NHS England Accelerated Access Programme

Data Protection Impact Assessment dated 04 October 2023

Prepared by the BMA GPC England

Submitting controller details

Name of controller	Spa Medical 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.

In the 2010 Conservative party manifesto, David Cameron said "*you'll be able to check your health records online in the same way that you do your bank account."* Thereafter in the Conservative Party manifesto of 2015, the 2010 pledge was repeated stating "*we will give you access to your own electronic health records*". It is therefore likely that the public have some awareness of the Government's commitment to make access to their patient data readily available online. The exact mechanism for this may come as a surprise to some patients and we believe that there is very little public knowledge around the new requirements for GPs to provide the facility for online access to all patients no later than 31 October 2023.

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 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.

Step 5: Identify and assess risks

	Describe source of risk and nature of potential impact on individuals	**Likelihood of harm** (Remote/Possible/Probable)	**Severity of harm** (Minimal/Significant/Severe)	**Overall risk** (Low/Medium/High)
1.	Risk of misfiling and inaccuracies within patient record: GPs and their staff may inadvertently misfile special category data on the wrong patient file. This may allow a third party accessing their own patient file to access data belonging to another. Such a circumstance could arise by simple administrative error, compounded by poor resourcing. Such a data breach would likely go undiscovered unless the third party drew the practice's attention to the breach, but it is possible that a third party may maliciously share the data more widely. In addition, these errors constitute a data breach and therefore the practice Data Protection Officer must decide within 72 hours whether to report the incident to the ICO and the patient.	Possible	Severe	Medium
2.	Risks to children and vulnerable patients: Children and vulnerable patients have particular risks which are set out below: 1. Children – we understand that a child's parent or legal guardian can have online access to their child's medical record from birth to 16, and that the child will have access or could obtain access to their records	Possible	Severe	Medium

	as early as 11. There are a number of risks associated with this, for example: (i) A child with access to their own medical records is unlikely to understand the significance of the data and may be vulnerable to being coerced into sharing their medical records amongst their peer group and online by social media in circumstances which are inappropriate; (ii) A Gillick-competent young person may not wish their parent to continue to have access to their online medical records or may prevail upon a GP to conceal information from their medical records and thus their parent(s) or legal guardian. This may particularly be the case where the young person is accessing family planning advice, or wishes to make a disclosure to a GP about physical, sexual or psychological abuse within the family or elsewhere; (iii) As a looked-after child moves from legal guardian to legal guardian, there is a risk that multiple people have access to the child's medical records when they have no legitimate legal or practical interest in accessing those records. There is a risk that social services do not update the GP in a timely fashion as to the child's current legal guardian(s). This is particularly relevant where a child is	Possible Possible Possible	Severe Severe Severe	Medium Medium Medium

	moving from one foster placement to another in quick succession. 2. Coercive control and domestic abuse - there is a real risk that the victims of domestic abuse and coercive control would be forced to disclose their medical records to their abuser. An abuser (unknown to the GP) may already have access to or control over their victim's mobile phone or NHS App and would therefore automatically gain access to their prospective medical record when 'switch on' occurs pursuant to GPs contractual obligation. This is particularly concerning where a GP may be a vital source of external help and where a GP would note the abuse by, for example, documenting injuries within the medical record or documenting contraceptive use or a termination of pregnancy procedure. An abusive partner is likely to be keen to note that their victim does not report the true nature of the mechanism of any inflicted injury. This may lead to the victims of domestic abuse/coercive control failing to report particular issues to their GP or reporting it and suffering the negative consequences from their abuser. This has potential to have a serious impact on the patient/doctor relationship and the confidence of patients to disclose issues of a deeply personal nature to their GP. 3. Mental Health - people who suffer significant mental health issues, and particularly those who self-harm or are suicidal, often are very focused on their medical condition such that their medical records could provide a trigger point for a spiral of self-harm	Probable	Severe	Medium

