Online services: Protecting the safety of patients and staff - sensitive data
Guidance for general practice

Executive Summary

All health care interventions have benefits, potential side effects and resource implications, and Patient Online is no different. This guidance covers all aspects of online services that affect the safety of patients, the practice and practice personnel. It explains how to minimise the risks from the content of the patient record and the actions or vulnerability of the patient.

There is little overall risk in patients using the transactional areas of Patient Online, other than coercion by others to allow access to the patient's prescription record. Online access to the patient record carries much greater risks. The record may contain information that can cause harm to the patient. They may discover something online that is upsetting, challenging or something that angers them, without anyone to explain it. In extreme cases that could put the safety of the patient, or members of the practice team, or others at risk. The record may also contain confidential third party data that the patient does not have a right to see.

To reduce the risk that the patient may see sensitive data that may cause them or the practice harm, practices should

- Prepare data quality standards, registration processes, patient information, and staff training.
- Register patients for online access safely, including checking if there is any data that should be redacted from display online, at least temporarily until the practice can explain the data to the patient, or refuse online record access to the patient.

A suitably qualified member of the practice team should check the elements of the record that will be available to the patient, looking at data quality and potentially harmful and confidential third party data. If any such data is found it should be redacted if the computer system allows and then it is reasonable to give the patient access to the rest of the coded data. If it cannot be redacted, it may be best in the interests of patient and practice safety to refuse the patient online access.

Checking the record thoroughly is time consuming, especially for the full medical record including free text and letters. It may be necessary to limit the number of patients that the practice will register for record access each month.

Attention to data quality, and redacting sensitive data, has to be continuous for patients with online access to their record. It is recommended that in future practices should manage all patient records as if the patient has online access, because anyone may request access at any time in the future.

Online access to the record should never be refused just because the practice is embarrassed about the quality of the record, or to try to avoid litigation in relation to past medical decisions.

Box 1: Definitions

'**Redacting**' means 'hiding from the patient online view of the record', not 'removing from the record itself'

'**Coded data**' and '**coded information**' refer to entries within the medical record which are stored in coded form, for example using Read codes, CTV3 or SNOMED-CT, but which are presented on-screen as text.

Introduction

Online access brings benefits for patients and the practice, supporting patient-centered care, especially if the patient has online access to their record. It can help patients manage their long-term conditions and feel more engaged with their care. Finally, access by proxies will help them to care for the patient.

There are risks to patients and the practice team in implementing online services. The risks relating to the use of transactional services (appointments and repeat prescriptions) are not great, but record access carries a new level of risk related to 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 who have been given access to the record willingly or unwillingly by the patient
- harm to the patient arising from the data that they see on line or a breach of the privacy of a third party if the patient sees confidential data in their record that relates to the third party.

The guidance describes how to implement Patient Online safely to mitigate these risks by good preparation for offering online record access and carefully registering new patients, even if they already have access for transactional services. There is more information about some specific areas in other documents and eLearning in the Patient Online Toolkit. They will be referenced for further reading.

Managing Patient Online safely

The GMS contract or PMS arrangements for 2015/16 require practices to promote and offer access to the detailed coded record in addition to the usual transactional services.
The contract and the arrangements allow practice to refuse access to the detailed coded record where it is

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.

Box 2 contains a number of scenarios in which the patient or the practice may be harmed by online access to data in the record.

Box 2: Scenarios where the patient may be at increased risk from the data in the health record

a) A patient may be **vulnerable to being upset or angered by seeing sensitive** information in their GP record in various circumstances. Examples include a specific or generalised anxiety state, depression or psychosis, learning disability or dementia; a family history of genetic diseases; previous experience of illness in themselves or others; they may see themselves as particularly at risk of a serious illness; or are frightened of a stigmatising diagnosis. This may be resolved by careful discussion with the patient, focusing on the meaning of the data in the record and the clinical purpose of recording the data. There is more information about how to manage this sensitive data below in box 5.

b) There may be **confidential data in the patient's record that was provided by or is about a third party**, to which the practice owes a duty of confidentiality (see box 5). The patient should not be allowed to see this data without the explicit consent of the third party.

c) A patient may be at risk from **poor quality records.** Omissions or mistakes may be misleading to healthcare staff. Please refer to RCGP guidance on Data Quality.

