PENNINGTONS MANCHES

GPDF
General Practitioners Defence Fund

THE GENERAL DATA PROTECTION REGULATION: IMPLICATION FOR LOCAL MEDICAL COMMITTEES

From 25th May 2018 onwards, the EU's General Data Protection Regulation 2016/79 (the "GDPR") and the UK's Data Protection Act 1998 ("DPA 2018") will govern how Local Medical Committees ("LMCs") use personal data.

Although many of the principles and rules in the GDPR are similar to, or the same as, those in the Data Protection Act 1998, there are new rules which will require some changes in approach by LMCs as data controllers. This Briefing examines how the GDPR will impact on current practices of use of personal data, what LMCs will have to do differently and what will no longer be possible.

LMC Background: their statutory and non-statutory functions

In broad terms:

- LMCs are local committees representing the interests of GPs. The British Medical Association ("**BMA**") has also established a national committee to represent the combined interests of GPs; this committee is known as the General Practitioners Committee of the BMA ("**GPC**").

- The NHS Act 2006 (as amended by the Health and Social Care Act 2012) allows for the legal recognition of LMCs (see s.97 NHS Act 2006 and s.54 NHS (Wales) Act 2006), but this statutory footing does not extend to Scottish LMCs or to "umbrella" LMCs.

- LMCs' statutory functions are set out in the NHS Acts and subordinate legislation made under them. A core function of LMCs are to liaise with CCGs and the GPC as representatives of GPs' views and interests, together with pastoral support for GPs relating to health, complaints and regulatory investigation. LMCs are also empowered to investigate complaints made to them by a medical practitioner about another medical practitioner and to report on medical examinations undertaken in relation to a practitioner's capability to provide contracted services. Their non-statutory functions include the provision of information, advice, guidance and training to local GPs and their practices. Some LMCs, and their umbrella organisations, establish incorporated companies through which they provide their services to GPs.

- Members of LMCs are democratically elected by their represented constituents and are made up of practising GPs and practice staff elected by local GPs. LMCs may also have members who are trainees or colleagues from other professions such as nursing and practice management. Each LMC may appoint a chair, vice chair, treasury, secretary, or any

other officers and sub-committees. LMCs are funded through statutory and voluntary levies paid by local GPs. A nominee from each LMC makes up the membership of the GPDF.

LMCs uses of personal data

Following an audit of a sample of data provided by LMCs during June 2018 it would appear that:

- LMCs obtain, hold and use personal information about the GPs they represent and about staff members at GP practices. In general, this will consist of names, contact details, some information about the individual's employment and practice, gender, nationality, National Insurance numbers and bank/payment details. LMCs will also tend to hold information about issues that members may have raised or with which they have sought the LMC's help. LMCs may also hold, use and share personal data including special category data in connection with their statutory powers and obligations.

- All of the information described in the bullet point above is **personal data** for the purposes of GDPR legislation. Much of it (names, contact details, etc.) is of very low sensitivity. Other information (National Insurance and bank details for example, as well as records of issues discussed in confidence) is of a more sensitive nature in terms of its potential impact on the individual's privacy.

- There is, however, no standardised approach to the personal data collected by LMCs. It appears that some obtain information about members' ethnicity, medical history and (for some individuals) trade union (BMA) membership. Such data is **special category** personal data within the meaning of Article 9 GDPR, and thus attracts more stringent levels of protection.

- LMCs obtain the above data from the individual data subjects themselves, or from the practices at which they work, from relevant third parties or from public sources such as websites and directories.

Are LMCs public authorities for the purposes of the GDPR/DPA 2018?

Under data protection legislation (the GDPR and DPA 2018), this question matters for two reasons:

- One is that, by Article 37(1)(a) GDPR, a LMC must appoint a Data Protection Officer if it is a **public authority or public body**.

- The other is that, to some extent, the availability of the lawful processing conditions under Article 6(1) GDPR is shaped by whether or not the data controller (here, each LMC) is a public authority. Specifically, Article 6(1) provides that the legitimate interests condition (Article

6(1)(f)) "*shall not apply to processing carried out by public authorities in the performance of their tasks*".

We understand that LMCs therefore wish to know whether or not they are public authorities (or public bodies) for these purposes. **In our view, the answer is no**.

The GDPR does not define the terms "*public authority*" or "*public body*". Those definitions are left to Member States.

In the UK, the definition comes at s.7 DPA 2018:	
(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom —	(a) a public authority as defined by the Freedom of Information Act 2000,
	(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002, and
	(c) an authority or body specified or described by the Secretary of State in regulations, subject to subsections (2), (3) and (4).