	or suicide. This could be envisaged as very concerning when a patient views online documents about their mental health assessments late in an evening when little support is available to the individual. GPs would ordinarily control patient access to any records which are likely to trigger episodes of significantly poor mental health.	Probable	Severe	High
3.	Risk of premature diagnosis: There is a risk that a patient would first learn about a significant diagnosis by seeing their own medical records before their GP or hospital specialist has the opportunity to discuss their diagnosis, prognosis and treatment options with them. There is also a risk that less serious diagnostic results or diagnoses are misunderstood by patients who use the internet or other independent sources instead of their GP. The risk that a patient reacts negatively to either a real significant diagnosis or misunderstands their clinical situation may give rise to the patient self-harming or experiencing significant psychological trauma.	Possible	Significant	Medium
4.	Risk to resources: There are numerous ways in which GP resources will be expended in relation to this matter, some of which are covered in other risks within this DPIA. In addition to those, see below: 1. A patient reviewing their medical records, and in particular correspondence or diagnostic results from secondary care, may fail to understand medical terminology used within the records. Additional GP time will be	Possible	Minimal	Medium

	expended in explaining relevant terminology. Patients may require this service out of hours when the GP Practice is closed; 2. GPs are best placed to understand their patients' medical needs and in particular how each individual patient might react to correspondence highlighting a particular diagnosis. Correspondence received from secondary care may not be sensitive to the patients' clinical, and in particular, psychological requirements therefore GPs will be required to carefully review each and every piece of correspondence in a timely fashion to ensure that the patient's needs can be effectively managed; 3. As matters currently stand, third party and other redactions required pursuant to the DPA 2018 are not routinely made unless a patient requests a copy of their medical record, at which time such redactions are made. GPs must now ensure that all such redactions are made to all correspondence before that entry is filed so as to comply with their obligations pursuant to the DPA 2018.	Possible Possible	Minimal Minimal	Medium Medium
5.	<u>Risk that the IT infrastructure is not secure</u>: It is recognised that GPs have no control over the IT infrastructure that will host the online medical record and have not been involved in the development or testing of it. No warranties have been given by NHS England or the DHSC over the security or robustness of the IT infrastructure and there is a risk	Possible	Severe	High

	that third parties may gain access to patient records and/or make those records available online. As data controller, GPs have assumed the legal risk for the data on the medical record but have no control over the IT infrastructure upon which it is hosted. It is therefore impossible to gauge the risk to patients, but it is at least possible that malicious actors could be able to obtain access to medical records.			
[6.]	[DELETE IF NO USE OF DOCMAN] [Capability of redaction software: There are a number of potential risks arising out of the primary inadequate redaction software, Docman, which has been provided by NHS England and which is used by many GP practices. The risks are highlighted separately below: 1. The Docman software can only allow redaction of a single word/line/paragraph in a document at the point of filing and before clinical review has occurred. The redaction, once passed to EMIS, is to be considered permanent. This redacted version is what will transfer via GP2GP should the patient move practice. The software also allows an entire document to be hidden from online view. A hidden document will still transfer via GP2GP should the patient move practice. There is a danger that if a document requires redaction and this is done at the point of filing then critical clinical data linked to the necessary redaction will be lost; and	Possible	Severe	High

	2. A clinician wishing to preserve valuable clinical information may elect not to redact where a redaction ought to have been made, or accidentally fails to redact where third party information is present and third party data becomes available to the patient in breach of their DPA/UK GDPR obligations leading to a complaint to the ICO/legal claim from the third party.]	Probable	Severe	High

Step 6: Identify measures to reduce risk

	Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
	Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated/reduced/accepted)	**Residual risk** (Low/medium/high)	**Measure approved** (Yes/no)
1.	Risk of misfiling and inaccuracies within patient record	Routine use of the NHS number in any primary search, in addition to the checking of name, date of birth and address when adding entries to medical records. This will require additional administrative resourcing. Practices may also wish to consider a two stage process, by which work is checked, improving quality control. It is recognised that not all correspondence uses the patient's NHS number particularly that which emanates from secondary care providers. This	Reduced	Medium	Yes

		reduces the effectiveness of the mitigation measure and additional resources will be required to ensure accuracy.			
2.	Risks to children and vulnerable patients	1. Children - (i) Only allow the child to have access in circumstances where it's thought clinically responsible to do so. (ii) To remove parents' or legal guardians' access in circumstances where the GP feels it's appropriate or to make certain entries on the medical record unavailable to the patient/parent/guardian. (iii) So far as the GP is able to remind each set of those legally responsible for the child and who have access to online medical records to request the practice revoke and reprovision access each time another adult takes responsibility for the child's welfare in order that only those who are currently responsible for the child's welfare are able to access the child's records. However the GP has ultimately no control over this mitigation process. GPs also to check how many proxy users have access and ensure that each of those users requires access and such access is appropriate.	Reduced Accepted Reduced	Medium Medium High	Yes Yes Yes

