GETTING STARTED WITH ONLINE RECORD ACCESS

Online access is helpful to both patients and GP practices. Record access can help patients manage their long-term conditions and feel more engaged with their care. Access by family members and carers will help them to care for the patient. Record access can present risks to patients and the practice related to privacy breaches and misuse of the data by other people. This guidance describes how to get started with offering and promoting online record access in a way that minimises the risks.

**Why offer online record access?**

Online Record Access is an essential part of collaborative person-centred care. It can help patients manage their long-term conditions and feel more engaged with their care. Access by family members and carers will help them to care for the patient.

Since March 2016 it has been a contractual requirement for English GP practices to promote and offer online access to ‘all information from the patient’s medical record which is held in coded form’ as well as the usual transactional services (see Box 1). The requirement has remained unchanged since then. By March 2017 over half a million patients in England had online record access.

An RCGP survey of practice members in August 2016 showed that common reasons for recommending online record access to patients were:

- See their test results
- See what is in their record
- Help self manage long term conditions
- Support family and carers
- View correspondence
- Prepare for consultations

The same survey showed that there some common perceived risks to online record access. Over 33% of respondents were concerned about at least one of the following:

- Coercion to share online access
- Access to data that may be harmful to the patient
- The wrong person may be given access
- Patients will not keep their records secure
- Patient will disagree with the data in their record

- Parents will demand access to their teenagers’ records

This guidance describes how to manage new applications for online access to minimise these risks and enable patients to use the system safely and get the full benefit of using record access. There is more information about some specific areas in other documents on the Patient Online toolkit.

There are a number of processes that practices should undertake to register new applicants for online record access safely. They can be time consuming but should not be omitted. It may be helpful to start to offer access to the coded record slowly, beginning with a test patient, then rolling it out to a small number of selected patients, involving the patient participation group. Once comfortable with how it all works, the next step is to promote record access more widely. Information leaflets and promotional materials are available from system suppliers and NHS England.

Suppliers may vary in the data that they display online but generally it includes the coded data listed in the graphic from NHS England. GP system suppliers also vary in how they will provide online access to the rest of the record, including free text and scanned documents (see Full medical record access, below). Providing a patient with online record access will not meet the requirements of a Subject Access Request under the Data Protection Act 1998.
Allocate practice team roles and provide training

It is important for practice team members to understand their role when providing online services so that it can be implemented safely. This is particularly true for record access. Consider a training needs assessment for your staff, which you might base on the RCGP guidance found in the Patient Online toolkit and NHS England training tools for practices.

Practice team roles for online record access include:
- Identity verification lead
- Identity verification team
- New applicant registration lead
- New applicant registration team
- Proxy access lead
- Proxy access registration team
- Information governance lead
- Safeguarding lead
- Record data quality lead
- Record checking and redaction team
- Decisions about granting and refusing record access

Box 1: GMS Contract paragraph 16.5.4 and 16.5.5

The Contractor must promote and offer to its registered patients, in circumstances where the medical records of its patients are held on the Contractor’s computerised clinical systems, the facility for a patient to:

1. access online any summary information derived from the patient’s medical records and any other data which the Contractor has agreed that the patient may access; and
2. view online, electronically export or print any summary information derived from the patient’s medical records and any other data which the Contractor has agreed that the patient may access.

... unless:

1. in the reasonable opinion of the Contractor, access to such information would not be in the patient’s best interests because it is likely to cause serious harm to:
   i. the patient’s physical or mental health, or
   ii. the physical or mental health of any other person;
2. the information includes a reference to any third party who has not consented to its disclosure; or
3. the information in the patient’s medical record contains a free text entry and it is not possible under the Contractor’s computerised clinical systems to separate that free text entry from other information in that medical record which is held in coded form.

Establish a protocol for registering new patients for record access

Your system supplier will provide guidance on how you can use the computer system to register new applicants and activate their new account. The RCGP Patient Online toolkit offers further guidance on registration processes and online access, and a registration form template.

Patients new to online record access must either register in person so that their identity can be verified when they are given their login details or arrange for them to be sent to a verified personal email address. Their login details should not be given to anyone else acting on their behalf, even if the patient is already using transactional services. It is essential protection against unlawful disclosure of confidential information to someone pretending to be the patient. The methods of identity verification are summarised in the identity verification guidance on the RCGP toolkit along with a template for a practice protocol on identify verification and an example of a patient
information leaflet on records access.

Consider the circumstances of each individual patient
The decision to provide online access to the detailed coded record is usually straightforward but there are circumstances where the practice should take more care with the decision (see Box 2). Each patient who requests record access must be assessed individually even if they already have access for appointments and repeat prescriptions. The same applies if a GP or practice nurse recommends online record access to the patient. It may be best to refuse access where there is a possible risk to the safety of the patient.

