Online services: Information governance and online access

Guidance for general practice

Executive Summary

This guidance describes the information governance required to manage Patient Online effectively and safely. Information governance is the term used to describe how healthcare organisations manage the information they handle. It is based on the balance established in law between privacy and sharing of confidential data, in the Data Protection Act 1998 in particular.

The practice has a duty to ensure the patient understands the potential implications of having online access to book appointments, request repeat prescriptions or view their record. This includes the patient's responsibility to maintain the safety and security of the information in their record.

Online access may be requested by the patient or suggested by the practice but whoever proposes it, it is essential that the practice confirms the identity of the person who will receive access to the patient's record, normally the patient.

The patient might choose to share their login details with another person, who can then act on their behalf to book appointments, or request repeat prescriptions for them or access their records in support of their healthcare. If GP system functionality allows, it is much safer for the patient's representative or carer to have their own separate account and login details. This is referred to as Proxy Access and should be recommended to patients in preference to sharing one set of login details whenever it is available. Patients should only opt for proxy access when they trust the other person to act in their best interests at all times.

Proxy access should only be given to named individuals whose identity has been verified. There are special circumstances that affect parents' right of online access to their children's health record, relating to their legal parental responsibility and the age and capacity of the patient to make informed decisions about access to their records.

The practice has a responsibility to ensure that patients are not abused by third parties who gain access to their record, possibly by coercing the patient into giving them online access. Patients may also be affected by data that causes them harm and third parties may be harmed if the patient gains access to confidential information about them in the patient's record.

The practice must also understand the potential impact of poor data quality on the patient and the practice's reputation.

This Guidance provides advice on how the practice should manage Patient Online to minimise any risks to information governance.

Introduction

Information governance (IG) is the term used to describe how healthcare organisations manage the information they handle. It covers the behaviours and standards needed to ensure that co

nfidential information is handled lawfully, securely, effectively and in a way that maintains public trust. It is based on the balance established in law between privacy and sharing of confidential data.

This guidance describes the information governance required to manage Patient Online effectively and safely.

Subject Access Requests

The introduction of Patient Online access to GP practice services and patient records does not change the right that patients already have to request access to their medical records through the subject access provisions of the Data Protection Act (DPA) 1998.

Although the DPA principles and confidentiality requirements apply equally to online access and subject access requests (SAR), there are significant differences between them. A practice must fulfill a request from a patient for access to information about the patient that they hold. They must provide them with a copy of the information requested, but they may withhold information that is exempt under the DPA. Confidential personal data which relates to a third person and data which is likely to cause serious harm to the patient or another person is exempt from the SAR legislation and may be withheld by the practice.

The threshold for refusing access to information, because it is potentially harmful to the patient, may be lower for online access, but it is better to allow access after redacting the harmful information from display online if it is possible. SARs are fairly uncommon and cover the record at one point in time; many more patients will ask for online access to their records and their access will continue over time.

New applications for online access

The practice has a duty to ensure the patient understands the potential implications of having online access to book appointments, request repeat prescriptions or view their record. This includes the patient's responsibility to maintain the safety and security of the information in their record. They should be given relevant verbal and written information. There are helpful patient information leaflets on the NHS England website.

The patient should be asked to confirm that they have understood the advice. There is an example of a recommended application form template in the RCGP Patient Online Toolkit, which includes suitable questions for the patient who is applying. (Example Registration Form: Word / PDF).

Verify the identity of anyone given login details for online access

Online access may be requested by the patient or suggested by the practice but whoever proposes it, it is essential that the practice confirms the identity of the person who will receive access to the patient's record, normally the patient. There are three ways of verifying identity:

- Inspection of acceptable identity evidence, usually documents presented by the applicant

- Vouching by a member of staff who knows the patient well
- By confirmation of information in the patient's record (while not disclosing information in questions, and taking care to avoid breaching the patient's privacy).

There is more information about this in the RCGP Guidance on Identity Verification.

Proxy access to adults' records

The patient might choose to share their login details with another person who can then act on their behalf to book appointments, or request repeat prescriptions for them or access their records in support of their healthcare. If GP system functionality allows, it is much safer for the patient's representative or carer to have their own separate account and login details. This is referred to as Proxy Access and should be recommended to patients in preference to sharing one set of login details whenever it is available.

If the proxy has their own access account, the practice can limit the proxy's access if the patient requires; perhaps just to allow them to book appointments or order repeat prescriptions for convenience, without providing record access. The practice can also switch off the proxy access if the patient wishes it or if problems arise. Patients should only opt for proxy access when they trust the other person to act in their best interests at all times.

