

Dr Katie Bramell-Stainer, Chair GPC England
Dr Mark Coley, GPC IT Policy Lead
All LMCs in England
All GPs in England

13th November 2023

An open letter to the profession

Dear Katie,

New regulations create “opt-in” for prospective access for some practices. Incorrect advice from NHS England.

I am writing to you and all GPs because of an e-mail my practice received from NHS England regarding prospective record access (attached as NHEmail.PDF). We have been repeatedly targeted because we have not yet enabled access. I have concerns about it, in my opinion it is hectoring and bullying, with threats of massive additional work for practices if they do not comply. Additionally, it has clearly been drafted with no understanding of (or ignoring?) the actual wording of the newly introduced regulations and it has several factual inaccuracies. My main concern is that it is inviting practices to break the law. However, it has one unintended benefit for some practices; rather than being forced to provide prospective access for all, they will be bound by regulation to operate an “opt-in” process.

As we know under the Data Protection Act 2018 (DPA18) before a Data Controller can introduce any new processing, they must complete a Data Privacy Impact Assessment (DPIA), to gauge to what extent the arrangement would put the data and or data subjects at risk. This is a legal requirement that has been made explicitly clear by the Information Commissioner on this very subject³. The degree of risk is assessed by considering the volume of the data and or its sensitivity. If that risk assessment reaches a threshold of high risk, there is a further legal requirement that the Data Controller must submit its DPIA to the Office of the Information Commissioner (OIC) so that they may either approve it or make suggestions for changes. Whether or not the Data Controller submits it's DPIA to the OIC the legal position is that the Data Controller **MUST NOT** allow the new processing to begin until the DPIA process has been successfully completed.

In your recently revised advice and guidance on this subject you emphasise the need to complete the DPAI process¹.

It is difficult to imagine that implementing prospective access to all a practice's patients personal medical records and limited access to some retrospective medical records could ever be considered to not be high risk.

If practices were to allow prospective access without completing a DPIA process they would be in breach of DPA18. Given the fines levied by the OIC in the past in relation to just a

single patient record, the potential sums would be alarming. However, the e-mail from NHS England makes no mention of this absolute legal requirement, despite its opening paragraph; "Access should only be withheld if it would not be provided under GDPR" As reasoned above the absence of a completed DPIA means access cannot be allowed under GDPR (Data Protection Act 2018).

By inviting practices to provide access without completing a DPIA means NHS England is inviting GP Data Controllers to break the law.

If a practice breaks the law, they also by default breach their GMS/PMS/APMS contract, which requires the contract holders to comply with all external laws.

I am sure this is a point that you would want to emphasise and take up with NHS England directly.

The next aspect of NHS England's mail is this statement.

"An 'opt-in' approach does not meet the contractual obligation (GMS, PMS and APMS) that requires all practices to provide each of their patients with online access to their prospective medical record by 31st October 2023."

This is the most worrying of their comments. It demonstrates a complete misunderstanding of their own regulations. In fact, the position is quite the opposite, far from not meeting contractual obligations an "opt in" is fully contractually compliant for some practices.

I shall explain. Like many other practices we did not allow access and bulk coded 104 prior to 31/10/23.

That means we are caught by paragraph 16.5ZA.7 of the new regulations. It reads:

16.5ZA.7 Where:

(a) the Contractor has not, before 1 November 2023, for whatever reason, provided P (the patient) with the facility to access online P's prospective medical record;

and

(b) P makes a request in writing to the Contractor on or after 31 October 2023 to be provided with that facility; the Contractor must provide P with that facility by the end of the compliance period.

My practice clearly meets (a). Please note the words for "whatever reason". This sentence acknowledges that practices had the right, for any reason they chose, to not allow access prior to 31/10/23. One of our reasons was that we had not completed a DPIA. As explained above to allow access without a DPIA would have been in breach of DPA18 therefore we did not enable. I am sure you would agree not wanting to break the law would be a reasonable "whatever reason".

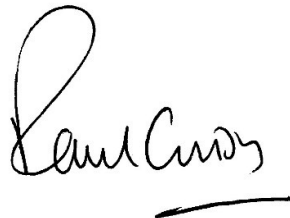
We now move to the next clause (b). To paraphrase it says if after 1/11/23 a patient asks for access, it must be given. So, (a) says its OK to block but (b) says post 1/11/23 provide access on request. Taken as a whole and to labour the point, 16.5ZA.7 says you can have a default of no access to everyone but then provide access when individually requested. That is de-facto an "opt in" process. In short para 16.5ZA.7 creates an opt in for practices such as mine. So, it is wrong to say that all practices must provide access for all patients. Some practices, those that did not allow access prior to 31st October 2023, are now only required to provide access on request, i.e. an "opt-in". Obviously, each individual request will be dealt with as a Subject Access Request (SAR) which will ensure due diligence, you might think of the SAR as being a DPIA but for an individual record.

It follows, and is somewhat ironic, that practices caught by 16.5ZA.7, because they only ever need to respond to individual requests for access and will never be providing wholesale access for all, will not need to go through the DPIA process.

I am sure you will be as concerned as I am that NHS England has failed to understand their own regulations. I am also certain you would want to contact them so that these issues can be clarified, particularly in relation to the contract allowing an "opt in" process for some practices. Given the deadline proposed by NHS England I thought it prudent to release this letter as an open letter.

I look forward to any comments you may have.

Yours sincerely

A handwritten signature in black ink that reads "Paul Cundy". The signature is written in a cursive style with a long, looping initial 'P' and a horizontal line underneath the name.

Dr Paul Cundy

GMC 2582641

- 1) BMA revised guidance
<https://www.pulsetoday.co.uk/news/technology/new-bma-guidance-advises-gps-to-carry-out-dpia-before-enabling-patient-records-access/>
- 2) The "Compliance period" is the response period for a Subject Access Request, i.e usually within one month but at the Data Controllers discretion up to 3 months in total.
- 3) <https://www.pulsetoday.co.uk/news/technology/gps-will-need-to-risk-assess-mass-patient-data-extraction-says-ico/>