Maintaining record data quality
Records that are well-organised and well-maintained, clear and unambiguous, are the most useful for practices and patients alike. They are the least likely to cause misunderstanding or errors. Conversely, poor quality records are less reliable for direct patient care, more likely to contain data that it is not safe for patients to see, which may upset them or mislead them about their health and harm the reputation of the practice in the eyes of the patient. There is more information about how to create good quality records for Patient Online in the RCGP guidance on data quality.

Online access to view the record should not be refused because the practice is embarrassed about its record or to avoid litigation over medical actions taken in the past.

Redacting sensitive data
Sensitive data is data that may be harmful to the patient or is confidential data about a third person. To ensure that the patient is not surprised by seeing this data online, it should always be redacted for all patients as it is recorded. This principle should be applied to patients who do not have online access. They may have access in the future and in fact it is not usually immediately apparent which patients do currently have record access. Usually redaction can be reversed after discussion with the patient. For example, it may be necessary to redact an abnormal test result until there is an opportunity to inform the patient directly. Redaction may occasionally need to be permanent. This is most likely to be necessary for third-party data.

Box 2: Sensitive data
Patients may be upset by data that they see in their record. The record may also contain data which the patient has no right to see because it would breach the privacy of another person to whom the practice has a duty of confidentiality. Sensitive data of either type should be hidden by redacting it. The data is not deleted from the record but redaction prevents it being displayed through Patient Online. System functionality will vary but all systems should allow data to be redacted (see your supplier’s training materials).

Scenario
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.

Ensure that the patient’s records are checked before access is switched on
There may be sensitive data in the patients record when they apply for record access. It is sensible to check the record before switching access on even if the patient is already using online transactional services. It is a clinical assurance task and should be the responsibility of a clinician, although software that can search the record for potentially sensitive codes and free text or a trained medical summariser can assist. The purpose of the check is to make sure that sensitive and third-party confidential data are redacted so that they are not made available to the patient. If harmful or third-party 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. The final decision to redact or refuse access must lie with the senior clinician.
Establish a policy on when an individual patient may be refused online record access
This should normally only be done where there is a clear direct risk to the safety of the patient, members of the practice team, or the privacy of a third-party. It should never be refused only because the practice is embarrassed about the quality of the record or to try to avoid litigation over past medical decisions.

If sensitive data cannot be successfully redacted and the practice remains concerned about the safety of Patient Online for the individual patient – or in extreme cases, remains concerned that the patient may react violently to information in the record – then the practice may refuse to give the patient online access, or else restrict the level of access. It may be possible to give the patient access in the future, give them access to a reduced part of the record, or restrict access to appointment booking and repeat prescription requesting. Record access should only be refused or restricted 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.

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) 1998. The DPA principles and confidentiality requirements apply in the same way as they do for subject access requests for paper copies of the record.

Well-informed patients
Patient leaflets, posters, websites and any other means of communication available to the practice can be used to communicate with patients about Patient Online. Verbal advice to the patient should be backed up by accessible written information on paper or on the practice website for patients with a visual disability who might prefer to use a screen reader. An automatic message on the practice telephone system can be effective. Local organisations such as pharmacies, post offices, voluntary agencies and libraries may be willing to help promote access.

It might be helpful to enroll members of the patient participation group early on to test the practice processes and provide feedback on how they use record access.

Decide who may recommend patients sign up for online record access. This might include all patients with long-term conditions attending practice clinics or requiring regular blood tests. Access can be especially helpful for patients with multimorbidity.

Consider giving information to help patients protect the security of the record, understand what to do if they spot omissions, mistakes or something that upsets them in the record and how to use the record to engage more fully in their healthcare (see box 4).

Managing complaints from patients
Patients may complain about the data in their record. Patients often check their record to see what is in it as soon as they have access. The practice team should know how to respond if a patient points out an error or an unexpected third-party reference or objects to an entry that they see online and want changed or deleted. This is no different to dealing with challenging or
threatening behaviour from patients in any other situation. Further guidance can be found in NICE guideline NG10 Violence and aggression: short-term management in mental health, health and community settings (May 2015).

The practice must 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 possibly seek advice from specialists, such as their medical defence organisation. The Information Commissioner’s guidelines and the GPs’ professional duty of candour require the practice to identify the source and extent of the problem, and inform the affected patient(s), apologise and provide a full explanation of what has happened and what steps will be taken to resolve the problem.

Data controllers have to report breaches of privacy of confidential data, which are detrimental to the data subject to the Information Commissioner’s Office (ICO). Further guidance is available from the ICO. There is also useful advice from the ICO that is relevant to replying to patients, who raise concerns about inaccuracies in their medical records.

**Full medical record access**

The benefits to patients and the practice of online access may be much greater with full medical record access but the risks to patient and practice safety are greater as well. Free text and scanned letters are more likely to contain expressions of clinicians’ opinions or suspicions about contentious issues such as abuse, potential diagnoses, diagnoses which may be perceived to be stigmatising; or may contain third-party data. They are also much more time consuming to check thoroughly for this sensitive data.