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.

The circumstances of the individual patient – 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 nurse recommends online record access to the 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).

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. (Please see example of Patient Information Leaflet). 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. Consider giving information to help patients.

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 RCGP Guidance on Data Quality for Online Access.

Sensitive data – Data that may upset or harm the patient, or alternatively that the patient has no right to see if it breaches the privacy of another person to whom the practice has a duty of confidentiality, must be hidden from display through Patient Online (see the scenario in box 3 and box 4 for a description of sensitive data). This is called redaction (see box 5). It does not delete the data from the record. System functionality will vary but all systems should allow data to be redacted.

Box 3: 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.

Box 4 – Sensitive data that might need redaction from online display

Harmful data

Patient records may contain sensitive data that patients find challenging or upsetting if it has not been explained to them before they come across it online. Examples include a psychological or psychiatric diagnosis; a serious diagnosis that they do not expect, or an opinion that they perceive to have stigmatising connotations (see scenario in box 4). It may also be an entry about substance misuse; or about suspected or actual abuse, violence or coercive behavior towards the patient or a third party.

Someone who is abusing the patient may use access to certain types of coded data as part of the abuse, particularly data about family planning or any indication that the abuse is suspected by the practice. Communication from domestic violence agencies and mul-

ti-agency risk assessment conferences (MARACs) to general practice will lead to highly sensitive letters being filed in the GP practice record. It is important to redact any entries, which might alert an abuser to the possibility that their activities are under suspicion.

Patients may research an entry that they do not understand, and come to the wrong conclusion about what it says about them. It is best to discuss the meaning of entries with the patient before they have online access, redacting data that may be sensitive if that is not possible (see Box 6).

It is not possible to create a list of codes that should be redacted 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.

Patients or their proxies may ask for entries to be altered or removed if they disagree with them or find them upsetting or offensive: in some cases the patient may be verbally or physically abusive, or try to resort to legal measures to have their requested changes effected. 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. Entries that may upset patients may be redacted to protect the safety of members of staff or third parties, possibly temporarily until the entry can be discussed with the patient.

Third party confidential data

Confidential data about someone other than the patient, referred to as a third party, may be recorded in a patient's record. It may be

- an entry made in the wrong patient's notes by mistake ,
- data intentionally recorded because it is relevant to the care of the patient but has been provided in confidence by a third party or there is confidential data about a third party that the patient should not have access to
- data in a letter or report that refers to more than one patient, most commonly reports about siblings or family members.

Third party data does not include data about the patient provided by a third party such as hospital letters. There is more information from the Information Commissioner's Office (ICO) about how to respond to patient's requests for access to personal information here.

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 1998 and may put the practice at risk of a fine from the ICO.

Before recording third-party data clinicians should do the following:

- Seek and record the consent of the third party to the patient seeing the data they have provided before they record the information
- Ensure that the third party understands that the patient may be able to infer the source of the information
- Ensure that the third party is prepared to bear that risk or to have their identity explicitly recorded.

References

The Caldicott Information Governance Review of 2013 lays out the professional standards for managing third-party data.

Redacting sensitive data - Consider implementing a practice policy for redacting such data, temporarily or permanently, for all patients, not just those with current online access (see box 5). Remember that levels of patient access to their record may change in the future. Data not currently available online may be available to the patient in the future.

Box 5: Redaction of data in the record

The GMS contract or PMS arrangements for 2015/16 require practices to promote and offer patient online access to coded data in the record by April 2016, **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 may be unsafe for the patient or their proxy to see. If such 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.

No indication that data has been redacted should be visible to the patient online. The nature of individual patient redactions and the reasons for redaction should be recorded in the patient's record. These entries should be redacted too. The data may be deleted if it was entered in the wrong patient's record by mistake. The practice should comply with all legal reporting requirements.

