Patient Online

Safe Patient Online Record Access

v1.0

Contents

Introduction 2
Examples of risk to the patient or others from record access 2
Safe records for online access 3
Sensitive data 4
Refusing online record access 5
Patient Complaints about the record 6
System configuration 6
Proxy access 6
Practice training 7
Summary 7
Further Reading 8
Introduction

Online access brings benefits for patients and the practice, supporting patient-centred care, especially if the patient has access to their health record. It can help them manage their long-term conditions and feel more engaged with their care. Access by family members or carers will help them to care for the patient.

Online access may also cause problems for both patients and the practice team which can be mitigated with careful implementation. Transactional services (appointments and repeat prescriptions) are straightforward and they create few risks. Record access is more complex and risks may arise from:

- access to potentially harmful or confidential third party data, privacy breaches and misuse of the data by other people:
  - misidentification of the person seeking access leading to access being given to the wrong person
  - poor attention to the security of the data by patients
  - misuse of the data by other people given access to the record willingly or unwillingly be the patient
  - access to potentially harmful data about the patient or a breach of the privacy if the patient sees confidential data in their record that relates to a third party

The guidance describes how to manage Patient Online record access safely by minimising these risks. It is intended for Patient Online and Information Governance leads in the practice but is relevant to anyone who works with Patient Online in the practice.

There is more information about specific areas in guidance on Information Governance, Identity Verification, Proxy Access, Children and Young People, and Data Quality in the Toolkit.

Examples of risk to the patient or others from record access

a) A patient may be vulnerable to being upset or angered by something they see in their GP record. It may be a diagnosis or finding that they do not expect, that they disagree with or find stigmatising or offensive. It may be a family history of genetic diseases; or relate to previous experience of illness in themselves or others. As with any complaint, it is helpful to listen carefully to patient, focusing on their interpretation of the data and the clinical purpose of recording the data.

b) There may be confidential data in the patient's record that was provided by or relates to a third party, to whom the practice owes a duty of confidentiality. The patient should not be allowed to see the data without the consent of the third party.

c) A poor quality record may confuse or upset the patient. Omissions or mistakes may also mislead healthcare professionals.

d) A newly registered patient’s record transferred by GP2GP may not carry redaction settings and the online record may look different to the patient in the new system. Paper records may not make it clear what has been redacted. Online access to the record for new patients should not be switched on until the new record has been summarised and checked.
e) **Failure to recognise that the patient is vulnerable** to coercion to share access to their record unwillingly or unable to keep their access or record secure can put the patient at risk.

**Safe records for online access**

Since 31 March 2016 English practices have been contractually required 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. provided that this does not reveal confidential third party information or material which might be harmful to the patient or healthcare workers. The regulations state that the practice may refuse the patient access if their record contains data, which it may be unsafe for the patient or their proxy to see. This is described in the GP contract:

a) 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:
   - the patient’s physical or mental health, or
   - the physical or mental health of any other person;

b) or the information includes a reference to any third party who has not consented to its disclosure

c) 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.

If sensitive data can be redacted from online display it may be safe for the practice to give the patient access to the rest of the record.

**The circumstances of the individual patient** – Each request for online record access must be assessed individually, looking for evidence of safeguarding risks or the possibility that the patient will be coerced into sharing their online access unwillingly. This is the responsibility of anyone who deals with the patient’s application. It is essential even if they already have access for appointments and repeat prescriptions, or if record access is recommended by a GP or nurse in the practice.

**Advice for 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 should be backed up by accessible written information either on paper or on the practice website for patients with a visual disability who might prefer to use a screen reader.

You can order patient information leaflets about safe Patient Online, including easy read versions, from NHS England at https://www.england.nhs.uk/gp-online-services/support/supporting-material/patient-information-guides/.

**Data quality** – Records that are well-organised and well-maintained, clear and unambiguous are the most useful for practices and patients alike and least likely to cause misunderstanding or errors. Poor quality records may 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. The practice may be able to view each record as it is displayed on-line to the patient to ensure that the view the patient has of their record is competent, complete and logical.
Online access to view the record should never be refused just because the practice is embarrassed about the quality of the record, or to try to avoid litigation over medical actions taken in the past.

There is more information about how to create good quality records for Patient Online in the Data Quality guidance in the Toolkit.

**Sensitive data**

This is data in the patient’s record that may be third party confidential data or potentially harmful to the patient if they see it. If possible such data should be redacted from a patient’s record before they are given the opportunity to see it through Patient Online record access.

**Third party confidential data** - This is data that relates to someone other than the patient, referred to as a third party. It may appear in the patient’s record as:

- An entry or attached file recorded in the wrong patient’s notes by mistake
- Information about the patient given in confidence by a third party (but not a health professional providing direct care to the patient)
- Data about a third party that is confidential to that person and to which the patient does not have a right to access
- A letter or report that refers to more than one patient.

Access to third party confidential data by the patient or a proxy, without the third party’s consent, constitutes a breach of the Data Protection Act 2018 and may put the practice at risk of a fine from the Information Commissioner’s Office.

