APPLICATIONS FOR RECORD ACCESS

This guidance describes the steps that you should take to register new applicants for Patient Online record access. It applies for patients who already have appointment or repeat prescription access and also for patients with detailed coded record access who want to have access to consultation notes and clinical correspondence as well. The guidance is intended for everyone in the practice team who works with new applications for record access. Its aim is to enable you to register new patients for record access safely and efficiently.

This guidance is set out in following the steps:
Step 1 - Receiving a new application for record access
Step 2 - Identity verification
Step 3 - Clinical authorisation
Step 4 - Inform the patient
Step 5 - Providing login credentials
Step 6 - Switch on record access

Step 1 - Receive a new application for record access
Ensure that the patient completes an application form and answers all the questions, including the level of record access that the patient wants: detailed coded record or more. Seek evidence that the patient may be vulnerable to coercion or control to allow someone else to access their record against their wishes. There is a registration form template that you can use in the toolkit.

Every patient who requests record access must be assessed individually. There may be circumstances where record access should be restricted or refused for the patient’s safety. The patient may be vulnerable to coercion or control by another person who wants access to their record as part of a pattern of abuse of the patient.

It is rare for this to happen but no opportunity to seek evidence of vulnerability to coercion should be missed. Everyone who deals with the patient’s request should be alert to the risk. This begins with the practice team member who deals with the patient when they ask for record access, even if they already have access for appointments and repeat prescriptions and even if a GP or practice nurse has recommended online record access to them.

Always ask the standard question to help identify the possibility that the patient may be being coerced to obtain and share their record access by someone else. If you have any suspicion of coercion discuss the possibility with a senior colleague or clinician. There is more information about this in the guidance on Coercion in the toolkit.

Another reason for restricting or refusing record access that must be considered at this stage is the possibility that the patient is unable to understand how to keep their online access secure. They may only need careful advice about how to manage passwords and access to a computer screen or smartphone while they are logged into Patient Online. If they need more help to understand how to use computers and the internet, they may need to attend a learning course. The Good Things Foundation co-ordinate a network of 5,000 local learning centres where patients can learn to use computers and the internet safely.

Patients who apply for Patient Online record access may already have an account to access appointments and repeat prescriptions. Record access carries a greater risk to the patient’s privacy so if a patient asks to add record access, they must verify their identity again and obtain new login credentials. There is more information about this in the Safe Patient Online Record Access guidance in the toolkit.

Step 2 - Identity verification
Confirm the person requesting record access is the person that the practice record relates to. It is essential to ensure that record access is not given to the wrong person. The patient must attend the practice for a face-to-face meeting with a designated and trained member of the practice team.

For proxy access the identity of the patient and the proxy must be verified.
The name of the practice team member who verified the identity of the patient (and proxy where appropriate) and the method of verification used should be recorded in the patient’s notes.

There is more information about the in the Proxy Access guidance and a Proxy Access Consent Form template in the toolkit.

There are three valid ways that the practice can use to verify the identity of an individual requesting Patient Online access:

*Personal documents* - Most patients can prove their identities presenting two forms of documentary evidence. One must carry a photo that clearly matches the appliance of patient. If this document does not carry the patient’s address, then a second item carrying the address at which the patient is registered with the practice is necessary. It should be reasonably likely to have been posted to the address such as a bank statement but not bills or receipts. A full list of acceptable documents is published by the Cabinet Office and available in the document GPG 45 identity proofing. Remember it is thought to be illegal to keep copies of the documents used for verification in the patient’s record.

*Vouching by a practice team member* - There will always be patients who do not have the documents described above (e.g. patients who have recently moved to a new house, travellers or young people living with their parents who do not have acceptable identity evidence). In these cases, an authorised member of staff, who knows the patient well enough may vouch that the patient is who they say they are. Practices must judge each patient on a case-by-case basis while ensuring that the agreed policy takes into account the duration of registration and frequency of patient contact.

*Vouching by answers to questions* - If neither of these methods of verification are available, you can use information in the patient’s health record to verify the applicant’s identity. A trained member of staff may be able to satisfy themselves of the applicant’s identity by obtaining responses to questions derived from information held in the medical records. This should take place discreetly, ideally at a planned appointment. It is extremely important that the questions posed do not incidentally disclose confidential information to the applicant before their identity is verified.

There is more information about this is the Identity Verification guidance in the toolkit.

**Step 3 - Clinical authorisation**
Check that the clinical record is fit to be shared with the patient. This is called “clinical assurance”. The purpose is to ensure that the patient can have record access safely. It is necessary for access restricted to the detailed coded record alone or to the full record. It is only necessary to assure the parts of the record that the patient will see, but the process will have to be repeated if the scope of their access is increased in the future.

It should not be used to hide information that the practice is embarrassed about or to try to avoid litigation over past medical decisions.

