Principles of Data Sharing for GPs and LMCs

August 2013

This advice is based on careful examination of the relevant legislation and guidance but it does not constitute a formal legal opinion.
Broadly there are two distinct categories of data sharing agreements between practices and other organisations: those that involve care record sharing and those that involve data reporting. Different considerations apply to these categories.

This is intended as guidance for GPs and LMCs who are being asked to approve or sign up to either of these types of data sharing agreements and has been taken from the Information Commissioner’s Office (ICO)’s code of practice {1} which GPs and LMCs should be familiar with. For further specialist guidance, the relevant codes of practice and for a free practice visit for advice please see the Information Commissioner’s Office (ICO) website www.ico.org.uk.

Currently GPs are being asked to sign up to a daunting plethora of “Data Sharing Agreements” and these “DSAs” - which share data between data controllers (e.g. a GP practice and a say a hospital) - are being requested to facilitate a wide range of purposes. However there are those requested by CCGs and Local Authorities for commissioning purposes which fall into the category of data reporting agreements using anonymised or pseudonymised data to produce, for example, performance dashboards for payment or quality improvement purposes and those requested for clinical care. These could include for example a request from a hospital for an agreement to allow ward pharmacists access to the GP patient record when a patient is admitted to hospital and these latter agreements involve care record sharing. Clearly distinct considerations apply to each (most notably around patient consent) and practices must be very clear at the outset whether they are being asked to agree a mechanism for data reporting (in which case anonymised or pseudonymised data is sufficient and more appropriate) or an agreement for sharing patient care records. A key problem we have encountered is that some organisations (notably CCGs) are requesting care record sharing inappropriately (and in some cases illegally) when their needs can be met by a data reporting agreement with anonymised or pseudonymised data.

Few GPs find evaluating the reasonableness of requests for data sharing an easy matter and mindful of their duty to protect patient confidentiality, most are understandably anxious about sharing their patients’ personal data. This guidance covers DSAs which are a systematic, routine form of data sharing involving general principles and often large volumes of data. It does not cover the ad hoc, one off, sharing requests that practices receive. Nor does it cover sharing of data with data processors - where another party processes data on a data controller’s behalf. The ICO have issued separate guidance on these circumstances. www.ico.org.uk.

Before a practice can safely share patient information it must ensure its own information governance is in order.

The Data Protection Act 1998 (DPA) requires organisations to have appropriate technical and organisational measures in place when processing (recording, sharing, viewing of data) personal data. Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements. These principles have been subsumed into the NHS confidentiality code of practice{2}.
This is a subject beyond the scope of this advice but at its most basic it means: keeping patient records up to date and accurate; it means implementing the Caldicott principles \(^3\) including the most recent one to correct an overly cautious stand on data sharing - the so called 7th Caldicott principle i.e. the duty to share information can be as important as the duty to protect patient confidentiality as long as such sharing is within the framework set out by the other 6 principles (see Appendix 1); and the DPA’s 8 principles (see Appendix 2); it means being familiar with the ICO’s Data Sharing Code of Practice; having a Caldicott guardian in the practice and to be registered with the ICO.

GPs are familiar with protecting patient information they hold themselves as data controllers, but establishing appropriate security in respect of shared information may present new challenges. One of the thorniest issues for GPs is the question of when the duty of confidentiality can be breached. Patients’ care records can be shared in most circumstances only with the patients’ consent. Otherwise the duty of protecting patient confidentiality can be breached only when under a legal framework there is: a) a higher duty, e.g. child protection; b) a specific legal framework, e.g. notifiable diseases; c) the requirement to supply coded GP data to the Health and Social Care Information Centre under authority given by the 2012 Health and Social Care Act, or d) support from the Secretary of State (SoS) (section 251 of the NHS Act 2006 carried over into the 2012 Act) or the Research Health Authority (RHA). It is the SoS who gives s251 support for non-research purposes and the RHA for research purposes. Advice to the SoS and the RHA is given by the Confidentiality Advisory Committee of the Research Health Authority (CAG HRA).

**Implied consent**

Briefly all personal data needs explicit informed patient consent for it to be shared unless it is shared within the NHS family and for legitimate reasons- i.e. for patient’s treatment or care- in which case implied consent generally applies. Implied consent can be relied on where there are very strong grounds for believing that the vast majority of patients have already given consent. Patients expect their data to work for them in this context because it benefits them. An example of this would be a standard GP referral letter. A GP could reasonably assume consent because all patients understand a referral letter will be sent with a referral that provides clinical information pertinent to the referral. Explicit consent is not required. Similarly, parents know the NHS compiles data on childhood immunisation coverage and invitation letters are sent out on behalf of the practice by the PCT or CCG sometimes and in some places. Patients know that screening programmes are run on the basis of some knowledge of a woman’s smear status. So we do not ask consent to let the NHS central bodies know that the woman did not attend her last smear, we assume implied consent to the screening programme and the information sharing that is involved.

