Blog 3

GDPR FOR GPs, THE DATA PROTECTION MEGABLOG

So far blogs 1[1] and 2[2] have been pretty low brow, gentle entrées before the main course, well feast your eyes on this. The powers that be advise a blog should be 5 to 600 words, this is a behemoth by comparison, putting DPOs under the spotlight in literally 4KHD (4 thousand words heavy in detail). Written by a GP for GPs.

Data Protection Officer

One of the new things that's causing a good deal of anguish in GP Land is the Data Protection Officer. These are brand new and shiny and never been played with before so it's a bit of an open book. Some of the words in the book are finalised and clear, the ink is dry, but others might need correcting and some of the pages haven't been written yet. Let's open the cover and see what we find……

What is a Data Protection Officer (DPO)?

A DPO a person who advises the DC (Data Controller) about GDPR and who acts as a point of contact for DSs (Data Subjects) and the ICO. They are legal entities who have their own rights and responsibilities. These are set out in Articles 37 to 39 of the GDPR[3]. The best way to think of a DPO is that they are the GDPR equivalent of the practice's CQC Registered Manager. The DPO is there to advise upon and as far as is possible, ensure compliance with GDPR and to protect the data the practice holds (note the absence of the word patient, its all the data, not just patient data). DPOs will have some statutory responsibilities to liaise and report but they have no statutory rights to mandate changes within their organisations, they advise, the DCs decide whether to accept their advice or not, DPOs are not directly regulatory.

We are an NHS Practice; do we have to have one?

Yes. Full stop, period, end off, talk to the hand, move on, but I'm feeling generous so here's the logic. There are three criteria that trigger needing a DPO;

Criteria one, Article 37(1)(a)[3], if you are a Public Authority you must have one. All NHS contract holding general practices are public authorities, by law, therefore every NHS contract holding practice must have one, Full stop, period, end off, talk to the hand, no debate, no argument, move on to the question 10

But I'm not an NHS contract holding GP, what do I do?

You move to criteria two Article 37(1)(b); if your core activity and purpose means you regularly and systematically monitor and process data of DSs and do so "on a large scale", you need a DPO. The core work of a GP is to provide reactive care, responding to those who believe themselves to be or who actually are (I know rare these days but it does happen) ill. This is not regular and systematic monitoring. Remember that GDPR is a refresh to account for the darker side of the wonders of modern social media, this clause, Article 37(1)(b) is there to deal with the Facebooks and Amazons. This clause does not apply to GPs because you are not "regularly and systematically monitoring" your patients". See later.

OK I'm not an NHS contract holding GP, and I'm not regularly and systematically spying on my patients, what do I do?

You test yourself against the third criteria requires a DPO, Article 37(1)(c), do you 1) process both Article 9 and Article 10 data and 2) do it "on a large scale"? Shortcut to an answer, Article 10 data relates to crimes and convictions and this third criteria as worded requires both Article 9 AND (i.e. Plus) Article 10 data so I'm guessing there are no GPs in the UK to whom this will apply, in fact almost no one in the entirety of the NHS could possibly be caught by this clause.

That's clear but if only it were that simple.

Hmm but there might be a problem. The wording of Article 37(1)(c) is quite clear and explicit, the word "and" links Article 9 special category data, i.e. patient records with Article 10 data, crimes and convictions. So as written the law is quite clear and unequivocal, both conditions have to be satisfied, if it's not both categories the clause does not apply. Unfortunately, someone somewhere realised this might be an unhelpful

conditionality and they've written guidance that the word "and" should in fact be read to mean "or"[4]. Hmm there's a quandary, the law says one thing on the tin, but the law writers want it to mean another.

What's your take on this Paul?

My take is, thank heavens I'm only a GP but lets err on the side of caution and assume Article 37(1)(c) doesn't mean what it actually says but what our expert EU international data security and protection law draughtsmen meant it to say, i.e. that it can apply when special category data alone is being processed. That means it would apply to a DC processing patient data alone, however the "on a large scale" condition still applies.

Q94 So, what's "on a large scale"?

See above, GDPR is about controlling the excesses of our digital world. It applies to any EU citizen and any DC or DS handling any data on any EU citizen no matter where on the planet that DC or DS is based. GDPR is not a meek timid piece of legislation dealing with a niche area of minority interest. "On a large scale" in the context of GDPR has got to mean at least big, enormous, mega, massive and involving terabytes plus of data being churned in climate-controlled warehouses filled with servers.

