surrey and sussex lmcs

To all practices in Surrey and Sussex LMCs

22nd May 2018

Dear Colleagues

GDPR Update

The GDPR comes into effect on 25th May 2018 and I am writing to update practices in terms of recommended preparation for this, but noting two important points: firstly, the Information Commissioner is not expecting all GDPR requirements to be in place on 25th May, practices should be aware of the Regulation and planning for compliance with it at that point but are NOT expected to be fully compliant: indeed, it would be impossible to be so, because, secondly, it is unclear how many aspects of the GDPR will work in reality, and some of these will only be established by case law; so it is impossible to provide definitive guidance on many points. In addition, the Data Protection Act 2018, which creates GDPR compliance within the UK, both before and after Brexit, has not yet been passed by Parliament.

The following are areas practices will wish to have put into place:

Privacy Notices [Fair Processing Notices]

Practices should aim to have a privacy notice in their waiting area and on their website by 25th May: the LMC has sent template privacy notices to all practices which can be adapted by individual practices but there are others available in the links provided in the LMCs presentation, which are also available at the end of this letter. Practices should check the wording within these templates to ensure it applies to their individual circumstances. Practices can use the 'Direct Care' privacy notice as their primary notice but provide hard copies of the others (and a list) in waiting areas of the others, and a link to it and all other notices via their website.

The 'direct care' privacy notice can also be provided to any patients with their SAR [Subject Access Request] Report.

One key feature of any Privacy Notice is to identify the Data Protection Officer (DPO).

Data Protection Officer (DPO)

Unless your practice has independently commissioned a DPO, then at this stage, across the LMC Confederation, the LMC is suggesting practices designate one of their partners as their DPO. This is probably not the ideal long-term solution and the LMC is exploring possible options and encouraging CCGs (perhaps via the CSU) to identify and support a DPO function for member practices.

Local Medical Committees for
Croydon, Kingston & Richmond, Surrey,
East Sussex and West Sussex

The White House
18 Church Road
Leatherhead
Surrey KT22 8BB

T: 01372 389270
F: 01372 389271
www.sslmcs.co.uk

Special note for GP practices within Guildford and Waverley, North West Surrey and Surrey Downs CCGs; Surrey Heartlands has agreed to commission a DPO to support practices from SCWCSU as a part of its commitment to support local General Practice; the LMC welcomes this decision, which will be subject to review, involving the LMC, as the role and workload of the DPO post become clarified. The LMC is seeking a long-term solution for DPO support for practices as part of future GDPR compliance. Practices within these three CCGs may therefore if they wish designate SCWCSU (South, Central and West Commissioning Support Unit) as their DPO in their Privacy Notices, and further details will be available shortly

At present your practice can designate a partner or Senior Practice Manager, who may also concurrently be your Caldicott Guardian, as your DPO. This should be documented within a partnership meeting minutes or as a partnership decision.

As a DPO, you should:

- Be involved by your practice in relevant decisions
- Be supported by your practice in terms of training and updating
- Be accessible to Data Subjects (patients with queries about their data) who ask to contact the DPO
- Not be constrained or controlled by your practice in terms of your DPO role

In order to avoid potential conflicts of interest, the LMC would recommend any advice the DPO gives to the practice is minuted or made available to all partners and senior practice manager(s) and partnership decisions relating to IT, data management or processing are then separately made, minuted or circulated amongst all partners and appropriate managers (including the DPO) so that the two are seen to be distinct processes.

DPOs do not have to be experts in "international data protection law" in the context of acting as a DPO of an NHS GP Practice however, DPOs should, for example, read the BMA (and LMCs) guidance on GDPR and any information being provided to the practice via your CCG or CSU.

Single-handed partnerships are clearly in a more difficult position and it would be preferable for their DPO to be external to the practice, however, by the 25th May this may not be achievable, and this is an important issue to resolve.

