

- To:
- GP practices
  - Primary care networks
  - NHS England regions directors and directors of commissioning
  - ICBs
  - Clinical leads and safety officers
  - Accountable officers

NHS England  
Wellington House  
133-155 Waterloo Road  
London  
SE1 8UG

**21 July 2022**

Dear Colleagues

### **Offering patients access to their future health information**

In line with the NHS Long Term Plan and [‘Data Saves Lives’ Data Strategy](#), the NHS is working to make it easier for patients to digitally access their future health information in their general practice records. In April 2020 NHS England introduced an obligation for practices to [give patients access to their prospective \(future\) medical record online \(including free text and documents\)](#).

Better access to health information enables patients to become partners in managing their health. Evidence has shown that this increases patients’ feelings of autonomy and reduces the need for patients to contact general practice<sup>1</sup>.

There is now a revised timeline for the automatic switch on of prospective access. On **01 November 2022**, patients at practices using TPP and EMIS systems will **automatically** have access to their **prospective** records online. Work is ongoing with Cegedim (previously Vision) to create the same functionality. This does not change the status of general practices as a data controller or alter existing obligations to [promote and offer access to historic information](#).

Over the coming months our aim is to build trust and confidence in clinicians and practice teams to provide online access. To prepare for this change we are asking general practice teams to:

- **identify patients who could be at risk** of serious harm from having automatic access to their records and ensure the right safeguarding processes are in place to support access to all future data, including free text and correspondence sent

---

<sup>1</sup> <https://qualitysafety.bmj.com/content/29/12/1019.long>

into general practice. An individual review may be required to exclude patients from having access due to a risk of serious harm. Further guidance is included in Annex A.

- **consider increasing the number of patients who have online access and/or enhance their level of access gradually over coming months prior to automatic rollout.** How this is achieved should be locally determined and may include wider patient promotion or improving the current default access level being provided. If practices would like to make prospective access available to all of their patients ahead of November, they can contact [england.NHSEimplementation@nhs.net](mailto:england.NHSEimplementation@nhs.net) who can support early deployment.

There are a number of resources available to support preparing for the change, including a series of webinars for practices and commissioners. These are available at <https://digital.nhs.uk/records> and include:

- An updated RCGP GP Online Services toolkit. Providing general practice guidance to manage online records access effectively, efficiently, safely and securely.
- A series of short videos on key topics including: an overview of upcoming changes; when and how to redact information; when to decline access to records; and conducting/documenting consultations that empower patients when they access their records.
- Details of what we have learned from the early adopter sites, including materials and GPIT system reports/protocols that they used to successfully prepare and a practice checklist.
- A package of communication materials for general practice teams to use, to inform their patients of the change and to promote access.
- Information Governance (IG) Guidance and a national template to support a Data Privacy Impact Assessment by a practice team.

### **Implications for the wider health system and partnership organisations**

ICB's and commissioners are asked to support awareness and preparations by providers within the wider health system.

Healthcare providers and partnership organisations should continue to share important information with general practice. This can be redacted (made invisible) from the patient

view when necessary. To reduce the risk of inappropriate disclosure, providers should clearly identify when correspondence shared with general practice should not be visible to a patient, as its disclosure could result in serious harm.

As outlined in [Securing Excellence in Primary Care \(GP\) Digital Services: The Primary Care \(GP\) Digital Services Operating Model](#), commissioners should provide a training service for practice staff to support the safe and effective use of clinical systems and national digital services. General practices requiring additional support should contact their local commissioner in the first instance. Specific training and awareness sessions are being offered to local GP IT training teams, so they are fully informed and able to support general practice with this change.

We will continue to update information at <https://digital.nhs.uk/records> and you can email queries to [England.NHSEimplementation@nhs.net](mailto:England.NHSEimplementation@nhs.net).

Time to prepare before 1<sup>st</sup> November launch

Following engagement with RCGP we committed to their recommendation of providing GP teams with a minimum preparation time of 2 months for this change. By confirming that the change will take place on **1 November 2022**, there is additional time for teams to prepare, access support, identify individuals potentially at-risk, build staff confidence and embed training.

We anticipate that with the assistance outlined above, alongside commissioner support, that automatic switch on of prospective access will be successfully deployed on 1 November. Patients will be able to view their online data in their GP record, as it is entered from that date. Practices and commissioners must be confident that the service can be provided safely. Practices should contact their commissioner where they see challenges with providing the necessary safeguards, so that commissioners can work supportively with them ahead of 1 November. We thank you in advance for your support in achieving this first step towards greater citizen access to health records.

Yours sincerely,



**Dr Ursula Montgomery**  
Director of Primary Care  
NHS England



**Dr Nikita Kanani MBE**  
Medical Director for Primary Care  
NHS England

## Annex A - identifying and managing patients who could be at risk

For the vast majority of patients digital access does not pose a specific risk - rather it enables people to better manage and understand their health and care, and it can reduce harm<sup>2</sup>. For a minority of patients who are considered vulnerable, such as people at risk of domestic violence or in coercive relationships, individual risk associated with online records access will need to be considered. When there are safeguarding concerns, healthcare workers can prevent patients from having automatic access to new information by adding [these codes](#) to the patient's record. Records with this code will be excluded from the changes, and these patients will then need to be reviewed on a case-by-case basis to identify if access can be provided without a risk of serious harm.

It is also necessary to redact (make invisible from patient view) information, for example when relating to third parties where it is not reasonable for the patient to be able to view this information, or information that is likely to pose a risk of serious harm to the patient or another individual. Information on how to redact can be found within your system supplier guidance.

General practice teams should therefore ensure that:

- All staff who enter information into their clinical system are aware of this change, including administrative staff, locums and other temporary staff.
- There are appropriate processes and safeguards in place to identify patients who should not have access to their records. Guidance is available at <http://rcgp.org.uk/patientonline> and example reports used by early adopter sites to identify at-risk patients are available at <https://digital.nhs.uk/records>. These are not exhaustive and should be supplemented by local knowledge.
- Patient access settings are reviewed and where necessary ensure they do not receive access to future information by [applying the appropriate Systematised Nomenclature of Medicine \(SNOMED CT\) code](#).
- There are appropriate processes and procedures in place to ensure that information that is not suitable for patient view is redacted when entered onto the GP IT system, in compliance with data protection legislation. More information is available in your system supplier guidance and included in these [short videos](#).
- Data quality of information entered onto GP IT systems is maintained, and patients are fully informed about their care. Some systems allow the automatic

---

<sup>2</sup> <https://qualitysafety.bmj.com/content/29/12/1019.long>

upload of items from other care settings into the GP record, such as discharge summaries, test results and letters. When this occurs, you must work with your local GPIT support teams to review your system settings to prevent inappropriate release or over-redaction of information.

Further [information governance advice](#) is available, including a template Data Protection Impact Assessment (DPIA) for general practice.