Q94 cont'd Has anyone defined "on a large scale"?

No and inevitably it will have to be seen in context, GDPR makes it clear that the nature and type of the data plays into what is meant by "on a large scale". The complex, comprehensive, intimately detailed, highly sensitive, multi contributor, multimedia, lifelong medical records of our patients need to be given greater weight than other types of data so "on a large scale" in terms of medical records probably means less than mega enormous but probably at least locality or area wide, think in terms of the ultra-fashionable "working at scale" groupings. Two examples specifically quoted in GDPR guidance[5] are the processing of data by a hospital (large scale) vs the sole professional practitioner (not large scale, even when accumulated over a lifetime). So, going for my second over the parapet medal, and given that the GDPR guidance is expecting these things to be established over time through standard practice and the developments of codes of conduct, I'm going to suggest that anything less than 100,000 GP patients is not "large scale".

So, a single handed solely private GP does not need a DPO?

Correct. They will never need a DPO[6].

So, a group of GPs working privately with, say 10,000 patients wouldn't need a DPO.

In my opinion, correct. Iniquitous isn't it, NHS GPs of any size have to have one, private ones not. Mind you I suppose we are being funded from the public purse.

What if I'm an OOH organisation?

If you are not a public authority 37(1)(a) will not apply. Can 37(1)(b) apply? The first threshold is if you are routinely and systematically processing data on those you serve, so what's "regular and systematic monitoring". Well its specifically doing things that are; ongoing or occurring at intervals for a particular period, recurring or repeated at fixed times, constantly or periodically taking place and as to 'systematic'; occurring system wide, pre-arranged, organised or methodical, occurring as part of a general plan or carried out as part of a strategy. It seems clear to me that a traditional GP OOH won't ever fall foul of that. Move on to 37(1)(c), and by that, I mean what its meant to mean rather than what it actually says, well there's no doubt OOH organisations are handling Article 9 special category data, but it is it "on a large scale"? Applying the Q94 criteria above I'd argue you'd have to be "hospital" sized or above before having to have a DPO. Furthermore, OOH records are not as comprehensive nor as complex nor continuous as hospital records so would it be reasonable to suggest "on a large scale" for an OOH organisation is regional? I think so.

But I'm not a traditional GP OOH service, I'm a new-fangled app-based GP in your pocket type Skype service, do I need a DPO?

If you're collecting the sort of stuff most apps collect, then yes, because you are spying on your patients.

I'm an LMC, do I need a DPO?

Most of the data you hold will be personal non-special category data but if you support GPs in complaints, investigations, fitness to practice, health and pastoral roles this will be sensitive data under GDPR. However, there are very few LMCs with more than 1,000 constituents and thus I'd argue you are not mandated by the act to have a DPO.

But I'm a regional LMC, we don't think we need a DPO?

If you are not a public authority and you're not spying on your patients then Article 37(1)(c) is the one that might catch you out; processing large quantities of data. Given there is no definition of "on a large scale" until there's been a determination by the ICO under the new law or a courts case it's all a matter of opinion. In my opinion only the largest regional LMCs are going to be anywhere near mandatory DPO designation. If you decide under 37(1)(c) you do not need a DPO, then document the decision-making process and proceed.

But I'm a regional LMC and or a mega OOH, we think we need a DPO?

See the next question.

Can I have a DPO if I want one?

Yes, Whilst the GDPR mandates certain condition where you must have a DPO it does not preclude your voluntarily having one if you feel that's a good thing to do. So, if I were a large regional LMC with thousands of constituents I'd probably want to have one, similarly if I were a multi-region OOH. A locality group or federation? Probably not. An STP or ACO, yes but you're mandated to have one anyway. Remember having a DPO does not mean having to employ an expensive international expert full time. A part time DPO might be just the ticket.

If we can designate a DPO voluntarily, would they need to be permanently retained?

Well another good question. Given that a DPO can be designated because an organisation would like to have one, rather than having to have one to comply with the law, it seems reasonable that the need to have one may vary in time and circumstance, so I think having a DPO that you can dip in and out of would be fine.

Q10, what does a DPO do?

