

BHATIA, Neil (THE OAKLEY HEALTH GROUP)

From: DPIAConsultation <DPIAConsultation@ico.org.uk>
Sent: 01 June 2021 11:46
To: BHATIA, Neil (THE OAKLEY HEALTH GROUP)
Cc: DPIAConsultation
Subject: RE: Urgent advice regarding the need to undertake a DPIA

Dear Dr Bhatia,

Thank you for your email. I understand you are seeking for our view as to whether GP practices are required to undertake a DPIA in light of the General Practice Data for Planning and Research extraction. We would agree, that as a controller, you would remain responsible for accounting for data protection considerations and any risks to the rights and freedoms of individuals. This includes scenarios whereby a DPIA would be required.

Kind regards,



Data Protection Impact Assessment Team

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow,
Cheshire SK9 5AF

ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

**For information about what we do with personal data see
our [privacy notice](#)**

From: BHATIA, Neil (THE OAKLEY HEALTH GROUP)>
Sent: 28 May 2021 17:49
To: DPIAConsultation <DPIAConsultation@ico.org.uk>
Subject: RE: Urgent advice regarding the need to undertake a DPIA

External: This email originated outside the ICO.

Dear ICO,

I do hope you can respond soon, please.

NHS Digital say it's the responsibility of the GP practices to uphold their patients' right to be informed (Radio 4).

I agree – we are, and remain, the data controller for our patient records, and any action taken upon it, legally-mandated transfer to another data controller or otherwise, is *processing*.

And we remain accountable for that processing, including the need to be able to demonstrate how we have upheld their right to be informed.

Now the British Medical Association today asserts that:

"As this is a legal direction, responsibility for communicating these changes to the general public sits with NHS Digital and the Department of Health and Social Care."

and

"We are concerned about the lack of public information being provided by NHS Digital and we have raised this with them directly, as this isn't something practices should be left to do".

Actually, it *is* something that we should do, and something that we are *legally obligated* to do under UK GDPR.

I am not aware that a "legal direction" to process data (which in this case allows us to satisfy the common law of confidentiality, the Article 6 basis remains 6(1)(e) public task) results in a *transfer of data processor obligations*, including upholding data subject rights, to the forthcoming recipient controller, *prior to* that controller actually receiving the information.

I'm not aware of *anything* that permits that transfer of any data controller obligations and responsibilities to a third party.

Again, your *urgent* advice is desperately needed.

Kind regards,

Dr Neil Bhatia
and 7000 other GP practices in England

From: DPIAConsultation <DPIAConsultation@ico.org.uk>
Sent: 25 May 2021 14:25
To: BHATIA, Neil (THE OAKLEY HEALTH GROUP) >
Cc: DPIAConsultation <DPIAConsultation@ico.org.uk>
Subject: RE: Urgent advice regarding the need to undertake a DPIA

Dear Dr Bhatia

Thank you for your request for advice in regard to the General Practice Data for Planning and Research extraction.

We note your reference to urgency in relation to this, and will be back in touch with you shortly.

Regards



Data Protection Impact Assessment Team

Information Commissioner's Office, Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

For information about what we do with personal data see our [privacy notice](#)

From: BHATIA, Neil (THE OAKLEY HEALTH GROUP)
Sent: 18 May 2021 10:39
To: DPIAConsultation <DPIAConsultation@ico.org.uk>
Subject: Urgent advice regarding the need to undertake a DPIA

External: This email originated outside the ICO.

(Apologies if this is not the correct email address to send this enquiry to. Please redirect as appropriate.)

Dear ICO,

I would be very grateful for your urgent advice about the need for our organisation (and indeed, every GP surgery in England) to undertake, and be able to so demonstrate under the principle of accountability, a DPIA for a forthcoming and huge nationwide data extraction and processing project.

It is my assessment that GP practices are required to undertake a DPIA, in accordance with Article 35, and *since we have not been provided with a DPIA that we can either adapt, or rely on entirely*, we need to undertake this (and imminently). I would be grateful if the ICO would confirm my assessment, or alternatively explain why we should not need to undertake a DPIA, as is required under Article 35.

As the ICO is fully aware, from 1st July – i.e. in just 6 weeks – GP surgeries across England will be legally compelled to extract and upload the entire GP records of every man, woman, child, and baby on their practice list. This personal confidential medical information – *special category data* – will be transmitted to NHS Digital, who become the data controller for the information. The information will be used/sold/disseminated for purposes beyond direct medical care, that is *secondary purposes*.

This project is called the General Practice Data for Planning and Research extraction. It is *not* processing under COVID-19 regulations.

<https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notice/data-provision-notice-dpns/general-practice-data-for-planning-and-research>

This involves:

- new processing of GP records (almost the *entire electronic record* as held by GPs)
- processing of sensitive data or data of a highly personal nature
- processing of data including:
 - Physical / Mental health
 - Sexual Life / Orientation
 - Family / Lifestyle / Social Circumstance
 - Religion or Other Beliefs
 - Racial / Ethnic Origin
- processing on a large scale (*55 million* people across England) *for our surgery, that's 30,000 individuals*
- processing of data concerning vulnerable data subjects
- processing of data concerning children (<16yrs old)
- processing of data concerning data subjects for whom English is not a first language
- processing of data concerning data subjects with disabilities, such as sight and hearing impairment, and learning difficulties

It is likely that, once the information is in NHS Digital's hands, processing will involve:

- profiling on a large scale (such as “risk stratification”)
- systematic monitoring by NHS Digital
- combining, comparing or matching data from multiple sources
the GP records will be linked to corresponding hospital records, mental health records, social care records, ambulance service records, and community provider records
- processing of personal data that could result in a risk of physical harm in the event of a security breach
- disclosure/selling of personal confidential information in pseudonymised and clearly identifiable formats, to unspecified 3rd parties
- re-identification of de-identified (pseudonymised) data – NHS Digital holds the “key”

GP surgeries were informed of this project on Tuesday May 12th, extraction/uploading/processing of the GP records of the population of England will commence on 1st July and continue on a daily basis thereafter. Individuals have until 23rd June to “opt-out” at their GP surgery.

If no opt-out is registered at their GP practice *before* 1st July then extraction will occur.

If an opt-out is registered at their GP practice *after* 1st July then no *new* information about them will flow to NHS Digital.

However, all previously uploaded information will:

- continue to be held by NHS Digital *indefinitely*
- continue to be processed by NHS Digital *indefinitely*
- continue to be disseminated/sold by NHS Digital *indefinitely*

and there does not appear to be a way by which an individual can prevent NHS Digital from continuing to hold and process their data.

There is, seeming, no *right of erasure*.

There are serious concerns about the ability for GP surgeries to uphold the *right to be informed*. It is impossible to inform more than a handful of patients in the next 6 weeks

- in the midst of a pandemic
- when footfall to GP surgeries is diminished
- when GP surgeries are overwhelmed with clinical demand
- when GP surgeries are *additionally* providing a mass vaccination service, out with their clinical NHS duties

NHS Digital have not advertised this huge scheme. There are no TV or radio adverts, they have not written, either to individuals or households. There are no newspaper ads, no junk mail leaflets.

They have left the *entire* burden of informing people – a data subject right - to GP surgeries, amidst the fog of COVID-19.

There a very high risk (a certainty, undeniably) that the overwhelming population of England will not be informed about this processing of their personal, confidential, medical information and so afforded the opportunity to opt-out – *before 1st July* –

and exert their right to control their medical record. Their privacy *will* be breached. They will lose *all control over their medical information*.

In light of all these matters, and concerns, I believe that such processing poses high risks to the rights and freedoms to individuals. Whether or not these can be mitigated, before 1st July, and how, is surely the purpose of a DPIA?

Accordingly I see no avenue to argue that GP surgeries *are exempt* from undertaking a DPIA for such new processing.

That we are in the midst of a pandemic, that GP surgeries are literally on their knees, that we are being tasked with vaccinating hundreds of thousands of people every day against COVID-19 *in addition to our clinical responsibilities*, does not relieve us of our data protection obligations and the requirement to undertake a DPIA.

That we are *legally compelled* - Article 6(1)(c) - to process our patients' data in this way, to disclose to NHS Digital for as yet unspecified, and seemingly unlimited, processing purposes, does not relieve us of our data protection obligations and the requirement to undertake a DPIA.

That the seeming, and wholly unjustified, "urgency" to extract and upload by 1st July does not relieve us of our data protection obligations and the requirement to undertake a DPIA.

Our surgery [has always undertaken DPIA's](#) for processing on a large scale, *and it doesn't come any bigger than this*.

The ICO might well have seen – and commented on – a DPIA produced by NHS Digital. But NHS Digital have *not* provided GP surgeries with it, and no doubt will not until *after* 1st July. And if we haven't got a DPIA to rely upon, we must undertake one from scratch.

I would be grateful for the ICO's urgent opinion. If practices need to undertake a DPIA – *which is surely a requirement under GDPR* - then they are going to need to do it *without delay* – or breach Article 35.

Many thanks,

Dr Neil Bhatia

GP, IG/FOI/Records Access lead, Caldicott Guardian, Data Privacy Officer, Data Protection Officer, Data Autonomy Advocate

Oakley Health Group

Yateley Medical Centre

Oaklands

Yateley

Hampshire GU46 7LS

T: [01252 872333](tel:01252872333)

W: www.oakleyhealth.org

F: www.facebook.com/oakleyhealth

This message may contain confidential information. If you are not the intended recipient please inform the