Before recording information about or provided by a third-party, clinicians should seek and record the consent of the third party to the patient becoming aware of the information they have provided. If the third party withholds consent, it may be possible to redact the information.


**Harmful data** - There is no standard list of dat items that may harm an individual patient. There are things that may be harmful or upsetting to one patient but not to another. Nevertheless it is possible to establish some principles. Some data items are very likely to be harmful, such as serious diagnosis that the patient is unaware of, an entry about substance misuse; or about suspected or actual abuse, violence or coercive behaviour towards the patient or a third party or an opinion that they may perceive to be stigmatising. Data may only be sensitive until a clinician has an opportunity to explain the meaning of the data to the patient. Abnormal test results may need to be redacted temporarily.

Some data may be more sensitive if there is still a risk that someone is still abusing a patient. If they gain access to it, it could lead to serious harm to the patient. Coded family planning data, including medication or any indication that the abuse is suspected by the practice is particularly sensitive. Communication from domestic violence agencies and multi-agency risk assessment conferences (MARACs) may be highly sensitive.
Patients or their proxies may ask for entries to be altered or removed if they disagree with them or find them upsetting or offensive. However, all health professionals have a right (and a duty) to make complete records of facts and their professional opinions about their patients’ health, indicating clearly which are facts and which are opinions.

There is more information about the right of patients under the General Data Protection Regulation 2018 to have personal data rectified at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/ (accessed on 23 October 2018).

Finding and redacting sensitive data - All GP systems have a method of preventing data being visible to patients with online record access. This is generally known as data redaction. Before record access is switched on all the data (detailed coded or full record access) that the patient will see should be checked for sensitive data that needs to be redacted.

It is not possible to create a standard complete list of codes that should be redacted from patient’s record because the sensitivity of a specific code depends upon the circumstances of the patient and whether the practice has had an opportunity to discuss the data with the patient. It is possible to run software that will find high risk codes in the patient’s record before record access is switched on such as the iGPR Toolkit for Record Access from Niche Health.

If the patient is to have access to clinical correspondence or free text, there may be sensitive information that can only be found by reading the records. Once record access is switched on it is important to continue to redact sensitive data as it is recorded. Sensitive test results or hospital reports can be redacted them temporarily, until they have been discussed with the patient.

Consider establishing a practice record keeping policy about recording and redacting new entries of potentially sensitive data even if they do not currently have online record access.

There is more information about about managing sensitive data in the Information Governance and Data Quality guidance documents in the Toolkit.

Refusing online record access to a patient

Online access to the record should never be refused just because the practice is embarrassed about the quality of the record or because of practice concern about litigation over past medical decisions. Access should only be refused where there is a clear risk of serious harm to the safety of the patient or members of the practice team, or to the privacy of a third party.

If sensitive data cannot be successfully redacted and the practice remains concerned about the safety of Patient Online for an 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 record access or restrict the level of access. It may be possible to give them access to a reduced part of the record, or restrict access to appointments and repeat prescriptions.

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 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 subject access requests under the DPA 2018 from the Information Commissioners Office at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

Patient complaints about the record

The practice team should know how to respond if a patient points out an error, a third party reference or objects to an entry that they see online and wants it changed or deleted, although it is no different to dealing with challenging or threatening behaviour from patients in any other situation.

There is more information about how to manage these situations in the NICE guideline NG10 Violence and aggression: short-term management in mental health, health and community settings (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 organisations. 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.

Practice must also report breaches of privacy of confidential data, which are detrimental to the data subject to the Information Commissioner (by phone on 03031231113).

There is more information about how to report a breach of personal data to the Information Commissioner at https://ico.org.uk/for-organisations/resources-and-support/pdb/

There is more information about the right of patients under the General Data Protection Regulation 2018 to have personal data rectified at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

System configuration

It is helpful to have a prominent entry on the patient’s record that alerts practice team members to the fact that the patient has online access to the record. This can be achieved by using a specific code as active significant or major problem such as Registered for online access to local practice (finding) (SNOMED CT code 939511000001001). An alternative is to use a standard system alert or icon but they may not transfer to a new practice in the future or to data shared for direct care with health professionals in other organisations.

Proxy Access

Proxy access is the provision of access to the patient’s record to someone else on the behalf of the patient. 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 the elements the patient wants them 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.

There is more information about this in the Proxy Access guidance in the Toolkit.

**Practice training**

Once patients have online access to their detailed coded record, the impact of data quality becomes a new responsibility for the practice. Not only is this relevant for patients who have online access, it should be borne in mind that any patient may sign up for online access in the future. It should be included in practice training and protocols on data quality and information governance for all staff who contribute to the patient records.

Ensuring that practice team members understand their roles in Patient Online is a very important part of safe implementation of online services. Consider carrying out a training needs assessment, based on the new processes and individual roles of members of the practice team in Patient Online.