Subsections (2), (3) and (4) are not relevant to whether or not a LMC is a public authority or public body.

The pivotal question is thus whether LMCs are public authorities for the purposes of the Freedom of Information Act 2000 ("**FOIA**") or its equivalent in Scotland ("**FOISA**").

FOIA defines "public authority" in s. 3 as follows:	
(a) subject to section 4(4), any body which, any other person who, or the holder of any office which —	(i) is listed in Schedule 1, or
	(ii) is designated by order under section 5, or
(b) a publicly-owned company as defined by section 6.	

LMCs do not fall within any of those limbs. Even the companies established by some LMCs do not fall within s. 6 FOIA, as they are not wholly owned by the Crown and/or "the wider public sector".

Exactly the same analysis applies under FOISA, yielding the same answers.

> In summary then, our view is that LMCs are not public authorities or public bodies for the purposes of data protection legislation. They are not caught by the qualification to the legitimate interests processing ground under Article 6(1)(f) GDPR and they do not have to appoint Data Protection Officers under Article 37 GDPR (for the avoidance of doubt, our view is that LMCs are not caught by any of the limbs of Article 37(1)).

What is the legal basis for processing personal data?

A key GDPR principle is to process information "*lawfully*". A data controller such as a LMC must be able to justify everything it does with personal data (obtaining, holding, using, sharing, etc.) by reference to one or more of the conditions from Article 6(1) GDPR. The GDPR sets out **six lawful bases for processing personal data**. Unless an exemption applies, **at least one of these will apply in all cases**. It is possible for more than one to apply at the same time.

There are processing conditions that apply to the processing of personal data and an additional set of conditions that apply to processing of special categories of data.

Article 6(1) GDPR provides that:	
Processing shall be lawful only if and to the extent that at least one of the following applies:	(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) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.	

Consent

- A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action.

Contractual necessity

- Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

Compliance with legal obligation

- Personal data may be processed if the controller is legally required to perform such processing (e.g. reporting of race or ethnic origin or gender pay data).

Vital interests

- Personal data may be processed to protect the 'vital interests' of the data subject (e.g. in a life or death situation, it is permissible to use a person's medical or emergency contact information without their consent).

Public interest

- Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest. This includes the exercise of official authority vested in the controller. Such authority could come from an Act of Parliament (e.g. the National Health Service Act 2006) or a statutory instrument made under it.

Legitimate interests

- This involves a balancing test between the controller (or a third party's) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

The balancing test for legitimate interest: Identify your legitimate interest

- What is the purpose of the processing and why is it important?;
- Carry out a necessity test;

- Is there another way of achieving your legitimate interest? If the answer is no, then it is necessary;
- Carry out a balancing test;
- Does the data subject's right override the legitimate interest?;
- Consider the nature of the processing, its impact and what mitigation you can put in place; and
- What possible negative impacts for privacy could there be.

What lawful processing conditions are available to LMCs?

- A LMC is a membership and representative body. It obtains and holds the personal data of GPs and others working at GP practices in their area primarily so that it can communicate with them to provide them with information and seek their views, and so that it can arrange payment for members for certain tasks.
- Following an audit of a sample of data provided by LMCs during June 2018 we understand that some LMCs have sought members' consent for certain activities, such as for contacting them by email. In the main, however, LMCs do not seem to us to work on a consent-based processing model in practice – nor is consent the appropriate condition for most of what they do. To the extent that LMCs send electronic communications (emails and text messages) for the purposes of "direct marketing", they should obtain recipients' consent to avoid falling foul of the Privacy and Electronic Communications Regulations 2003. **If a LMC wishes to disclose specific information about a particular member's situation because of a case-specific problem, it should seek the member's consent.** Otherwise, however, LMCs do not seem to us to be suited to a consent-based processing model. Article 6(1)(a) GDPR will thus not be applicable to the bulk of the processing done by LMCs.
- As we understand it, LMCs do not have contracts with the individuals whose personal data they process. Article 6(1)(b) does not therefore apply here.
- Article 6(1)(c) could apply to some of LMCs' processing: s.97 of the NHS Act 2006 **allows** for formal recognition of LMCs, and it **requires** LMCs so recognised to make arrangements for determining and collecting levies from members. In order to discharge that duty, a LMC needs to know which persons it represents, and it needs some information about their practices. Once an LMC is recognised, it acquires legal obligations and/or statutory powers pursuant to the NHS Act 2006 and subordinate legislation made under it. Where the LMC is

obliged to undertake specific tasks that involve the processing of personal data, the lawful basis will be that the LMC is complying with its legal obligations. Where the LMC exercises powers, then the correct lawful basis is Article 6(1)(e) (see below).