Subject Access Requests (SARs)

After 25th May GP practices must follow a new process for managing any Subject Access Requests they receive; in summary:

- You cannot routinely charge for copies of the Data Subjects (patients) records
- When providing a SAR report, you should also provide a copy of the relevant Privacy Notice [which is likely to be the 'Direct Care' Privacy Notice]

- The SAR response must (in most circumstances) be within "one month" and it may be best to simply have a 28-day practice policy response time
- When responding to a SAR you can:
    - Agree to provide
    - Decline (this is not recommended, and you should consult your DPO if you believe you have a justification for doing so)
    - Ask for additional time, up to two months, which may be appropriate in some circumstances
    - Ask to negotiate, or clarify, the extent of the information required by the Data Subject (patient) under their SAR

GDPR allows the Data Controller to specify the information the SAR relates to, which may narrow the data that may be provided, however, the proviso is that Data Subject (patient) must agree to this voluntarily. This may mean the SAR is modified to, for example, only relate to information beyond a certain date, or, only to information relating to a specific procedure. Practices may therefore routinely wish to clarify with patients making a SAR whether they wish to include older, paper records, or if the SAR is really designed to obtain information from a certain date or about a particular aspect of their care, or illness. Practices should keep a written record of any changes to the SAR that are agreed with the patient.

Although there are now multiple points of view over charging for both copy SARs and any that are "unfounded or excessive" (terms that are not defined within the GDPR) at present the LMC would recommend practices are cautious in trying to charge: if the volume of work associated with a SAR is known to be significant, the LMC suggests trying to clarify the extent of the SAR first and negotiating this with the patient in terms of how much information is actually needed for what the Data Subject is seeking to establish. Clearly it is very unsatisfactory that such uncertainty exists at this point, but this is true for several GDPR issues.

Requests by Third Parties

Third parties such as solicitors, are allowed to request SARs on behalf of the Data Subject (patient) and the fact that a third party has requested a SAR does not of itself then mean a charge can be made.

Provision of SARs

You can agree the medium via which the information is provided and if the SAR is made electronically, it is presumed the response will also be electronic. However, you **are not** required to provide a SAR report on a USB stick, CD or via an encrypted message. You should however make an appropriate effort to ensure the Data Subject recipient email (or that of a third party on their behalf) is genuine; perhaps by sending a test or confirmatory initial email or confirming this by phone.

Requests from Solicitors, Insurers and Employers

As colleagues will be aware, some organisations tried to get around the Access to Medical Records Act by getting patients to request SARs which were then passed to insurers; however, if this occurs after 25th May, practices are recommended to clarify if any such requests should be more properly made under the Access to Medical Records Act (AMRA) which deals with reports for employment and insurance purposes. The Data Protection Act, when passed into law, will extend the offence of 'enforced subject access' to cover a situation in which a Data Subject is in effect being asked to provide a SAR when another process should be followed.

The LMC will provide a template letter to use if a third parties request appears unclear.

Record of Processing Activities (Data/Information Asset Register)

Practices should have started to prepare this data spreadsheet. There are a number of templates available via the links in this letter; the record must be accurate, and kept up to date, and include,

- The name and contact details of the Data Controller (DC)
- The name and contact details of the DCs Data Protection Officer (DPO)
- The purpose of the processing, this is a list of the purposes derived from the Privacy Notices
- The description of the data subjects [which will be patients, and employed or engaged staff] and categories of personal data
- A list of recipients to whom the personal data is disclosed; these represent your Data Processors,
- If such recipients are a third country [outside the EU] this will not apply to most practices, unless using remote dictation or equivalent.
- The time limits for erasures: for electronic records there are none, for paper records, this is under NHS England guidelines
- A general description of the practices technical and organisational security measures: this is not designed to be exhaustive and for all practices will include:
    - NHS supplied and maintained IT
    - GPSoC systems
    - N3 Network
    - NHS Smartcards
    - IT toolkit
    - GMC confidentiality guidance
    - Contracts of Employment
- Confirmation that information in the record of processing activity is maintained and can be accessed by the ICO (and a CQC Inspection may also require the same evidence of compliance)

In addition, practices should keep a record of any breaches, analogous to the record they would keep of a, for example, clinical or organisational significant incident/event.

In summary, by 25th May, all practices should:

- Have created and publicised Privacy Notices; however, there may be more such Notices in future
- Have designated a DPO
- Have a GDPR compliant policy in place to manage SARs, recognising further information will be required on managing these
- Have started to create a record of data processing activities.

There will clearly be further guidance to follow, and the LMC will highlight this when available.

With best wishes

Yours sincerely

Dr Julius Parker
Chief Executive

Useful Links:-

- IGA [Information Governance Alliance] Key points for GPs https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance
- BMA https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers
- Information Commissioner www.ico.org.uk
- Dr Paul Cundy (Chair of GPC IT Committee) Blogs at https://www.dropbox.com/sh/h22kak6pxlt8ily/AAB4gAuHKib_MZ44Xi3AbAf4a?dl=0