy policy includes:

1. Information we may collect from you.
2. Uses made of the information.
3. Disclosure of your information.
4. Where we story your personal data.
5. Changes to our privacy policy.

Please ask at Reception for a copy.

Legitimate interests:

Under GDPR, legitimate interests may apply where:

"processing is necessary for the purposes of the legitimate interests pursues buy the controller or the third party, except where such interests are overridden by the interests or fundamental right and freedom of the data subject which require protection of personal data, in particular where the data subject is a child."

The GDPR states the processing of personal data for direct marketing may be regarded as carried out for a legitimate interest.

Prescription Information – on behalf of the Business Services Authority

A new data privacy law will be introduced in the UK in May 2018. As a result, we have published a new privacy notice to make it easier for you to find out how the NHS Business Services Authority uses and protects your prescription information.

Your Doctor or Pharmacist sends your prescriptions to us after dispensing your medical products to you, as stated on the prescription form. We manage the information on the forms as required by Data Protection Law and we use it to:

- Pay the organisation providing you with medical products
- Secure effective and efficient delivery of NHS services
- Analyse general trends to support more effective planning of NHS services
- Check for fraud and mistakes, including checking claims you make for help with NHS charges. If we can't confirm you are entitled to help, you may be sent a Penalty Charge Notice.
- Monitor the safety of new medicines.

To prevent, detect and investigate fraud and errors, we may share your information with:

- NHS Counter Fraud Authority
- The Department of Work and Pensions
- HM Revenues and Customs
- Veterans UK
- NHS Commissioners and service providers

We'll only share information that can identify you with those directly involved in your NHS care or reviewing your NHS care, those who have a legal right to it and those who you have given us permission to share it with.

We also share information with Public Health England to help them protect and improve the health of the population of England. You can only be identified from this information where Public Health England had the legal power to do so. We share patient identifiable information for new medicines with the Drug Safety Research Unit at Southampton University. They have a legal right to this. They will contact your GP to ask for your permission to take part in the medicine safety study. If you do not want to take part, your information will be deleted.
You can find out more about the above at:
www.nhsbsa.nhs.uk/yourinformation