Response to questions asked during GP training sessions around the implications of GDPR

During the training sessions that have been provided over the last few months by Midlands and Lancashire CSU, a number of questions have been raised about how the new General Data Protection Regulations (GDPR) will impact some of the ways in which practices work. Please see below a number of FAQs for information.

1) **Practices use text messaging services to remind patients about their appointments. Patients may have been initially opted in and then contacted afterwards advising them of their opt out options. Do practices need to contact all patients who did not respond to the opt out to request consent?**

   A) *Firstly you must have covered the use of this type of messaging in your privacy notices.*

   Secondly it is fine to carry on using text messaging as you do currently to advise of appointments etc without explicit consent. The two articles below apply in this case.

   Article 6(e) Public Task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

   Article 9(h) …..for the purposes of preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care…..

2) **Practices use text messaging services to send patients the friends and family test following their appointments. Is consent required for this?**

   A) *It should be noted that the friends and family test does not have to be sent to patients after every consultation. However, this is a national request of the NHS and is used to improve services. You should only be sending this by text if you have valid consent by the patient to do this. If you not currently have valid consent you should stop sending this request by text and obtain valid consent by the patient. This could be done at the patients next consultation or when they next contact the surgery. You must always include the option for patients to opt out of this service. It should also be included in your privacy notice.*

Response to questions asked during GP training sessions around the implications of GDPR

3) Practices use email to send information about new services to patients. Is consent required for this?

A) *this could potentially be classed as marketing under PECR – Privacy electronic Communication Regulations and therefore would require explicit consent to do this. This processing would also need to be included within your privacy notice.*

4) What is the legal basis for GPs to access, process and refer patient information as part of a patient's consultation?

A) *Provision of direct care*

— Explicit consent under the GDPR is distinct from implied consent for sharing for direct care purposes under the common law duty of confidentiality. The GDPR creates a lawful basis for processing special category health data when it is for the provision of direct care that does not require explicit consent. GP data controllers must establish both a lawful basis for processing ***and*** *a special category condition for processing.*

— The lawful basis for processing special category health data for direct care is that processing is:

'necessary… in the exercise of official authority vested in the controller' (Article 6(1)(e)).

It is also possible for NHS GP practices to rely on 'processing is necessary for compliance with a legal obligation to which the controller is subject' (Article 6(1)(c).

— The special category condition for processing for direct care is that processing is:

'necessary for the purposes of preventative 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...' (Article 9(2)(h)).

— When relying on Articles 6(1)(e) and 9(2)(h) to share data for the provision of direct care, consent under GDPR is not needed. However, in addition to the GDPR, data controllers

must also satisfy the common law duty of confidentiality. In order to satisfy the common law data controllers can continue to rely on implied consent to share confidential health data for the provision of direct care.14 The most common example of when consent can be implied is when a patient agrees to a referral from one healthcare professional to another. In these circumstances, when the patient agrees to the referral this implies their consent for sharing relevant information to support the referral (unless the patient objects).
The referral information can then be disclosed under GDPR using articles 6(1)(e) and 9(2)(h) as above.

5) Under GDPR data subjects have more rights over their data including the right of erasure. How should a practice respond to a patient asking for their medical records to be erased?

A) *see the following link to ICO guidance - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/*

Particularly - When does the right to erasure not apply?

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- *if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or*
- *if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).*

Response to questions asked during GP training sessions around the implications of GDPR

6) Who can act as the DPO for a GP practice?

A) *All practices which provide services under an NHS contract are public authorities43 therefore it is mandatory that they designate, but not necessarily employ or retain, a DPO; a person with expert knowledge of data protection law. (A single-handed private practice which is not carrying out NHS work and does not carry out 'large scale' processing is unlikely to be required to designate a DPO).44 Designation is a decision to be made by the practice. The DPO is expected to monitor compliance, however, responsibility for compliance remains with the data controller and data processor. Large practices and multi-practice groups are likely to have in-house DPOs but smaller practices may prefer to designate external DPOs that could for instance be provided by a Clinical Commissioning Group, Business Services Organisation or local/regional health board.*

— The DPO must not carry out duties which result in a conflict of interests and must not hold a position that leads him or her to determine the purposes and the means of the processing of personal data – this requirement will vary depending on whether the DPO is an internal or external appointment. In most cases, the data controller will be the GP practice rather than an individual GP and that internal practice decisions about data processing (ie the purpose and means of processing) will be subject to the governance arrangements of the practice partnership. This means it might be possible for GP partners to fulfil the role of DPO provided the role is defined to avoid conflict of interests and decisions are documented.

7) Can we charge for Subject Access Requests?

A) *Handling subject access requests is the subject of a separate BMA guidance document titled Access to health records.42 In most cases, patients must be given access to their medical records free of charge, including when a patient authorises access by a third party such as a solicitor. A 'reasonable fee' can be charged if the request is manifestly unfounded or excessive, however, these circumstances are likely to be rare.*

Response to questions asked during GP training sessions around the implications of GDPR

8) What makes consent valid?

A) *Valid Consent -*

- *Consent must be fully informed and freely given.*
- *It does not always have to be written consent as long as has been recorded in case the consent is challenged.*
- *Implied consent will not exist.*
- *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.*

NOTE:- You cannot obtain consent by emailing or texting patients as this will breach the Privacy Electronic Communication Regulations (PECR). Consent should ideally by obtained when the patient contacts the practice.

USEFUL LINKS:-

IGA - THE EU GENERAL DATA PROTECTION REGULATION: THE KEY POINTS FOR GPS

https://digital.nhs.uk/binaries/content/assets/legacy/pdf/l/r/iga_-_gdpr_gp_advice_note_-_v1_final.pdf

ICO – GDPR information

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

BMA - GPs as data controllers under the General Data Protection Regulation

https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers