NHS England Accelerated Access Programme

Data Protection Impact Assessment dated 06 October 2023

Prepared by the BMA GPC England

Submitting controller details

Name of controller	Warwick Gates Family Health Centre
Subject/title of DPO	DPIA (Data Protection Impact Assessment)
Name of controller contact/DPO	Kelly Huckvale agem.dpo@nhs.net

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA:
Pursuant to regulation 71ZA-71ZB of the National Health Service (General Medical Services Contracts) Regulations 2015/1862 and Regulation 64ZA-64ZB of The National Health Service (Personal Medical Services) Agreements Regulations 2015/1879 (referred to together herein as "the Regulations") and forced changes to General Practitioner ("GP") Practices' ("Practices") contracts for services. GPs and Practices whose contracts have been so changed are now obliged to provide their patients with the facility to access their prospective medical record on or after 31 October 2023. It is understood that the requirement is for both (a) the facility to be provided no later than 31 October, and (b) medical records added to or received into the GP-held record on or after the 31 October to be made available to patients online from that date. It is clear that a GP's obligations pursuant to the Data Protection Act 2018 ("DPA 2018") and UK GPDR as a primary statute override any contrary obligations which may appear pursuant to the Regulations as it could not have been NHS England/The Secretary of State's intention, nor could it be legally permissible, to override a GP's duties imposed by an Act of Parliament. The new requirements require a different way of processing. They require changes to the way that GPs and Practices as data controllers of the GP-held medical record process their patients' personal data and, as such, a DPIA is required by law.

Step 2: Describe the processing

Describe the nature of the processing:
There will be very limited changes to the way in which the data that forms medical records is collated, used and stored, save where a GP or Practice creates a new document by redacting an existing document. However, we do not consider this to be a significant change in the nature of the data processing. The source of the data will remain the same, that being from primary, secondary and community care providers within the health service. The most significant change is that the data will be automatically made available for patients to view online through the NHS app or NHS website where the patient has the requisite NHS account and login details set up. Such access is required to be provided automatically, unless: (1) the patient has opted out; (2) the information contained in the medical record is "excepted information" i.e. if a GP would not be required to disclose such information pursuant to Article 15 of UK GDPR and (3) the serious harm test in Part 2 of Schedule 3 of the DPA 2018 applies (i.e. the GP has decided it will be potentially harmful for the patient to have access). The definition of processing under the UK GDPR is very broad ("any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"). That broad definition includes making a computer record of personal data accessible online to the data subject. The information in a patient's medical records amounts to 'personal data' as defined by Article 4(1) of the UK GDPR, which falls within the special categories identified in Article 9 of the UK GDPR.

Describe the scope of processing:
The information in a patient's medical records amounts to 'personal data' as defined by Article 4(1) of the UK GDPR, which falls within the special categories identified in Article 9 of the UK GDPR. In addition, it is highly likely that other special categories of personal data will form part of the patient's medical record such as data revealing racial or ethnic origin, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation etc. The medical record will also include non-special category personal data such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person. The data will be collected and processed whenever a patient interacts with primary or secondary health care services, chiefly by GPs adding consultation notes together with correspondence between primary, secondary and community care providers including hospitals, pathology labs, and other out-patient clinical settings. The data amounts to a patient's medical record and is not deleted.

Direct access to a patient's own medical record is open to any individual with a NHS identification number who is registered with a general practice, which represents almost every individual in England. They can access their own medical record through the NHS app or NHS website to the extent that parts of their medical record have been made available.

Describe the context of the processing:

GPs and Practices play a vital role in the health system by being the trusted primary source of health provision for over 50 million patients in England. GPs build up deep and enduring relationships of trust with their patients and are expected to ensure the accuracy and security of the medical records of their patients. They are responsible for their patient's care from cradle to grave.

Patients have little control over their own medical records and generally do not input any data directly on to them save for limited circumstances where a patient supplies their doctor with information or photos by SMS text message or where a photograph and data provided by a patient in another way is added into the medical record.

Children's medical records will be available to their parents or legal guardians by proxy.

The position in respect of those individuals who lack capacity is currently unclear as the Regulations are silent in relation to access for carers/legal guardians. It is assumed that where appropriate a carer/legal guardian could be granted access to the medical record.