Under GDPR they have some statutory responsibilities and protections. The roles of the DPO are laid out in Article 38 and a summarised as being at least;

To pre-emptively inform and advise DCs, DPs and their staff

To provide advice to the DCs when requested, in particular for any Data Protection Impact Assessments (DPIA).

To act as the contact for data subjects

To act as the contact for, and co-operate with, the ICO when necessary

Q11 what does the DC have to do for the DPO?

The DC must provide an environment in which the DPO can operate independently and without limitation. The GDPR sets out these requirements in Article 39. Briefly they are;

To involve the DPO in all relevant issues

Provide support and resources for them to carry out the tasks listed in question 10 above, including training and knowledge updating.

Not issue the DPO with any instructions or place any constraints relating to their DPO role.

Allow data subjects to access the DPO

Not allow the DPO to be conflicted by other tasks, jobs or responsibilities that they may have. This includes other tasks, jobs or responsibilities outside your organisation, practice or body, such as might apply to shared DPOs or part time workers.

Who can be a DPO?

Anyone can be a DPO. They can be internal to the practice or external, an employee or a contractor or contracted for as a service. The legal requirement is that the practice must "designate" a DPO, as opposed to appointing one. A DPO could be for instance from; your CCG or PCO, your LMC, your federation, your locality group, an interested individual, a patient, a member of your PPG, a company or any other third party.

OK I'm a small to medium sized practice but don't want to have our own DPO, can we share a DPO?

Yes, DPOs can be joint or shared. A DPO can act for both groups of DCs as well as independently for others.

Could my LMC provide an area wide DPO?

Yes

Could the BMA provide a DPO for us all?

Yes. DPOs may "act for such associations and other bodies representing controllers or processors". Article 37 clause 4 appears make it possible that the BMA could provide a DPO for all the practices in the country. Interesting.

Does every DPO need to be an "expert in data protection law"?

No.

Err that's not what we've been told.

Told by whom? The GDPR Working party is being quoted as saying that DPOs must be experts in international data protection law and this is being touted widely by companies wanting to flog you their DPO services. As per my comments above, GDPR will apply to companies like Facebook, Apple and Google as well as the smallest NHS surgery, in other words everything between mega enormous and street corner. The working party's guidance has thus to cater for this broad spectrum. It is nonsensical to imagine there being 10,000 experts in international data protection law ready and available for designation by UK general practices. There's a distinction between being an expert and having access to expert knowledge. So, lets dissect what GDPR actually says about this expert knowledge. Clause 97 states that in relation to the DPO; "…a person with expert knowledge of data protection law and practices should assist the controller" it then continues in the same clause with "The ***necessary level of expert knowledge……".*** So GDPR accepts that there will be different levels of "expert knowledge" needed according to the sort of processing being done, some will need more expert knowledge than others. Article 37 clause 5 is what the scaremongers are touting; "The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39." When they do read them back this[7], taken verbatim from GDPR guidance, "The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation". So, take as an example a company that processed data gleaned from social media, analysed it and then sent it abroad for use in foreign political campaigns, would they want to have an expert DPO?

Finally, if the ICO is happy for partner GPs to be DPOs (see next question) they are clearly not imagining that each one is going to be a national expert.

In short GPs do not need to seek out national experts to be their DPOs and any “expert” who says they do is clearly not. What GDPR does specify are their roles and their rights, see Q10 and Q11 above.

Can a partner be a DPO?

Yes. There is nothing in the GDPR that says a partner in an NHS practice cannot be a DPO. People worry about conflict, GDPR does not allow a DPO to be conflicted, i.e. they cannot be a directly controlling the data processing and a DPO at the same time, and for obvious reasons. This might be misinterpreted to mean a partner, who on the face of it is a data controller, cannot also be a DPO. This is incorrect because for an NHS general practice it is the practice, the partnership, the organisation, the entity, the legal body, that is the data controller, not any individual doctor within it. A partner in a practice might be thought of as being an internal data processor; no individual partner (in a partnership of more than one) can be the data controller for the entire practice because they cannot singlehandedly control all the processing occurring in it. Legally it is the practice that registers with the ICO as the DC. In addition, GPs are required by a variety of other laws as well as the common law of confidentiality to have a default position of protecting their patient’s records, which is what GDPR is all about, so the two roles are aligned anyway. Finally, the DPO role is advisory and except for reporting rarely requires action that would conflict with a partnership role, indeed being found lacking as a DPO, if you were also a partner, would breach the usual “to not bring into disrepute” clauses found in partnership agreements. The ICO has confirmed the above with GPC and advised that providing the reasons for such a decision being made are properly documented then there should be no problem.