It will be good practice in the future to identify these entries and redact them from patient view as new records are created, and when scanned letters are filed electronically.

Meanwhile GP systems offer granular levels of record access that practices may use. This functionality differs between systems but includes switching on patient access to comments attached to laboratory results, consultation free text or attachments. These settings can be customised for individual patients and may develop in future. They can significantly improve the value of online access to person-centred care while carrying less risk than full record access.

**Proxy access and safeguarding**

Proxy access is the provision of access to the patient’s record to someone else on the behalf of the patient. Where the computer system allows, the proxy should be given their own log in details and the same safety advice as the patient. This makes it clear to the practice who has access to each patient’s record, and the practice can withdraw access for the proxy if necessary at the patient’s request or in the patient’s best interests.

The patient should check the contents of their practice record before allowing anyone else to have access to it. The safest option is to allow proxy online access to the minimum amount of the patient record necessary for the purposes for which proxy access is intended, e.g. proxy access to book appointments or order repeat prescriptions does not require permission to view coded record data. Patients may not realise that proxy access to the repeat prescription list can reveal information about their diagnoses and reasons for attending the practice, e.g. a repeat prescription for contraception.

If the patient wants their proxy to have access to the detailed coded record, it may be possible to restrict access to elements of the record so the proxy can only see elements of the patient record that they want to see. The practice may be able to redact parts of the record so the proxy cannot see them, but then the patient may not be able to see them either. If neither are possible, the patient will have to decide whether to allow the proxy access at all. Record the patient’s consent to proxy access, and the level of access that the patient has agreed for each proxy.

**Proxy access without patient consent**

A third person, such as a carer, someone with parental responsibility for the patient, or power of attorney for health and wellbeing, may ask for proxy access on behalf of a patient who does not have the capacity to make an informed choice. The practice should carefully weigh the benefits to the patient with the risks of giving the third person access and in certain cases, their legal duty to do so. There is detailed advice about this in the RCGP guidance on proxy access.
Box 4: Information for the patient about record access

Advice on the following will help patients use Patient Online safely. Verbal advice should be supported by providing written advice. There are posters, leaflets and other materials for patients on the NHS England website.

1. How to protect their online access, the risks of sharing their login credentials and what to do if they lose their password or suspect that someone has access to it without their consent. Patients should be encouraged to inform the practice if anyone puts them under pressure to share access to their record.
2. The risk of a breach of their privacy if they make paper copies of their records or do not keep their personal access details secure. It must be made clear to patients that once they have accessed, downloaded or printed their record, the security of that information is their own responsibility and they choose to share that information with other people at their own risk.
3. They must feel confident to report omissions, mistakes, or something that they find upsetting or with which they disagree in the record.
4. The limitations of using printouts from Patient Online as the only source of information for completing insurance, employment or legal reports. This is discussed in more detail in the RCGP guidance on Information Governance.
5. If they see 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.
6. Confidence to give the practice feedback on anything they see in the detailed coded record, and report to the practice if they feel that they are vulnerable to being coerced into sharing their online access.
7. Data in their record may be redacted from online display in their own best interests. This is usually a temporary measure for new entries that may be upsetting and normal access will be given as soon as the responsible clinician has had an opportunity to discuss the data with the patient.
8. How to make the best use of booking appointments, ordering repeat prescriptions and the coded record; using the information to improve self-management of their health and feel more in control of their care. Please see RCGP guidance on getting started with online appointments, repeat prescription management and detailed coded record.
9. How to use their online record access to be more engaged in the management of their health. This may be tailored to their specific long term conditions or relate to specific data types such as laboratory results. For further information please see RCGP guidance on multimorbidity.

Summary

Although there are clear benefits to patients and practices, Patient Online may also cause harm if the patient, or someone else, gains access to data that they find upsetting or harmful; if they come across data about other individuals in their record that should have been held confidentially by the practice; or if someone with malicious intent gains access to the record through coercion or a failure of the patient to protect the security of their Patient Online access. This may affect the safety of the patient, the practice, and also practice team members and others if patients react aggressively or violently to what they find in their records.

It is wrong to try to avoid these risks by refusing online access or by failing to record potentially contentious data in the electronic patient record, particularly suspected diagnoses or suspicions of abuse, creating an unsafe, poor quality record that does not fully support patient care. The risks can be reduced by:

- continuous attention to detail in data quality and the recording and redaction of potentially harmful, upsetting data or confidential third-party data
- detailed checks on the content of the health record before online access is switched on
- if sensitive data cannot be redacted, considering either temporarily withholding online access until the responsible GP can discuss the matters with the patient, or else refusing access altogether if the data cannot be redacted.
- careful communication with patients about the risks and how to avoid them when they register for online access
- an open, accepting response to feedback from the patient about errors and omissions, and a sensitive approach to contentious data in the record
- careful watchfulness for indications of coercion of malicious or inappropriate use of proxy access.