- Article 6(1)(d) (vital interests) does not apply here.

- The **majority** of the processing of personal data undertaken by LMCs can be justified by reference to Articles 6(1)(e) (**processing necessary for the performance of a task carried out in the public interest or the exercise of official authority**) or 6(1)(f) (**legitimate interests**).

- In order to rely on the former, a LMC does not need to be a public authority – it simply needs to carry out tasks in the public interest. Our view is that LMCs' core representative functions fall within that description, certainly insofar as they are established under s.97 of the NHS Act 2006. LMCs and related companies that have no statutory footing may not be able to rely on Article 6(1)(e), because Article 6(3) requires that the *"basis for the processing…shall be laid down by Union law or Member State law"*. S.97 of the NHS Act 2006 probably does constitute a basis for processing as laid down by law, but where that section is inapplicable, Article 6(1)(e) cannot be relied upon.

- More broadly, however, our view is that LMCs **can and should rely on their legitimate interests and those of the members they represent** to justify why they obtain, hold and use personal data. We see no barrier to their reliance on Article 6(1)(f) GDPR.

- As noted above, it appears that some LMCs may collect special category personal data for purposes other than the exercise of official authority vested in the LMC. It is not clear to us why they do so, and indeed we recommend that this question (do you hold special category data, and if so why?) be addressed by all LMCs. If there is no clear answer to why such data is held, it should be securely deleted.

- Where LMCs do need to collect **special category data**, this must be justified not only under **Article 6(1)** GDPR (see discussion above) but also **Article 9(2)**. (Note, these conditions are additional (not alternatives) to relying on a condition for processing personal data.)

Article 9(2) GDPR provides that:
Paragraph 1 shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) 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;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- The best basis for LMCs' use of special category data will generally be the **explicit consent of the data subjects** (Article 9(2)(a) GDPR).

- Article 9(2)(d) GDPR could apply to limited types of processing. That condition is met where:
  "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects".

- Applying this to the example of a LMC assisting a member in defending himself in fitness to practice proceedings which might involve information about the member's health, including (to take an example) alcoholism or misuse of alcohol that is sufficiently serious as to constitute information as to the member's health. The member's consent would be required in order to share special category outside the LMC in such circumstances.

- Article 9(2)(f) applies to processing of special category data that it is necessary in connection with legal claims. This could be relevant to supporting a GP in relation to an allegation of negligence where consideration needs to be given to medical information about the complainant (i.e. the patient's special category data rather than the GP's). Care should be taken in relation to the necessity of the processing – if it is not necessary to identify the patient in order to support the GP, then Article 9(2)(f) may not be available.

- Article 9(2)(g) is potentially available to LMCs exercising official authority, e.g. in cases where special category data must be shared irrespective of the consent of the data subject. Whether this or an alternative Article 9 condition is available will depend upon the exact nature of the statutory authority and whether the LMC is obliged (i.e. complying with legal obligations) or empowered (i.e. exercising discretion) to undertake the prescribed processing.

Could Article 9(2)(d) GDPR be relied upon to process such data for such purposes?

"Can you act "with a trade union aim" and not be a trade union?" As a matter of statutory language, we think the answer is yes. If a LMC is comfortable asserting that, in assisting members with such regulatory proceedings, it is acting with a trade union aim, then our view is that this condition would be available. LMCs should however, question its utility: in such a case, the special category data (for example about the member's alcoholism) may need to be shared externally (for example, with the General Medical Council or the panel tasked with the proceedings), in which case the member's consent would be required anyway.

Our overall view is therefore that the LMCs should take the approach of seeking members' explicit consent for obtaining and using any special category data that, upon consideration, they feel they need.

For completeness, the only other conditions that could conceivably apply are conditions 8 (monitoring equality of opportunity) or 9 (monitoring ethnic diversity) from Schedule 1 DPA 2018, if the LMCs are in fact engaged in activities within those provisions – but it is not clear to us that they are.

PENNINGTONS MANCHES

GPDF
General Practitioners Defence Fund

GDPR 10-POINT PLAN – PRACTICAL STEPS BY LMCs TOWARDS COMPLIANCE WITH DATA PROTECTION LEGISLATION

Step 1:

Data audit: Each LMC should undertake a data "audit" which would involve it reviewing and documenting what personal data it holds (which data subjects (including members, volunteers), what items of personal data), what it uses that data for and how old it is (including whether it is still needed for use). The outputs of this audit will help LMCs plan for compliance, and will also form the bedrock of the "records of processing activities" they are likely to need to draw up under Article 30 GDPR.