There are four parts to the assurance process:

1. Screening for data that the patient should not be allowed to see online and redacting the data where possible. This is sensitive data that may upset or harm the patient, or that the patient has no right to see because it would breach the privacy of third person to whom the practice has a duty of confidentiality. The patient’s personal circumstances should be considered. Where possible the screen should be carried out by a clinician who knows the patient well. If this is not possible, it may be helpful for the screener to confirm decisions about redaction with a senior clinician or a clinician who knows the patient well.

   1. Screening for any data that should be discussed with the patient before access is switched on, such as evidence of abuse or serious diagnoses or test results that the patient may misunderstand: if found, an appointment should be arranged for the patient with whichever clinician is best able to have the discussion with the patient.

2. Curating the records to make sure that they are as clear, accurate and complete as possible; in particular it is helpful to make sure that the problem list is accurate and up-to-date. There is more information about this in the Data Quality guidance in the toolkit.

3. Deciding whether record access should be permitted, restricted or refused. It may help to discuss the decision with the practice Patient Online or safeguarding lead.

All GP systems allow you to redact specific data items, which hides the data from online access by the patient or other health and social care
organisations. The data is not deleted or hidden from practice team members and it will always be available for use in patient care in the practice.

Redaction can often be reversed after discussion with the patient. For example, it may be best to redact an abnormal test result until there is an opportunity to inform the patient directly. Redaction may occasionally need to be permanent.

If sensitive data cannot be redacted it may be necessary to refuse online record access at least until the patient is able to discuss the content of the record with their doctor.

Clinical assurance of the record can be a time-consuming process. It may be necessary to limit the number of patients that the practice can register for record access each month. This makes it possible to advice an applicant how long they may have to wait for their access to be switched on.

There is commercial software that screens the coded data, consultation notes and scanned documents for a set of high risk codes and words. This may speed up the process but an assessment of the circumstances of each individual patient is still necessary. It may not be necessary to redact all the suspect data that the software finds and there may be data in the record that is sensitive to the individual patient that the software has missed.

When data is redacted a note should be added to record the reason for redaction. The note should be redacted as well.

There is more information on the management of sensitive data in the guidance on Safe Patient Online Record Access in the RCGP toolkit.

Step 4 - Inform the patient

Patients need help from the practice to use Patient Online record access effectively and safely. The methods of accessing Patient Online are no different for the patient with record access but the risk of a breach of confidentiality is greater and it is important to ensure that they understand how to keep their access secure.

With regard to record access they may need to know the following:

- The scope of record access may vary from the detailed coded record to include consultation notes and scanned documents. The options may depend upon the GP computer system you use.
- The detailed coded record represents the headlines of the data in their record. It includes information about illnesses and diagnoses, operations, physical examination, lifestyle, screening tests, medication, allergies and adverse drug reactions, vaccinations and immunisations, laboratory and radiology test results and other major investigations.
- Patients can use record access to understand and manage their own health. In particular, they can check information that will help them prepare for consultations. Access to test results and hospital reports before consultations can be very useful.
- Full use of record access requires an adequate level of health literacy focussed on the patient’s health problems. Medical records are technical documents that use medical terminology such as diagnoses and laboratory tests that the patient may not recognise or understand. There are several good websites that provide clear and unbiased information about terms that the patient may come across in the record. Patient’s should remember that the explanations are not personalised to their circumstances and it may be helpful to discuss anything that they are not sure about with their nurse or doctor.
- Some data may be redacted or hidden from online access by the practice if it is thought to be in the patient’s best interests or is confidential information about a third party. Records should be checked for harmful or confidential third-party data should be redacted before record access is switched on and as it is added to the record in future.
- Ensure that patients feel confident to report any questions they have about their record content. There may be things they do not

Clinical scenario: sensitive data

John Brown is an 18-year-old student who has just started at University. He registers with the University practice and hears that his friends are accessing their records online. He decides to request access as well.

His records have been received via GP2GP. The staff at the practice review his records and see that there is a coded record of Family History of Huntington’s Chorea. It is not clear from the record whether John is aware of this history, so they elect to hide this code from online viewing until John has been seen and the doctor can ascertain whether he is aware of this history.
understand in the record, omissions, mistakes, or something that they find upsetting or with which they disagree. Their comments should be discussed openly and honestly, and changes made to the record if appropriate. The practice is under no obligation to change the record unless you think that the change is correct. If you refuse to make a change at the request of a patient, it is reasonable to add a note that the patient asked for the entry to be changed or added. There is more information about the right of patients under the General Data Protection Regulation 2018 to have personal data rectified.