**Explicit consent**

Outside the NHS family, there is no public expectation that personal health data will be shared. That is why it is necessary to obtain explicit consent, and why it is important we always insist on it. Further, implied consent cannot be implied for new data flows where patients could not reasonably be expected to know that the data flow will take place.

**Data sharing agreements (DSAs) check list for GPs and LMCs**

DSAs (sometimes known as ‘data sharing protocols’) set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is essential to have a DSA in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.
Please note, though, that the organisations the data is disclosed to will take on their own legal responsibilities in respect of the data, including its security. Therefore it is important to note that GP practices are not liable for breaches of confidentiality by the organisation with whom data is shared, provided the data was lawfully shared in the first place. It is the receiving organisation that is liable for their own breaches of information governance.

The summary check list on the following page provides a practical and pragmatic ‘working’ list of points to incorporate into any data sharing agreement and is derived from existing legislation and guidance.

The Law Commission plans to review the extensive and confusing legislation on data sharing between public bodies. A report on the overall scope of the complex legal issues involved should be published in May 2014.

Check List:

GPs and the LMC should not agree a data sharing agreement unless the agreement has documented answers to the following 10 point checklist:

1. The purpose, or purposes, of the sharing;
2. The potential recipients or types of recipient and the circumstances in which they will have access;
3. The data to be shared;
4. Patient consent required;
5. Data quality – accuracy, relevance, usability etc.;
6. Data security - accessibility;
7. Retention of shared data- how long will data be retained and under what circumstances;
8. Patients’ rights – procedures for dealing with patients who do not wish their data to be shared (patient dissent); access requests, queries and complaints;
9. Review of effectiveness/termination of the sharing agreement;
10. Sanctions for failure to comply with the agreement or breaches by individual staff.

Interrogating a data sharing agreement: The questions you need answered:

Use the check list to interrogate the data sharing agreement you are presented with.

When deciding whether to enter into an arrangement to share your patient’s personal data you must identify the objective that it is meant to achieve. You should consider the potential benefits and risks, either to individuals or society, of sharing the data. You should also assess the likely results of not sharing the data. You should interrogate the data sharing agreement and ask yourself:

1. The purpose, or purposes, of the sharing;
   What is the sharing meant to achieve?
   You should have in the DSA a clear objective, or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document this.

2. The data to be shared;
   The most important question to ask of any data
sharing agreement is: Could the objective of the sharing be achieved without sharing the data or by anonymising or pseudonymising it? This applies particularly with a data reporting sharing agreement.

It is not appropriate to use personally identifiable data for CCGs commissioning purposes or to plan service provision, for example, where this could be done with pseudonymised or anonymised data or aggregate data (number counts).

3. What information needs to be shared?

Here the “need to know” principle applies and the DSA should not require more of a person’s record than is necessary for the objectives. So a patient’s consultation history may not be shared when say a drug history is all that is needed for example.

4. Is explicit patient consent required?

Consent (explicit and informed consent for sensitive personal data) is one of the conditions the Data Protection Act 1998 (DPA) provides to legitimise processing. The Data Protection Directive on which the UK’s DPA is based defines ‘the data subject’s consent’ as:

‘Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.

There must therefore be some form of active communication where the informed individual knowingly indicates consent. Whilst consent will provide a basis on which organisations can share personal data, the ICO recognises that it is not always achievable or even desirable. If you are going to rely on consent as your condition you must be sure that individuals know precisely what data sharing they are consenting to and understand its implications for them. They must also have genuine control over whether or not the data sharing takes place and be able to have their dissent respected.

It is bad practice to offer individuals a ‘choice’ if the data sharing is going to take place regardless of their wishes, for example where it is required by statute or is necessary for the provision of an essential service.

Explicit informed consent for data sharing is most likely to be needed where:

- Confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
- The individual would be likely to object should the data be shared without his or her consent; or
- The sharing is likely to have a significant impact on an individual or group of individuals.

Patient dissent

Practices must allow patients to dissent from sharing their records and must record and respect that dissent. You must give patients this opportunity by informing them fully of the circumstances in which their data will be shared. Whilst the leaflet ‘Your Information – Our Key to Your Best Healthcare’ informs patients of most of the usual uses of their information and will be sufficient for the majority of patients for whom GP practices hold data, practices must satisfy themselves that they can clearly identify patients (for example by the appropriate READ code) who have expressed an objection to their data being processed other than by the GP Practice and or being transferred to third parties (even for a lawful purpose) outside of the GP practice system. Additionally, prior to data extraction, it is incumbent upon the GP practice to ensure that all the statutory prohibitions in relation to certain, special, conditions of their registered patients (such as those covered by the Human Fertilisation and Embryology (Disclosure of Information) Act 2002) are readily identifiable and able to be excluded from data transfer. For advice on this visit the Information Commissioner’s Office (ICO) website (www.ico.org.uk).
5. Who requires access to the shared personal data?

