**We as a practice have been offering full access to the GP electronic health record (prospective and retrospective access to the whole GP electronic health record) since 2004** through an **explicit consent process** and **responsible sharing** <https://www.htmc.co.uk/responsible-sharing/> and over 81% of all our patients already enjoy this service. <https://www.htmc.co.uk/do-you-want-to-see-what-your-doctor-or-nurse-has-written-about-you-or-check-your-gp-electronic-health-record-2/how-many-have-signed-up-for-full-records-access-and-understanding/> We published our data for over 16000 patients that have completed the questionnaire showing our robust processes and potential harm and how we have mitigated this by doing this on a patient by patient basis. <https://www.htmc.co.uk/over-16000-questionnaires-done-for-records-access-and-understanding/>. He have published our method for all to see <https://www.htmc.co.uk/patients-accessing-the-gp-electronic-health-record-and-understanding-the-haughton-thornley-medical-centres-way/>.

The government / NHS England have imposed a contractual change that means patients with online accounts such as through the NHS App will be able to read new entries, including free text, in their health record. This change only applies to future (prospective) record entries and not historic data (from 31st October 2023. <https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/guidance-on-nhs-app-features/online-access-to-gp-health-records>. I talked about this at the national LMC conference in 2022 where I raised concerns about the programme and why it is unsafe (3 minutes 20 seconds long) <https://youtu.be/VS1R-xCr5L8>

Due to widespread concerns about the approach being taken and to safeguard patients as well as practices, we as a practice instructed EMIS not to automatically upload data from patients records <https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/guidance-on-nhs-app-features/accelerating-patient-access-to-their-record/update-from-nhs-england> and put a 104 code in place to also stop patient records from being uploaded UNLESS they had been consented by completing our Records Access and Understanding Safety Checklist Questionnaire <https://www.htmc.co.uk/do-you-want-to-see-what-your-doctor-or-nurse-has-written-about-you-or-check-your-gp-electronic-health-record-2/>

We need to do a Data Protection Impact Assessment (DPIA) in relation to the Accelerated Access to Records Programme Implementation on Wednesday morning as a practice.

As this is very new and most if not all of us have little understanding of what this is, I have tried to pull out the most relevant information to help us all get the most from this.

The ICO (Information Commissioner’s Office) defines a DPIA (Data Protection Impact Assessment) as a process designed to help systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of a GP contractor’s accountability obligations under the UK GDPR, and when done properly helps assess and demonstrate how contractors must comply with their data protection obligations.

If a data controller wishes to process personal data in a new way, it must by law carry out a DPIA. Providing patients with access online to their medical records in accordance with the new legal requirements is a new form of processing, so GPs as data controllers need to conduct a DPIA. The BMA has conducted a general DPIA on behalf of the profession as a way of sharing the data protection analysis it has carried out. It is intended to help practices carry out their own DPIAs.

We as Partners and the Data Controllers of the patients data (the GP electronic health record) have THE responsibility to look after the patient’s record. We are responsible for ensuring our processing – including any processing carried out by a processor on your behalf – complies with the UK GDPR (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/>)

If we complete a DPIA, take actions to mitigate risks and determine that any remaining risks are acceptable then we have fulfilled our duty to complete a DPIA. However, as data controllers, GPs have an ongoing responsibility to comply with our general duties under data protection law, so processing must always be carried out in accordance with those duties.

Once the DPIA has been completed and if we consider the risks of automatic access to prospective records high then we can safely add 104

codes to all patients records that have not got full records access and invite all remaining patients to complete the online questionnaire / consent process. A 106 code can then be added that revokes this. Those patients who do not wish to ever have prospective access can have a 103 code added.

As this could directly impact patient care and as part of the ethos of the practice to promote a “Partnership of Trust”, I feel we should do this with members of our Patient Participation Group as well as with our Partners and also Practice Manager too.

It is essential you read this BEFORE the meeting tomorrow and complete the exercise yourself to see what you think. There are a number of scenarios that the BMA and their lawyers have put together where things could go wrong resulting in harm. The DPIA is about identifying what we as a practice think is the likelihood of such harm (remote / possible / probable), how severe it may be (minimal / significant / severe) and what the overall risk is (low / medium / high).

Below you can see the template and the scenarios we need to consider and below this is the BMA’s answers that they have provided to see how this works.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **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 or probable | Significant or severe | Medium to high |
| 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 as early as 11. There are a number of risks associated with this, for example: 1. 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;
2. 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;
3. 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 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 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. | PossiblePossible or probablePossiblePossible or probablePossible or probable | Significant or severeSignificant or severeSignificant or severeSignificant or severeSignificant or severe | MediumMedium to highMedium to highMedium to highMedium to 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 it could happen | Significant if it happens | Unknown |
| 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 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 to probablePossible to probableProbable | Significant to severeSignificant to severeSignificant to be in breach of data protection obligations to third parties. | Medium to highMedium to highMedium  |
| 5. | Risk that the IT infrastructure is not secure: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 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. | Possible it could happen | Significant if it happens | Unknown |
| [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
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.]
 | Possible or probablePossible or probable | Significant or severeSignificant or severe | Medium to highMedium to high |

The BMA has done its own assessment of the above and here are their answers (so you can see what we have to do).

|  |  |
| --- | --- |
|  | **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 reduces the effectiveness of the mitigation measure and additional resources will be required to ensure accuracy. | Reduced | Medium – even with stringent processes the risk of human error and the significant number of interactions with patient data is such that mistakes are bound to occur. | Yes |
| 2.  | Risks to children and vulnerable patients | 1. Children - 1. Only allow the child to have access in circumstances where it’s thought clinically responsible to do so.
2. 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.
3. 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.

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.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 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. | AcceptedReducedReducedReducedReduced | LowMediumMediumMediumMedium | YesYesYesYesYes |
| 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 significant illness or have a progressive disease. | Reduced | Medium | Yes |
| 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.  | Not reduced | High | No effective mitigation |
| 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 the risk of malicious third party actors obtaining information by this means.  | Eliminated | Low | Yes |
| [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.]  | EliminatedAccepted | LowLow | YesYes |