- If the patient sees confidential information about a third party in the record they should log out of Patient Online immediately and inform the practice as soon as possible. The practice will need to investigate swiftly and thoroughly and will need to consider whether the error is isolated or whether it could have occurred in more than one record. In such situations practices will need to follow the Information Commissioner’s guidelines and also to seek specialist advice, such as from the GMC or their medical defence organisations. Having identified the source and extent of the problem, the Information Commissioner’s guidelines and the GPs’ professional duty of candour require the practice to inform the patient(s) affected, apologise and provide a full explanation of what has happened and what steps will be taken to resolve the problem. There is more information available about how to report a breach of personal data to the Information Commissioner.

- The level of access set may be a standard choice by the practice for all patients or may be set according to the needs and wishes of individual patients.

- Depending on system functionality, patients may be able to use their phone or tablet to show elements of their record to other health professionals outside the practice or give specific health professionals 24-hour access to their GP record.

- Patients should be advised not to use paper printouts or direct copies of the information that is displayed in Patient Online in place of legal, insurance, insurance, financial or employment reports or applications.

- Some Patient Online systems also have functionality that allows patients to record their own health data and view it alongside the GP record. Some also allow the data to be copied into the GP record.

Tried and trusted techniques such as “chunk and check” and “teach back” help patients retain information about their health and GP services. Verbal advice about Patient Online should be backed up by accessible written information on paper or on the practice website, which patients with a visual disability often prefer. Patient leaflets, posters, websites and any other means of communication available to the practice can be used to communicate with patients about Patient Online.

You can view and download PDF versions of free patient leaflets and promotional materials about Patient Online produced by NHS England and order paper copies for patients by following the Orderline link on the NHS England webpage.

There is also more guidance on patient information in the toolkit and templates for patient leaflets on understanding abnormal laboratory results and other topics.

Patients can use their detailed coded record as a list of terms to learn about to understand their condition. By encouraging patients to engage with their own health record, they are more likely to become inquisitive and engaged with their diagnoses, investigations and treatments that they identify within their record itself.

There is more information about how to support health literacy in the RCGP Person-Centred Care toolkit.

Useful websites that patients can rely on for information about a wide range of health matters include:

https://www.nhs.uk
https://patient.info
https://labtestsonline.org.uk

Step 5 - Provide login credentials

The next step is to set the agreed level of record access, detailed coded record or more and generate the automatic letter that the GP system will provide. The letter content may vary depending upon whether the patient wants to use the practice system supplier’s Patient Online system or a third-party application.

You may hand the letter to the patient, post it or email it to an address given by the patient. You may leave the choice to the patient provided they understand any risk attached to their choice. For example, they may share a postal or an email
address. Record in the patient’s notes which method of communication they chose.

When the patient logs in to Patient Online for the first time they have to create a new password. Advise them to do this immediately because once it is done anyone gaining access to the credentials letter will not be able to access their Patient Online account.

The login details should not be given to anyone else claiming to be acting on the patient’s behalf, even if the patient is already using transactional services. This is essential protection against unlawful disclosure of confidential information to someone pretending to be the patient.

There is more information in the guidance on Identity Verification and a template for a practice protocol for Identity Verification in the toolkit.

Step 6 - Switch on record access
Finally, unless the decision has been made to refuse record access, all that is required is to switch on Patient Online access to the patient’s record. Be careful to switch on access at the level that has been agreed for the individual patient.

Refusing record access
Sometimes Patient Online record access may present a clear direct risk to the safety of the patient, members of the practice team, or the privacy of a third party, especially when it may not be possible to redact sensitive data. It may be necessary to (and English practice may, within their NHS contract) limit the scope of record access or refuse it completely.

This should only happen after discussion with the practice leads for Patient Online and Safeguarding or after seeking further professional advice from a local relevant agency or national medical indemnity organisation. Access should never be refused solely because the practice is embarrassed about the quality of the record or to try to avoid litigation over past medical decisions.

You should discuss the reason for refusal or restriction with the patient as far as it is possible without revealing the nature of the sensitive information. It may be possible to give the patient access in the future.

The introduction of online patient access to services does not change the right that patients already have to request access to their medical records provided by the subject access provisions of the Data Protection Act (DPA) 2018. The DPA principles and confidentiality requirements apply in the same way as they do for subject access requests for paper copies of the record.

There is more information about patients’ rights to request access to their health record under a subject access request on the Information Commissioner’s Office website.

Documenting patients’ record access
a) At the end of the registration process the complete application form, and the consent form for proxy access, should be scanned and attached to the patient’s record, whatever the outcome of the application.

b) Once the record has been checked for sensitive data and data quality, the outcome and recommendation on whether access should be allowed must be recorded.

c) If online access to transactional services or the record is to be refused or withdrawn at any time the reason must be recorded with the identity of anyone involved in the decision.

d) If data is redacted or redaction is removed, the reason should be recorded.

e) If any change is made to the record, to alter or delete data, as a result of feedback from the patient, the change and the reason must be recorded.