Here it is important to establish ‘need to know’ principles, meaning that other organisations should only have access to your data if they need it for legitimate reasons, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties. The DSA should specify the potential recipients or types of recipient and the circumstances in which they will have access.

6. When should it be shared?

This should be clearly documented, setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

7. Data security;

How should it be shared?

This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

Difficulties can arise when the organisations involved have different standards of security and security cultures or use different protective marking systems. It can also be difficult to establish common security standards where there are differences in organisations’ IT systems and procedures. Any such problems should be resolved before any personal data is shared and an agreed set of security standards must be signed up to by all the parties involved in a data sharing agreement.

There should be clear instructions about the security steps which need to be followed when sharing information by a variety of methods, for example phone, fax, email or face to face.

8. Review of effectiveness/termination of the sharing agreement.

How can we check the sharing is achieving its objectives?

You will need the opportunity at some specified future date to be able to judge whether the DSA is still appropriate and confirm that the safeguards still match the risks.

What is the lifespan of the agreement?

9. What risk does the data sharing pose?

Is any patient likely to be damaged by it? Is any patient likely to object? Might it undermine patients’ trust in their practice?

10. Do I need to update my notification?

You need to ensure that the sharing is covered in your ICO register entry.

References


Acknowledgements

Thanks to Dr Julie Sharman, author of this document. Thanks are also due to Dr Kambiz Boomla of Tower Hamlets LMC whose expert guidance was invaluable in writing this document.

About Londonwide LMCs

Londonwide Local Medical Committees (LMCs) is here to support and represent the 6000+ GPs and their practices in the capital. We are the professional voice of general practice in London and we strive to help all members of the practice team. Following the repeated negative press coverage GPs have been receiving over the last few months, Londonwide LMCs has launched a patient information poster campaign (www.lmc.org.uk/article.php?group_id=8409) to help patients and the public understand that across many GP practices, the staff are caring, hard working, dedicated and focussed on patients’ needs. For more information, visit our website (www.lmc.org.uk).
APPENDIX 1

CALDICOTT PRINCIPLES:

In the original 1997 Caldicott report 6 principles were established:

1. Justify the purpose(s)

   Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don’t use patient identifiable information unless it is absolutely necessary

   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary patient-identifiable information

   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. Access to patient identifiable information should be on a strict need-to-know basis

   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. Everyone with access to patient identifiable information should be aware of their responsibilities

   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

   Caldicott 2.

   The original Caldicott report has been modified by the second, 2013, Caldicott report.

   Three principles informed the report:

   i. Protect patient and service user confidential data from inappropriate use and disclosure.

   ii. Address the unhelpful “culture of anxiety” that surrounds sharing patient confidential data that is often detrimental to care.

   iii. Improve service users’ understanding of how their data is used.

   Consequentially, for data controllers like GPs there is a new seventh Caldicott principle:

7. The duty to share personal confidential data can be as important as the duty to respect service user confidentiality.

   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
Summary of recommendations

Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be re-tested regularly.

1. A programme of work should be established to reinforce awareness of confidentiality and information security requirements amongst all staff within the NHS.

2. A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.

3. Clear guidance should be provided for those individuals/bodies responsible for approving uses of patient-identifiable information.

4. Protocols should be developed to protect the exchange of patient-identifiable information between NHS and non-NHS bodies.

5. The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be clearly communicated.

6. An accreditation system which recognises those organisations following good practice with respect to confidentiality should be considered.

7. The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.

8. Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.

9. Where particularly sensitive information is transferred, privacy enhancing technologies (e.g. encrypting identifiers or “patient identifying information”) must be explored.

10. Those involved in developing health information systems should ensure that best practice principles are incorporated during the design stage.

11. Where practicable, the internal structure and administration of databases holding patient-identifiable information should reflect the principles developed in this report.

12. The NHS number should replace the patient’s name on Items of Service Claims made by General Practitioners as soon as practically possible.

13. The design of new systems for the transfer of prescription data should incorporate the principles developed in this report.

14. Future negotiations on pay and conditions for General Practitioners should, where possible, avoid systems of payment which require patient identifying details to be transmitted.

Consideration should be given to procedures for General Practice claims and payments which do not require patient-identifying information to be transferred, which can then be piloted.
APPENDIX 2

The 8 Data protection principles

Schedule 1 to the Data Protection Act lists 8 data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

See website www.ico.org.uk.