So, a partner can be our DPO and they don’t have to be an expert in international law?

Correct. They will however need to bone up on GDPR.

What about singlehanded GPs holding NHS contracts?

We’ve seen that singlehanded non-NHS GPs don’t need to have DPOs. Singlehanded NHS contract holding GPs by virtue of their being Public authorities must have a DPO, but they are unlikely to need a full time DPO. Although the argument may be less appealing it is still the case for a singlehanded NHS contract holding practice it is the practice, not the individual GP that is the DC. So for all the same reasons they could also be the DPO. However can you imagine the difficulty trying to persuade any convinced committed conspiracy theorist that a singlehanded GP DPO was acting independently and impartialy, I’m thinking sharing a DPO with others might be a better and more transparent option?

Would you recommend a partner being the DPO?

Yes. GDPR is meant to be pragmatic and is being introduced to provide controls for our new social media dominated world. The original directive was written when medical records were a known issue, so GDPR is not intended to add to the bureaucracy of protecting medical records. The last thing the profession needs is another regulatory burden being introduced and as the guidance says “The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation“. Healthcare is a complex area in terms of data rights. A working knowledge of how it works will be essential, hence a person with inside knowledge is likely to be more appropriate than any external applicant. Think of pensions, how many FCAs are conversant with the NHS Pension scheme?

In my opinion a partner is ideally placed to be DPO but a senior practice manager would be equally suitable.

Why is it best if they are internal?

Obviously, it depends very much on where you are and what capacity you have but a well organised practice happy with its understanding of the current DPA could probably easily and reasonably designate its own internal DPO. Larger groupings such as federations and those ultra-fashionable working at scale setups are likely to want to provide their own corporate DPO, but again it’s probably best if they are internal.

Can a CCG provide a DPO?

Yes. GPC has agreed with NHSE and its now official; CCGs are required under the revised GP IT Operating Framework to provide, directly or via their IT provider service, a DPO support function (i.e

training, documentation etc). They may also provide an actual DPO, but these are at present not going to be free to practices. The Practice CCG agreement will need to be amended to reflect this. There is a clear precedent that the NHS should pay for GP's DPO costs in exactly the same way that CQC registration fees are re-imbursed. The GPC has submitted as part of this year's DDRB evidence a request that GDPR costs be considered.

Who else can provide a DPO?

Basically anyone.

Do we have to accept everything the DPO advises?

No. the DPO role is advisory so a DC could decide to act differently or even against the advice of their DPO.

So, when might we go against a DPO's advice?

Well, purely speculatively, for instance a CCG or Federation appointed DPO may be pushing for all local practices to be on one common clinical system, this is rarely necessary, causes massive disruption and in the long term unhelpful, a practice would be wise to think very carefully about accepting such advice without challenge.

And so, if our DPO advises something we aren't sure about, can we seek other advice as well?

Yes of course, and as described above sometimes that may be a very sensible path to take, think of it as a second opinion.

If we do go against a DPO's advice, what next?

Well not necessarily anything. Their roles are mostly advisory. However, if a practice did decide to go against the advice of their DPO they would be wise to comprehensively record and thoroughly document their reasons for doing so[8]. The wording of the guidance reads; "The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice." Additionally the DPO must have the right to report and register their advice and opinions at the highest level in the organisation, so that means partnership or management board level.

And remember……

Currently and as drafted, any communications between an entity and its DPO are NOT subject to legal privilege, unlike, for instance the discussions between a barrister and his paedophile client. So, anything you say, send or exchange with or any instruction you give your DPO could be demanded and disclosed to the ICO and a court.

How busy are DPOs likely to be?

It is likely that for UK general practices there will be an initial period during which compliance with GDPR is established, implemented and confirmed. This is likely to take a few months. The GPC will be providing as much generic template material as is feasible to make this process as streamlined as possible. Once compliance has been established unless there are new data processes being established it is not thought that the DPO role will be terrible busy. Responding to requests from DSs will of course be an unknown.

I've been designated my practice's DPO, am I personally liable for anything?

No. That is providing you don't wilfully defy the law or knowingly gave incorrect advice.