GPs and Practices have not selected the technology platform upon which digital access to patient records is given, nor are they and the BMA privy to the data security measures which NHS England and the technology companies have built into the software save for the requirement to provide a password, finger print or Face-ID on login. However, as a key piece of the Government's IT infrastructure, we expect that the DHSC and NHS England will have taken all necessary precautions to build, develop and test a secure data platform though we are not in a position to confirm that the platform is properly secure.

We believe that NHS patients put the data security of their medical records as a very high priority and would expect that the system is totally secure given the utmost confidential nature of the data. The security of patients' confidential medical data is repeatedly the subject of national news where concerns are raised about such data being used unlawfully for secondary uses by government contractors. The security of NHS patients' data is clearly a matter of significant public interest.

Describe the purposes of the processing:

The BMA is supportive of patients having online access to their medical record as long as it is done in a way that is safe for patients and GPs. However, it did not agree to GPs being placed under a contractual requirement to provide all patients with access unless they have opted out – the processing that is the subject of this DPIA. This processing requirement is being imposed upon GPs through regulations and unilateral variations of contract, despite reasoned objections from the BMA.

The purposes of the processing are therefore twofold (a) to ensure GPs and Practices do not breach their contracts and (b) to enable patients who would benefit from their prospective medical record being available online to be provided with the facility to access it online.

The legal requirement for this processing is underpinned by government policy and regulations made pursuant to the same. The Government say that there is "*widespread international consensus about the benefits to patients and the effectiveness of the health system to provide digital access to personal health information*". By providing online access to a patient's medical record, the Government believes that this will make the delivery of primary care health resources more efficient, by giving access and control of test results and referral correspondence to the patient it will relieve pressure on GP practices by saving time on fielding enquiries. Further, the Government believes that online access will promote better long-term health for patients, supporting prevention and improving health outcomes by encouraging patients to engage more fully with their medical records and manage their health conditions.

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

We believe that there will be a number of patients who do not wish to have online access to their medical records. For this reason, if resources allow, ahead of the Government's implementation date and in any event before patients are automatically given access to their medical records, GPs and Practices will be encouraged to contact their patients asking whether they wish to have access. For those patients who wish to 'opt out' and confirm that they do not wish to have access, a SNOMED CT code "Online access to own health record declined by patient" (SCTID: 1290331000000103) ("SNOMED 103") code may be applied to their record which will indicate that their record should not be available for viewing by the patient online and any existing access rights should be revoked.

We do not believe that the DHSC or NHS England have consulted adequately with a wide variety of patient stakeholders across the country in relation to this new processing which they have required to be carried out and GPs and Practices have not been provided with the outcomes of any such consultation. In addition, we are not aware of any publicity campaign by NHS England or triangulation with essential external stakeholders.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures:

In providing online access, GPs are processing their patients' personal data within the meaning of Article 4(2) of UK GDPR. Article 6(1)(c), (d), (e) and (f) provide a lawful basis for processing patients' special category data, together with Article 9(2)(h). Processing data in this way allows patients to view their online medical record in accordance with the Government's amended Regulation and GMS/PMS contracts.

We maintain that there is a more appropriate way to allow patients to have online access to their medical records, which would rely on patients actively opting in to access rather than being provided access automatically.

An 'opt in' process would have the following advantages:

- It would give patients and GPs more control over the roll out of online access;
- It would allow GPs and Practices to speak directly with the patient during a consultation or by other means of communication to discuss the merits of having online access and whether such access is suitable and appropriate for that patient in all of the circumstances;
- It would allow the patient to give proper informed consent and would, in our view, make it more likely that the patients who do wish to access their medical records online will understand the full benefits of the system;
- It would help to safeguard access to patients' data and accord with Article 5(1)(f) UKGDPR, which requires appropriate security; and it would allow an opportunity for GPs to identify patients who may be at risk from coercive control of their medical records via a partner accessing their records on the NHS App or NHS website without their permission.

The BMA has advocated for an opt-in process but the DHSC has proceeded to establish a contractual obligation for GPs to provide access no later than 31 October 2023, except for patients that have opted out.