Proxy access should only be given to named individuals, and not to organisations where the patient and the practice may lose track of who actually has access to the record. Patients should be advised not to provide access to insurance companies or solicitors who request access to their medical records and if the practice suspects that the patient is being coerced into requesting proxy access, it would be better to withhold access until the situation can be fully investigated.

Box 1 Scenarios of unwanted effects of sharing online access with a third party

Patients requesting proxy access should check what is visible online in their record before allowing someone else to have access to it.

- They should be aware that there could be details in their record that reveal information about them without specifically stating it. Even with limited access to just appointments and repeat prescriptions a proxy may learn more about their health than they may expect. For example there may be repeat medication that indicates a particular health condition.
- The elderly mother requesting proxy access for her daughter, but needing to be aware that she should first think about redacting her pre-marital termination.
- If proxy access login details are given to a care home or a care team, it may not be clear who has access and a member of staff who leaves the organisation may retain access if the proxy login details are not changed

It is essential to confirm that requests for proxy access have the explicit consent of the patient. Verify the identity of the person who will be given access and the patient giving consent.

When the patient lacks capacity to give consent, it may be in the patient's best interests for the practice to give someone proxy access. There is more information about proxy access and identity verification in RCGP guidance in the Patient Online Toolkit.

Proxy access to children's and young people's records

It may be in a child's best interests for their parent(s) or legal guardian to have proxy access to their record and services online, especially if they have long term conditions. When someone requests online access to a child's record, it is essential to establish that they have parental responsibility and right of access to the child's record. Their identity must be verified.

Up until their 11th birthday it can be assumed that the child is not competent to make a choice about this. At some point after this the child is likely to become competent to do so. This may become a problem if a young person becomes competent to seek confidential help from the practice but is inhibited from doing so by parental proxy access or if there is a risk that the parents discover something that the young person would want to keep confidential. For this reason consider switching off proxy access for all children on their 11th birthday.

A young person who is deemed to be competent may choose to have online access or allow parental proxy access at any age. Parental access may be restricted to booking appointments and ordering repeat prescriptions. Each decision for the practice to allow access must be made by the practice on a case by case basis after a careful assessment of the young person's competence and best interests.

After their 16th birthday every young person is deemed to be competent to make an informed choice about proxy access unless a careful assessment shows that they do not have the capacity to understand the implications of the decision.

It may be helpful to discuss difficult cases with the practice or local safeguarding lead, particularly if there are existing safeguarding concerns. Practices should not avoid recording safeguarding concerns in case an abuser may become aware that abuse has been detected. Such data should be redacted, where the computer system has the functionality to do so, so that it is not visible online.

There is more information in the RCGP Guidance on Proxy Access on behalf of Children and Young People in the Patient Online Toolkit. The GMC provides detailed guidance on confidentiality, including confidentiality and children. Advice or the local safeguarding lead can also be sought from medical defence organisations.

Safeguarding

Practices should also bear in mind that some patients may be coerced by others into sharing information unwillingly or they may reveal information without realising the implications for them of not keeping the information confidential. For guidance about what a member of the practice should do if a staff member has any suspicion that a patient may be coerced or tricked into providing access to their health record to a third party, please read the RCGP Guidance on Coercion.

If there is evidence of child abuse, consideration should be given to refusing or withdrawing online access and any mention of abuse in the record must be redacted from online display.

Data quality

The quality of data in a patient's record can be assessed by the extent to which it meets the various purposes that the record is used for. For online services this means that it must be clear and unambiguous for the patient to understand, without displaying information that might be harmful to the patient or others or confidential to other (third) parties. Poor data quality may be confusing and may mislead both patients and clinicians with a negative impact on the patient's health care and safety.

The starting point is to think of data quality in terms of five headings: Complete, Accurate, Relevant, Accessible and Timely (CARAT). There are specific aspects of data quality that affect particular parts of the record such as problems and diagnoses, other consultation codes, data from summarising, and laboratory results. There is more about this in the RCGP Guidance on Data Quality.

Patients' reaction to the information in the record

Many patients' records contain very sensitive information, which could cause significant distress or harm. Patients may be distressed by seeing new test results that are abnormal without an opportunity to discuss them with their doctor, or by information they have forgotten or find offensive.