		2. Coercive control and domestic abuse – it is accepted that although GPs will be aware that some of their patients are the victims of domestic abuse or coercive control, this will not be apparent in every case. Where a patient specifically draws the GP's attention to this issue, remote access should be removed or the utmost care should be taken to ensure that only those entries which are appropriate are available to the patient for viewing. The risk of a GP not being aware of a patient who is the victim of domestic abuse or coercive control is high (recent government data shows that 1 in 20 relationships are coercive in nature), therefore the most appropriate mitigation step would be for the GP to speak with each patient before online access is granted (the 'opt in' model) in order that the GP can ensure that the patient understands the scope of access and is content that it is safe and appropriate for the patient to be granted access.	Reduced	High	Yes
		3. Mental health – for those individuals where the GP feels that access to their medical records would be a triggering factor in self-harm or suicide, access should be withheld/withdrawn. A GP will not always know whether a patient's access to their medical records would trigger self-harm and/or suicide therefore a GP should review the clinical	Reduced	High	Yes

		appropriateness of providing online access to medical records with a patient before it is given and this should be kept under review to ensure that the patient is providing informed consent and that the GP is discharging its clinical and legal duties to the patient.			
3.	Risk of premature diagnosis	It is accepted particularly where third party correspondence, for example from secondary care or community providers or diagnostic results, are placed on the patient file that the GP may not have had the opportunity to properly review and forewarn and counsel the patient before the record is made accessible to the patient. It is not practical or appropriate for all GPs to routinely conceal all correspondence from secondary care/diagnostic results from patients and the IT system does not permit the GP to configure a delay on the records being made available to the patient. As such the only effective mitigation appears to be for GPs to withhold access to online patient records until the GP has properly explained this risk to the patient and the patient has provided informed consent that they accept this type of risk (an opt-in process) This would allow patients to understand and manage the risks of accessing their own medical records particularly in circumstances where they have undertaken diagnostic tests for a	Reduced	Medium	Yes

		significant illness or have a progressive disease.			
4.	Risk to resources	1. Unless all clinicians in primary, secondary and community care settings are aware of this issue and when corresponding provide “patient friendly” explanations there is no mitigation step that will not require GPs to spend additional resources. It is recognised that such mitigations are not possible in every case in any event and would require a sea change in NHS policy with its own resource implications. 2. The only mitigation is to not provide online access for those who may be triggered or at risk of serious harm by viewing clinical documents without explanation from a GP. 3. There is no mitigation step in order for GPs to comply with their obligations under the DPA. Additional time will need to be devoted to dealing with redactions.	Accepted Reduced Accepted	Medium Medium Medium	Yes Yes Yes
5.	Risk that the IT infrastructure is not secure	GPs have not been provided with sufficient information about the IT infrastructure to be able to put into place sensible mitigation for a risk which is unknown. If and until NHS England/DHSC provide such assurances that satisfy the data controller that the data is secure, the only mitigation step available is to restrict access to all patients as this eliminates	Accepted	Medium	Yes

		the risk of malicious third party actors obtaining information by this means.			
[6.]	[Capability of redaction software]	[1. Where a document includes clinically important information, a separate copy of the document should be created, saved to the patient record, and the unredacted version of the documents should be hidden from patient view. 2. Clinicians should make the redaction and make a copy - see above. Necessary redactions may inadvertently be missed, given the resource pressures on GPs and their staff, the daily number of documents to be reviewed along with patient interactions. No system can be completely without error and there are no mitigations which can fully protect third parties.]	N/A N/A Accepted	N/A N/A Medium	N/A N/A Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Dr Timothy Knight 4/10/23	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Kelly Huckvale DPO	If accepting any residual high risk, consult the UCO before going ahead
DPO advice provided:	Kelly Huckvale	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	Accepted	If overruled, reason why:
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	Kelly Huckvale/ Dr Timothy Knight / Kam Rai	The DPO should also review ongoing compliance with DPIA