I've been designated my practice's DPO, should I have protected time for the role?

Yes.

I've been designated my practice's DPO, should I be get training?

Both training and updating.

Where can I get training?

There's likely to be a mini south sea bubble of GDPR training days, modules, webinars and courses. However, I'd get fully acquainted with everything available on the web first, you may not need to shell out those hard earned QUOF pounds just yet. I'll be pointing to what I think are the best on-line resources in my next but one blog so you'll have plenty of time to spare. Remember the ICO does not expect every practice to be fully 100% up to speed with every detail in place by 25th May. The same applies to DPOs, see my comments on "experts" above.

I'm my practice's Caldicott Guardian, can I also be our DPO?

If you know what a Caldicott Guardian is you've passed the interview already! There's no reason why the two roles can't be incorporated, indeed they lie together like two peas in a pod. I'm going to be both.

Can we change our DPO?

Looks like no one's thought of that. Depends on whether yours is mandated or voluntary. If mandated under Article 37 all GDPR requires is that you have a DPO, therefore it must be possible to change one, but there clearly must be no gaps or time during which you don't have one. I assume a departing DPO will be granted unfettered communication with the new DPO and vice versa. If you change your mandatory DPO, it would have to be for reasons unrelated to their activity as your DPO. If you voluntarily designated a DPO thinking is was a good idea you could just as easily decide it's no longer such a good idea and de-designate them.

Can we sack our DPO?

Depends on what they've done. If manifestly incompetent or for instance, in cases of theft, physical, psychological or sexual harassment or gross misconduct, yes. Similarly if they had knowingly acted in contempt of GDPR and DS privacy, otherwise, No.

A DPO cannot be removed, replaced, sacked or in any other way terminated just because you don't like the advice they are giving, the words from the GDPR are; "He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.". This would apply to both mandated and voluntary DPOs.

So why don't we just find a compliant DPO and relax?

Because it's you the DC who's accountable. You may find a very pliable DPO who plays the game but if you fall foul of the ICO its you that suffer the convictions and fines. There is a defence under GDPR of deciding to not follow the advice of your DPO, providing you've got reasonable grounds for doing so, but there is no defence for following incorrect advice. If the DPO acted knowingly in contravention of GDPR they also will be liable.

Can our DPO liaise with other DPOs?

I see no reason why a DPO should not liaise and seek advice or exchange views and policies with other DPOs. This would be part of their role. However, the DPO will know that the data of their host organisation are confidential.

Will DPOs need to be appraised in that role?

Yes.

What will DPOs cost?

No idea. This blog, for what its worth, is free, please plagiarise. There are likely to be (correction, there are already) many companies offering DPO facilities to GPs so a market will operate. Its likely they will want to charge several thousand £s per year. I would advise very strongly looking at all the potential options from within the "NHS family" before contracting with any external company, given some of the scaremongering codswallop they are pedalling. If a practice did decide to use a third party it would be essential to clarify the liabilities if the ICO ever decided to fine the practice. If the DPO service offered by the 3rd party were implicated the practice might want to seek recompense from them.

As a sessional or salaried doctor do I need a DPO?

No. You do not need a DPO. However, the data you hold on your "suppliers" (the practice(s) that employ(s) you) are subject to GDPR and must be protected accordingly.

As a sessional or salaried doctor's chambers do we need a DPO?

Based on the "on a large scale" definitions even a large chambers won't need a DPO. However, if they hold other information such as informal feedback from members, which might identify practices or individuals then although a DPO is not mandated they might want to have access to a DPO's advice. Just as for each individual member any data they do hold on their members and suppliers would have to be protected according to GDPR rules.

Dr Paul Cundy

GMC 2582641

28th March 2018

1 https://www.bma.org.uk/connecting-doctors/the_practice/b/weblog/posts/gdpr-for-gps-from-the-it-lead-for-gpc

2 https://www.bma.org.uk/connecting-doctors/the_practice/b/weblog/posts/gdpr-part-two-the-story-continues

3 https://gdpr-info.eu/art-37-gdpr/ , https://gdpr-info.eu/art-38-gdpr/ and https://gdpr-info.eu/art-39-gdpr/

4 http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 page 9, para 2.1.5

5 http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 page 8, 5th bullet point.

6 http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 page 8, 11th bullet point.

7 http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 section 2.5, page 11.

8 http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 page 14, second bullet point.