The practice should ensure that when a patient applies for record access they are aware that the record may contain information that they don't understand or that might worry them. There may be inaccuracies or omissions, abnormal results or bad news in the records. The patient should be advised to contact the practice as soon as possible if any of these things happen and the practice must be ready to discuss such worries with the patients. There is helpful information for patients about these issues on the NHS England website.

Practice team members should be careful when entering data in the record that may be upsetting, confusing or misunderstood by the patient. Such data should be redacted from online display, perhaps until the practice has had time to discuss the information with the patient. There is more about this in the RCGP Guidance on Protecting the Safety of Patients and Practices – Sensitive Data in the Patient Online Toolkit.

Confidential third party information

Patients' records may contain confidential information that relate to a third person. This may be information from or about the other person. It may be entered in the record intentionally or by accident when, for example, a letter about another patient is attached to the patient's record. Even if they are not named, it may be possible for the patient to work out their identity. If there is any suspicion that the third party's identity may be confidential, the patient should not be allowed access to it.

When the information is confidential to the third person, the patient must not be allowed access to it without the third person's consent. If confidential third party information is entered in the patient record, it must be redacted if possible, or online access to the record should be refused. This does not apply to information about or provided by a third party that the patient would normally have access to, such as hospital letters. There is more information about what constitutes confidential third party data in the Information Governance Review – Information to share or not to share.

Box 2: When is third party data not confidential?

This is information in a patient's health record that relates to another person where there is no need for the practice to prevent the patient having access to the information. This may occur because the third party has consented to the patient having access to the information or the information is not confidential:

- Information about third parties provided by the patient usually need not be redacted, as access to this by the patient would not breach confidentiality.
- Entries made by care professionals, including additions to the record such as letters from other organisations are not third party information. These are created with the understanding that the patient has a right to see them.

When patients apply for online record access they should be advised that if they come across anything that should not be in their records, whether or not it relates to another identifiable person, they should log out of their record and let the practice know as soon as possible. The practice will need to switch off online access, including any proxy access, investigate swiftly and thoroughly and take appropriate action. This may be to obtain the third party's consent to the patient having access to the information, to redact the information, delete it if it has been entered in error or, if no other action is possible, to refuse the patient online record access in future. Decisions must be made on a case-by-case basis.

In such situations practices will need to follow the Information Commissioner's guidelines and probably seek specialist advice, possibly from their medical defence organisations.

Having identified the source and extent of the problem, the Information Commissioner's guidelines and the GPs' professional duty of candour require the practice to inform the patient(s) affected, apologise and provide a full explanation of what has happened and what steps will be taken to resolve the problem.

Data controllers, in this case the practice, do have to report breaches of privacy of confidential data which are detrimental to the data subject (whether it is the patient or a third party) to the Information Commissioner's office. Further guidance is available from the Information Commissioner's office.

There is general information about managing disclosure of third party information in the Information Commissioner's Office guidance on Subject Access Requests. Medical defence organisations have also produced useful guidance on how to handle third-party data and on general principles of confidentiality.

Practice actions to support information governance for patient online access

While each practice may face unique situations and circumstances, there are some information governance issues that can be predicted and planned for when implementing online services.

- Practices need to remain up to date with their NHS Information Governance Toolkit assessments to ensure they are managing information responsibly in compliance with their legal obligations. The Information Governance Review is a useful resource about the practice's responsibilities.

- A designated information governance lead for Patient Online services should be appointed. This may be the practice Caldicott Guardian.

- Information governance policies should be put in place that provide clear guidance to help staff manage Patient Online safely and securely. They must be updated to cover the provision of access to online services, which may change with time. All staff members involved in Patient Online services need to understand the information governance requirements of their roles.

- A designated safeguarding lead for Patient Online services should be appointed and safeguarding policies put in place that provide clear guidance to help staff manage patient online access safely.

- Staff members who make entries in patient records should be aware that patients will be able to view their entries online, and bear this in mind when deciding what to enter in the records. In addition to the usual care over data quality, staff should be aware that abbreviations, euphemisms and medical jargon may be misunderstood by patients and avoid recording third-party data unless it can be safely redacted. There is more information about this in the RCGP Guidance on Data Quality in the Patient Online Toolkit.

- Screening records for sensitive data before allowing access can be a time consuming process, especially if retrospective access to the entire medical record is offered to patients, including attachments and consultation free text. Practices should have a process that allows this to be done in a timely fashion, using available resources. If there are frequent requests for online record access it may be necessary to limit the number of records that can be checked each month. It is better to check a few records carefully than not check the record thoroughly. If demand is high it may be better to offer limited access, if the GP system allows, as an interim measure, until the full record can be screened.

