

 GP Online Services Guidance

*Managing potentially harmful information*

Contents

1. Introduction 1
2. Examples of risk to the patient or others from record access 2
3. Safe records for online access 3
4. Third-party confidential information 4
5. Potentially harmful information 4
6. Finding and redacting potentially harmful information 5
7. Data quality for record access 5
8. Automatic record access 6
9. Refusing online record access 6
10. Information for patients 7
11. Proxy access 7
12. Practice training 8
13. Summary 8
14. Further Reading 9

Appendix 1 - When may record access be harmful to the patient 10

Appendix 2 - Practice policy template for checking records for online access 11

Introduction

Online access to GP Online Services 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 may help them to care for the patient.

On the other hand, online record access may also cause problems for patients and the practice team which can be mitigated with careful implementation. Transactional services (appointments and repeat prescriptions) are associated with risks. Record access is more complex, and risks may arise in a number of ways:

* 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 by the patient
* access to potentially harmful data about the patient or a breach of confidentiality if the patient sees confidential data in their record that relates to a third-party

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

Ref: There are several nuances in how potentially harmful information should be managed in the context of specific aspects of GP Online Services which are covered in numerous guidance documents in the Toolkit.

Examples of risk to the patient or others from record access

1. **A patient may be 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 the patient, focusing on their interpretation of the data and the clinical purpose of recording the data.
2. 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, and of which the patient is unaware. The patient should not be allowed to see the data without the consent of the third-party.
3. **A poor-quality record** may confuse or upset the patient**.** Omissions or mistakes may also mislead healthcare professionals.
4. **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.
5. **Failure to recognise that the patient is vulnerable** to coercion to share record access or unable to keep their access or record secure can put the patient at risk.

Ref: Schust, G., Manning, M. & Weil, A. OpenNotes and Patient Safety: A Perilous Voyage into Uncharted Waters, J General Internal Medicine (2022). https://doi.org/10.1007/s11606-021-07384-2 (accessed 10 May 2022)

Ref: Woodman J et al, Online access to medical records: finding ways to minimise harms, BJGP, 2015, https://bjgp.org/content/65/635/280 (accessed 10 May 2022).

Safe records for online access

In a joint clarification of the GMS Contract commitment 5.10 (ii) for 2019 – 2020, NHS England and the BMA General Practitioners Committee contained the paragraphs in the box below published in November 2019:

NHS England and BMA Joint Statement on Commitment 5.10(ii) in the GMS Contract for 2019-2020

**Safeguarding**

Patient access to any element of their record is subject to appropriate safeguards. These are designed to ensure that access to records

* does not cause harm to the patient
* that legal confidentiality obligations for the non-disclosure of third-party information are adhered to

**Sensitive information**

If based on clinical judgement, it is considered that some information could be harmful to the patient, this information should not be shared with them. This information can be redacted from the patient view and must not be deleted from the record. If system functionality to redact information is not available, the record should not be shared with the patient.

**Third party information**

Legal confidentiality requirements require that where the information is not already known to the patient, any information contained must be redacted, but not deleted from the record. If system functionality to redact information is not available, the record should not be shared with the patient.

Ref: Online Access to GP Digital Records, NHS England and British Medical Association, https://www.england.nhs.uk/wp-content/uploads/2019/12/bma-nhse-joint-statement-prospective-record-access-v1.1.pdf (accessed 22 August 2022)

Third-party confidential information

This is information 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)
* information 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 information 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.

Ref: The Caldicott Information Governance Review of 2013, “Information Sharing, to Share or Not to Share” describes the professional standards for managing third-party data, https://www.gov.uk/government/publications/the-information-governance-review (accessed on 22 August 2022)

Potentially harmful information

There is no standard list of data items that may cause 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 information is very likely to be harmful, such as a serious diagnosis that the patient is unaware of, an entry about substance misuse; or 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 or could be re-traumatising. Abnormal test results may need to be hidden from online view (also known as redaction) temporarily until there is an opportunity to discuss the result with the patient.

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.

Ref: 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 22 August 2022)

Finding and redacting potentially harmful information

All GP clinical IT systems have a method of redacting or preventing information being visible to patients with online record access. GP IT systems manage this differently, the redaction of an entry is usually flagged on the computer screen in the practice. Redacted data is shared with other organisations for direct care but the redaction flags are not transferred to them or, at the time of writing, between practices via GP2GP.

It is not possible to create a standard complete list of codes or concepts that should be redacted from patient’s record because the sensitivity of a specific piece of information 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 on individual's records that will find high risk codes in the patient’s record.

If the patient is to have access to clinical correspondence or free text, there may be harmful information that can only be found by reading the al the documents.

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 temporarily, until they have been discussed with the patient.

It is worth being aware that redacted information and redaction flags may be visible on-screen during consultations and may be seen by the patient or anyone accompanying the patient in the consultation.

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.

Ref: There is more information about managing sensitive data in the “Information Governance and “Data Quality for Record Access” guidance documents in the Toolkit”.

Data quality for record access

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 information that it is not safe for patients to see, which may upset them, or mislead them about their health and damage the essential relationship between the patient and the practice. Practice may be able to set individual computers to display a view of the record as it is displayed online to the patient.

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.

Ref: There is more information about how to create good quality records for record access and how to manage complaints about data quality in “Data Quality for Record Access” in the Toolkit.

Automatic Record access

Patients must apply to their practice for access to their full historic record including historical information or if they want proxy access for a trusted third-party. Each request for access should be assessed individually, looking for evidence of safeguarding risks or the possibility that the patient will be coerced into sharing their online access unwillingly or they are at risk from harm by another means. Most patients with record access will have full prospective record access automatically as part of their access to GP online services.