Recording sensitive data - Practice team members who are responsible for making entries in the patients' records should understand the reasons for redacting data and ensure that all sensitive data are redacted, whether or not the patient currently has online access. This does not remove the need to review the record for harmful or third party data when a patient first asks for online access but will make the task easier and safer.

Impact of proxy access - A patient who has asked for someone to have proxy access may want to redact specific information that they don't want their proxy to see. For example, an elderly, infirm woman might wish her daughter to have proxy access to her record — but only once the entry referring to the termination the patient had before she married had been redacted from the online view. It may be helpful to meet the patient to agree what should and should not appear on the viewable record. The patient should be told that anything redacted from view by a proxy will also no longer be visible online to the patient.

System suppliers training materials should cover the redaction functionality that their system provides.

The practice policy on checking patients' records – The practice should adopt or create a standard policy that covers how the patient's record will be checked before offering online access to the record (see box 6).

Box 6: Practice policy on checking patient's records before online access

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

a) A statement about 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. In some practices the task is carried out well by experienced well-trained non-clinical staff. Whoever does it must understand the practice plan for escalating the problem if they need advice about redacting an item or refusing or restricting the patient's online access.

b) Checking the records effectively is time consuming and may necessitate placing a practice limit on the number of patients that can be assessed for online access in each month. It helps to warn patients how long they may have to wait for access if there is a waiting list for assessment.

c) Check the record thoroughly for quality, clarity of presentation, completeness, accuracy and the presence of sensitive data that should be redacted. (see Boxes 5 and 6). It may be possible to speed up the process by running searches for codes that are most likely to be harmful or upsetting to the patient, but this is not a substitute for carefully viewing the remaining record content.

d) 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.

e) The reasons for refusing, limiting or redaction of online access should always be recorded in the patient's records (in an entry which should also be redacted) and, where possible, discussed fully and openly with the patient. The goal is to be able to allow the patient access to their full detailed coded record whenever possible.

f) With full health record access, that includes free text and letters, a likely future contractual requirement, the principles of redacting data remain the same, but the task is an order of greater magnitude. The most sensitive and detailed information is usually recorded in free text and letters, which take much longer to screen than simple lists of codes.

g) If there is data that cannot be redacted but, which, in the opinion of an experienced clinician such as the practice Patient Online or Safeguarding Lead, would not be in the best interest of the patient to see, the practice should not give the patient access. It may be possible to allow access after a careful discussion with the patient.

h) It is important to record that the patient's record has been checked before individual access is switched on.

i) In the future, practices should feel confident in recording what they need to, fully and honestly, distinguishing carefully between facts and opinions, and then immediately redacting those entries, which they feel are currently inappropriate for on-line viewing.

Refusing online 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 to try to avoid litigation over past medical decisions. It should only be done where there is a clear risk or serious harm to the safety of the patient, members of the practice team, or the privacy of a third party from access to the record.

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.

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 behavior 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 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.

Data controllers have to report breaches of privacy of confidential data, which are detrimental to the data subject to the 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 here.

Staff training – 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.

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 specific codes as active significant or major problems - *Registered for access to Patient Facing Services* (Read V2 9lW..; CTV3 XabsS; SNOMED 936481000000102) - the system alert functionality or a system icon.

Formal 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.

Full medical record access

The benefits of online access to patients and the practice 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 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, or when scanned letters are filed electronically.

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
- An open, accepting response to feedback in regards to 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 information and resources

- GMS contract
- PMS arrangements
- RCGP Guidance: Proxy Access, Coercion, Information Governance, Data Quality
- Patient Information Leaflet
- Information Commissioner's Office (ICO) advice on notification of data security breaches to the ICO
- ICO's Subject Access Code of Practice
- ICO advice on correcting inaccuracies in the record
- NICE guideline NG10 Violence and aggression: short-term management in mental health, health and community settings
- 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 Patient Safety Toolkit for General Practice
- Safeguarding Children Toolkit for General Practice
- Patient Online: The Road Map