Information governance issues should be discussed regularly at practice meetings to help ensure policies are maintained and adhered to. Practice staff members should be encouraged to help each other raise standards of handling information about patients.

Practices are encouraged to seek specialist advice on information governance issues locally from Local Medical Committees, medical defence organisations, the clinical commissioning group (CCG) Caldicott Guardian or the NHS England's Local Area Teams.

Advice can be sought centrally from the Information Governance Alliance, a team drawn from DH, NHS England and HSCIC by writing to IGA@nhs.net.

System suppliers can provide advice about the best way to use their system to provide safe and secure online services.

Further Information and Resources

- GMC Confidentiality Guidance
- HSCIC: Information Governance (IG)
- HSCIC: Caldicott Guardians
- Information Commissioner's Office guidance on Subject Access Requests
- Information Governance Review – Information to share or not to share
- MDU Disclosing records to third parties
- MDU Medico-legal guide to confidentiality
- National Register of Caldicott Guardians
- NHS England Materials for patients and Patient information leaflets
- NHS Information Governance Toolkit
- NHS: Keeping your online health and social care records safe and secure
- Patient Online: The Road Map
- Patient Online: The Road Map: Information Governance Risk Register
- RCGP example registration form: Word / PDF
- RCGP: It's your practice – A patient guide to GP services
- RCGP Patient Online Toolkit
- RCGP Guidance Documents:
  - Coercion
  - Data quality
  - Identity verification
  - Protecting the safety of patients and practices – sensitive data
  - Proxy access on behalf of children and young people

Appendix:

Information Governance planning checklist for practices

This checklist is a list of considerations which practices can adapt into a policy if they wish. It may form part of the practice policy and protocols for Patient Online.

Patient Online Information Governance Checklist		
Index		**Comment**
Information Governance general foundations		
1	The practice should seek to achieve a “satisfactory” in the NHS Information Governance Toolkit.	
2	There should be clear practice guidelines for staff on information handling and data quality.	
3	Patient information will normally be divulged to anyone not directly involved in their care only with the patient’s explicit consent. Exceptions may occur in special circumstances, such as where it would be required by law, is in the public interest, or to help protect a vulnerable child or adult.	
4	The practice should provide information for patients that explains that the practice has policies in place to ensure that access to information from personal health records will only be granted where there is a clear legal justification.	
New applications for online access		
5	Where online access is being considered, the practice has a duty to ensure the patient understands the potential implications.	
6	Patients should be given verbal and written information about the risks and how to manage their online access safely and securely. There are useful leaflets for patients on the NHS England Patient Online website.	
7	The application form that patients complete to request online access should include questions that ask patients to confirm that they have understood the advice. There is a template for an application form in the RCGP Patient Online Toolkit.	

Index		Comment
8	The information for patients should include the following: • The patient must let the practice know as soon as possible if they come across anything that should not be in their records, whether or not it relates to another identifiable person, or if they find any errors, omissions, anything that they disagree with or anything else that troubles them. • The practice welcomes the feedback and will investigate and reply to them as soon as possible. • Once they have accessed, downloaded or printed their record, the security of that information is their own responsibility. It will be at their own risk, if they choose to share that information with other people, , make paper copies of their records or do not keep their personal access details secure. • The record presented online cannot be assumed to be fit to act as an insurance or legal report. It may only show some of the required information and may not present it in the way that the report requires. • Someone who has access to the record may use it to harm the patient. Patients should be aware of the danger of being coerced into sharing information unwillingly, and tell the practice if it happens or they suspect it may happen. The practice will support them fully. (Practice staff involved in managing new applications should be able assess the risk of coercion and discuss it with the patient when they have concerns). • If the patient knows or suspects that their record has been accessed by someone without their agreement, then they should change their password immediately. If they can't do this for some reason, they should contact the practice so that staff can remove the online access until the patient is able to reset their password. (Staff members need to know how to manage password resets for patients and how and when to remove online access to safeguard patients and their confidentiality.) • The practice takes the security and confidentiality of the records very seriously.	
Identity verification		
9	Applicants for online services must have their identity verified before access is switched on to prevent unlawful disclosure of confidential information to someone pretending to be the patient.	
10	Practices may wish to nominate an access management lead to take responsibility for identity verification procedures.	