From 2022 patients who have only GP Online Services for prescriptions and appointments will automatically be given access to their full prospective record including consultations and documents. There is an opportunity to screen all such patients for risk of harm from record access. This can be a complex and time-consuming process, which has been discussed in detail elsewhere in the Toolkit.

Before patients have automatic record access, it is helpful to identify patients who may be at risk of serious harm from online record access. This offers an opportunity to prevent record access switching on automatically by adding a specific SNOMED term (*Enhanced review indicated before granting access to own health record -* 1364731000000104)to the individual’s records. There is then time to have a discussion with patients who may be at risk to come to a joint decision about record access may be harmful. If the decision is to allow record access, the …104 blocking SNOMED term can be overridden by adding the term *Enhanced review* ***not*** *indicated before granting access to own health record –* 1364731000000106.

Anyone who obtains access to GP online services through an NHS Login will have access to their full prospective record without having to apply to the practice. This makes it very important to clinically assure the records of all patients with any GP online services before automatic record access is launched in November 2022 and continue to create and manage all records with online access in mind at all times.

Ref: There is more detailed information about how automatic record access works and how to maintain patient safety in the Toolkit.

Refusing online record access to a patient

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 potentially harmful information cannot be successfully redacted and the practice remains concerned about the safety of record access 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 such as the Summary Care Record or restrict access to appointments and repeat prescriptions.

Record access should only be refused or restricted after discussion with the practice leads for GP Online Services and Safeguarding, or after seeking further professional advice from a local relevant agency or national medical indemnity organisation.

The introduction of online GP 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.

Ref: 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/.

Information for patients

Patient leaflets, posters, websites and any other means of communication available to the practice can be used to communicate with patients about online record access. 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.

Ref: There is guidance that you can use to create practice publications about record access in “Patient Information Themes for GP Online Services” in the Toolkit

Alternatively, you can view patient information leaflets about safe record access, including easy read versions, from NHS England at https://www.england.nhs.uk/gp-online-services/support/supporting-material/patient-information-guides/ (accessed 22 August 2022)

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.

Ref: There is more information about this in the “Proxy Access” and “Children and Young People” guidance in the Toolkit.

Practice training

Once patients have online access to their GP record, the impact of data quality becomes an increasing 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 providing GP online services 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 practice team members.

Summary

Although there are clear benefits to patients and practices, online record access may cause harm if the patient, or someone else, gains access to health information that they find upsetting or harmful; if they come across information 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, the practice team members and others, if patients or others 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, this creates an unsafe poor-quality record that does not fully support patient care. These 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
* An open, accepting response to feedback from the patient 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 hidden.

**Further Reading**

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 Patient Safety Toolkit for General Practice (http://www.rcgp.org.uk/clinical-and-research/resources/toolkits/patient-safety.aspx)

RCGP Safeguarding Adults Toolkit (https://elearning.rcgp.org.uk/mod/book/view.php?id=12530)

RCGP Safeguarding Children Toolkit for General Practice (https://elearning.rcgp.org.uk/mod/book/view.php?id=12531)

RCGP GP Online: The Road Map in the GP Online Toolkit (https://elearning.rcgp.org.uk/pluginfile.php/179161/mod\_book/chapter/760/Patient%20Online%20The%20Road%20Map.pdf)

*Appendix 1*

When may record access be harmful to the patient

1. **Potentially harmful information -** 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.
2. **Confidential third-party information -** 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.
3. **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.
4. **Newly registered patients -** If their old practice record was transferred by GP2GP redaction settings will be removed (at the time of writing this guidance). 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 online record access but if the patient has an NHS Login they will have access to the new practice’s online services, including all future records as soon as they register. Patients will be able to access information entered at the new practice and this needs to be considered as information is entered and new risk is identified. Consider adding the preventive SNOMED term (*Enhanced review indicated before granting access to own health record -* 1364731000000104) when patients register at the practice. Inform patients that if their old practice used a different GP clinical system, the record they see online may look very different.
5. **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 significant risk of using online record access. New applicants for online access should always be asked questions that probe whether the patient is under pressure to open an 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, but it is important to remain vigilant for evidence of abuse or coercion at all times.

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

1. **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. (https://www.goodthingsfoundation.org).

*Appendix 2*

Practice policy template for checking 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.

1. **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 Online app or webpage from the record in the practice system.
2. **Which parts of the record should be checked?** All of the record that the patient will be able to see should be checked. It may be helpful to check the entire record for clinical risk factors related to online record access such as safeguarding risks, impaired intellectual capacity, serious mental health disorders and substance misuse. As with any clinical risk assessment, the decision about whether to allow record access must be individualized and made after discussion with the patient whenever possible.
3. **What should be redacted?** Information that may lead to harm to the patient and confidential data that relates to a third-party.Information that may relate to safeguarding issues should always be redacted. The risk of serious harm 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 information should be redacted.

Ref: There is more information about these problems in the Toolkit.

1. **Every record must be checked** when a patient, or a proxy requests online record access. 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. Consider auditing all patient records before automatic record access is switched on for key risk factors such as safeguarding risks, impaired intellectual capacity, serious mental health disorders and substance misuse.

Ref: There is more information about preparing for automatic record access in the Toolkit

1. **Who should check the record?** This could be a task for the clinician who knows the patient best, another experienced clinician, or the practice clinical lead for GP online services. 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.
2. **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 tell patients how long they may have to wait when they apply for record access.
3. **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 online services or safeguarding leads. It may be possible to allow access after a careful discussion with the patient.
4. **Should the patient be told that information 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).
5. **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.