Step 2:

Cleansing: LMCs should "cleanse" their systems and records so as to securely delete information for which they no longer have a need (see in particular our query about why some LMCs collect special category personal data). This will entail deciding on an appropriate retention period for personal data.

Step 3:

Update policies & notices:

Privacy notice: Each LMC will need to be content with and commit to the contents of a privacy notice that complies with Articles 13 and 14 GDPR. To this end, LMCs must always tell people in a concise, easy to understand way how it intends to use their data, how long it will keep data for and what lawful basis it has to process personal data. It will then need to "provide" that information to data subjects. This can be done on each LMC's website (if it has one), by email and/or in other correspondence with data subjects.

As regards GP practices, the LMC could either write to/email each individual about whom it holds personal data, or contact the practice and ask it to ensure that the LMC's privacy notice is disseminated or provide the notice on the LMC's website. (Please see our sample privacy notice in respect of represented GPs at Appendix 1.)

Data retention & disposal: LMCs should ensure that it updates its data retention policy and informs all data subjects how long it will retain data. When disposing of records and equipment, LMCs should make sure that personal data cannot be retrieved from them.

Step 4:

Data security arrangements: LMCs should review their data security arrangements so as to accord with Articles 24 and 32 GDPR in particular. This should encompass not only the technical (IT) aspects such as computer systems, encryption, passwords, and access and so on, but also hard-copy material and human resources measures (implementing procedures as to who has access to what material).

Step 5:

Staff training: Those who work for LMCs should be given training about data protection issues, data security and what can and cannot be done with personal data.

Step 6:

Data subjects' rights: LMCs should have procedures in place for acting on requests by data subjects to exercise their rights under the GDPR, including (most notably) subject access requests and erasure requests (see Articles 15-21 GDPR).

Step 7:

Data breach: LMCs should have a procedure in place for what to do in the event of a data breach. A data breach is a breach of security leading to "*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*". All staff should know who to report the matter to within the LMC, and that central point of contact should know what steps to take to mitigate the problem. The GDPR introduces a duty to report certain types of data breaches to the ICO within 72 hours and in some cases to the individuals concerned.

Examples of personal data breaches and steps to avoid them include:

- Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient.
- The wrong people being copied in to emails and attachments – use BCC (Blind Carbon Copy) where necessary.
- Lost memory sticks – LMCs should put protocols in place for memory stick usage.
- Malware (IT) attack – ensure up to date anti-virus software is in place.
- Equipment theft – check security provisions.

Step 8:

Data processors: LMCs should review any use they make of the services of data processors, i.e. any external person or party that processes personal data on the LMC's behalf. Examples could include IT service providers, payment service providers and document storage companies. LMCs will need to have contracts in place with data processors that comply with Article 28 GDPR.

If a LMC shares personal data with any third party, it should review that data-sharing arrangement. It should interrogate the justification for and extent of the data-sharing, and seek to document an information-sharing agreement that binds the recipient to using personal data only for specified purposes. (Please see our sample data processing agreement at Appendix 2.)

Step 9:

Build data protection into your new projects: Privacy by design means building data protection into all your new projects and services. It has always been good practice, but the GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large

scale. LMCs should clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them.

Step 10:

Accountability: LMCs should keep audit trails and records of the work they have done towards data protection compliance. This will be important in discharging their "*accountability*" duty under Article 5(2) GDPR, i.e. the duty to demonstrate how they comply.

Steps a LMC can recommend to GP practices

The 10-point plan set out above would apply equally to GP practices and could be recommended by LMCs to help GP practices work towards compliance with data protection legislation. Steps 3-10 above can be readily applied to GP practices.

Steps 1-2 (data audit and cleansing) are less straightforward for GP practices, given the amount of patient data they hold and the legal and regulatory requirements that apply to patient data. For a GP practice, step 1 above (data audit) can be carried out at a high level (e.g. patient records on computer systems; patient records in paper files; employee records, and so on) and step 2 (cleansing) probably needs little attention as regards patient data, the retention of which is governed by bespoke legislation and guidance that is unaffected by the introduction of the GDPR and DPA 2018.

With accommodation for those features of GP practices, the 10-point plan outlined above would apply equally as guidance to help GP practices work towards full compliance with data protection legislation.

We hope that this Advice assists LMCs in understanding and preparing to discharge their duties under the GDPR and DPA 2018 and in helping GP practices do so.

PENNINGTONS MANCHES LLP