Index		Comment
11	Verification should be simple, quick, patient-friendly and not overly demanding for the practice or the patient. It should be done by using personal documents, vouching by a member of the practice team or by using information in the patient's records.	
	Sensitive data	
12	Before recording anything in a patient health record about a third party or information from a third party that might be confidential, clinicians should consider doing the following: 1. Seek and record the consent of the third party to the patient seeing the data they have provided before they record the information 2. Ensure that the third party understands that the patient may be able to infer the source of the information even if their identity is not recorded 3. Ensure that the third party is prepared to bear that risk or to have their identity explicitly recorded. The third party may decide to withhold the information or make it clear that they do not wish it to appear on the record of the patient.	
13	Before enabling online record access for a patient, their record must be checked for confidential third-party information and information that has the potential to harm the patient or the practice.	
14	If, on checking the record, confidential third-party information is found, consider taking one of the following actions: 1. The data may be redacted permanently or until the third party gives consent for the patient to see it 2. Deny access to the part of the record containing the sensitive data by other means, such as limiting access to data only recorded at a later date, or to that part of the record, e.g. free text or letters. 3. But on occasions, it may be that sensitive information cannot be hidden or redacted, so enabling online access is then not appropriate.	

Index		Comment
15	If potentially harmful data is found consider taking one of the following actions: 1. The data may be redacted permanently or until an appropriate person in the practice is able to discuss the meaning of the data with the patient 2. Deny access to the part of the record containing the sensitive data by other means, such as limiting access to data only recorded at a later date, or to that part of the record, e.g. laboratory results. 3. But on occasions, it may be that sensitive information cannot be hidden or redacted, so enabling online access is then not appropriate.	
Data quality		
16	Data that is routinely recorded about every patient should be fit for viewing by the patient online, whether or not they currently have record access. The record must be clear and unambiguous for the patient to understand, avoiding displaying information that might be harmful to the patient or others or information that is confidential to other (third) parties. (Poor data quality may be confusing and may mislead both patients and clinicians with a negative impact on the patient's health care and safety.)	
17	Before enabling online record access for a patient, the record must be checked for quality as well as sensitive data. Where necessary the data quality should be improved. This applies particularly to coding for problem titles where omissions, duplications or poor coding should be corrected as far as the system functionality allows without changing the historical record.	
Proxy access		
18	Where system functionality permits, practices should offer separate login details to identified individuals who will be the patient's representative or proxy. This is safer and more flexible for patients than sharing a single set of login details with someone.	
19	Proxy access should not be given to organisations or care teams.	
20	The proxy may be nominated by the patient. The patient should complete a consent form for the practice. Someone may also act on behalf of a patient who lacks the capacity to make an informed choice about proxy access. In this case the practice must ensure that it is in the patient's best interests for the individual requesting access to be given proxy access. The decision and reasons for it should be recorded in the patient's notes.	

Index		Comment
21	Nominated third parties may be granted full access to a patient record or their access may be limited to booking and cancelling appointments, or ordering repeat prescriptions. This may depend on the patient's preference or the need to minimise the risk that the proxy will see sensitive or confidential information in the record.	
22	The identity of the person being given proxy access and the patient giving consent must be verified in the usual way before proxy access is switched on.	
Children and young people		
23	Up until their 11th birthday it can be assumed that a child is not competent to make a choice about parental proxy access to their record. People with parental responsibility may be given proxy access to the child's online services and record unless the practice suspects that it would not be in the child's best interests, e.g. where there are safeguarding issues. Each request for child proxy access must be made on a case-by-case basis and the reasons for the decision recorded in the child's notes.	
24	On the child's 11th birthday, GP computer systems should automatically restrict the scope of existing proxy access or withdraw access altogether. Consider giving the parents warning that this will happen.	
25	Parental proxy access may be reinstated if, after discussion with the parent(s) requesting access, the child's GP believes that proxy access would be in the child's best interest. The reasons for reinstatement should be recorded in the child's notes.	
26	At some point after their 11th birthday young people are likely to become competent to make an informed choice to ask for online access, for their parents or another representative to have proxy access, or for current proxy access to be switched off. The practice should have a protocol that enables the decision to allow online access appropriately on a case-by-case basis. Again the reasons for the decisions made should be recorded in the patient's notes.	
27	On the young persons' 16th birthday, the systems should switch off all the remaining proxy access except where the young person is competent and has given explicit consent to the access.	

Index		Comment
Audit trails		
28	Audit trails may record details about everyone who has accessed to a patient's record. Where system functionality allows, practices make audit trails available to a patient if they express concerns and ask to see it.	
29	Patients may need help to interpret the content of audit trails.	