**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. 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 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
- Careful communication with patients about the risks when they register for online access
- A open, accepting response to feedback from the about errors and omissions, and a sensitive approach to contentious data in the record
If sensitive data cannot be redacted, consider 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.
Further Reading

Patients’ online access to their electronic health records and linked online services: a systematic interpretative review (BMJ Open 08-09-2014)

Patients’ online access to their electronic health records and linked online services: a systematic review in primary care (BJGP 1 March 2015; DOI: 10.3399/bjgp15X683941)

RCGP resources


Domestic violence (http://www.rcgp.org.uk/clinical-and-research/resources/a-to-z-clinical-resources/domestic-violence.aspx)


RCGP Patient Online: The Road Map in the Patient Online Toolkit
Appendix 1

Summary of when record access may be detrimental to the patient

a) **Sensitive data** - A patient may be upset or angered by something they find in their GP record. They may misunderstand the significance of something and believe a serious illness has been kept from them or a diagnosis has been made that they disagree with. Careful discussion with the patient, focusing on the meaning of the data and the clinical reasons recording the data will often resolve the issue.

b) **Third party data** - There may be confidential data in the patient’s record that was provided by or is about a third party, to whom the practice owes a duty of confidentiality. If someone’s privacy has been breached by record access, they must be informed as soon as possible.

c) **Poor quality records** - especially omissions or mistakes, may be misleading to healthcare staff and lead to poor care. Be prepared to add substantiated past medical history to the patient’s record.

d) **Newly registered patients** - If their old practice record was transferred by GP2GP redaction settings may be removed. They may not be recorded at all in paper printouts. It may be some weeks before the record can be summarised and clinically assured for Patient Online. Online access should not be switched on until the new record has been summarised and checked. Warn patients that if their old practice used a different GP clinical system, the record may look very different.

e) **Coercion** - A patient may be at risk from one or more malign third parties. A child or a vulnerable adult may be coerced by someone who may want access to the patient’s record to control their access to healthcare. This is perhaps the most important risk of using Patient Online. New applicants for online access should always be asked questions that probe whether the patient is under pressure to open a Patient Online account unwillingly. Check the record for evidence of previous domestic violence or abuse. This is not only relevant when a patient applies for online access, it is important to remain vigilant for evidence of abuse or coercion at all times.

There is more advice on how to recognise and prevent this form of abuse in the guidance on Coercion in the Toolkit.

f) **Data security** - If the patient is unable to understand how to keep their online access secure, they may be at particular risk of a third party gaining access to their record.

The Good Things Foundation co-ordinate a network of 5000 local learning centres where patients can learn to use computers and the internet safely.

Appendix 2

Outline practice policy on checking the records for online access

A practice policy on checking patients’ records before they are given online access to their record should be written to establish meet the practice’s requirements. The following are worth considering for inclusion.

a) What is the purpose of checking the record? To ensure the clarity completeness, accuracy and redaction of all sensitive data. Remember that the data may look different in the Patient Online app or webpage from the record in the practice system.

b) Which parts of the record should be checked? All of the record that the patient will be able to see should be checked. If access to consultation notes and clinical correspondence is being considered, it may reduce the risk of missing sensitive data in a large record with many scanned documents and save time by restricting access to new scanned documents or consultation notes made after Patient Online access is switched on. This is called ‘prospective access’.

c) What should be redacted? Data that may lead to harm to the patient and confidential data that relates to a third party. Data that may relate to safeguarding issues should always be redacted. The sensitivity of the data is strongly influenced by the circumstances and views of the patient. The assessment of what should be redacted must be made in the individual patient’s best interests. Clinicians must use their professional judgment and knowledge of the individual in deciding whether data should be redacted.

There is more information about these problems in the guidance on Safe Use of Patient Online Record Access in the Toolkit.

d) Every record must be checked before a patient or a proxy is allowed access to the record online. For proxy access, ensure that the patient has seen the record and is happy to allow the proxy access, possibly after redaction of some data.

e) Who should check the record? This could be a task for the clinician who knows the patient best, another experienced clinician, or the Patient Online clinical lead. It can be done by well-trained non-clinical staff. Agree when to escalate decisions about redacting an item or refusing or restricting the patient’s online access.

f) How many records can be checked? Record checks are time consuming, even with using software to screen the record before a manual check. It may help to limit the number of records checked each month. It helps to be able to warn patients how long they may have to wait when they apply for record access.

g) When should online record access be refused? If there is sensitive data that cannot be redacted, it may be best to refuse of limit record access. Consider discussing the decision with an experienced clinician such as the practice Patient Online or Safeguarding Leads. It may be possible to allow access after a careful discussion with the patient.

h) Should the patient be told that data has been redacted? The reasons for redaction, for refusing or limiting online access should, where possible, be discussed fully and openly with the patient. The goal is to be able to allow the patient online access whenever possible. The reasons for redaction, for refusing or
limiting online access should always be recorded in the patient’s records (in an entry which should also be redacted).

i) In future, practices should feel confident to record whatever is needed, fully and honestly, distinguishing carefully between facts and opinions, and then immediately redact entries, which they feel are currently unsuitable for online viewing.