WESSEX
Local Medical Committees
Incorporating Wessex LEaD

# Principles of Data Sharing for GPs

**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 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 (ICOs) code of practice (please note, this is in the process of being updated in the light of the DPA 2018 becoming law). For further specialist guidance, please see the Information Commissioner's Office (ICO) website www.ico.org.uk.*

GPs are being asked to sign up to a plethora of "Data Sharing Agreements" (DSA) - which share data between data controllers (e.g. a GP practice and a hospital) – and these are being requested to facilitate a wide range of purposes related to the provision of care.

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 performance dashboards for payment or quality improvement purposes as well as those requested for clinical care.

These latter agreements involve care record sharing. Distinct considerations apply to each (notably around the lawful basis for sharing and common law confidentiality issues) 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.

We are also seeing developments of data reporting where the purpose is to identify cohorts of patients that may be managed in a different way. These should work so that the commissioner can only see aggregate or pseudonymised data, but that the care provider can ‘re-identify’ individuals they may need to approach.

Few GPs find evaluating the reasonableness of requests for data sharing an easy matter and are 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. Data Protection legislation 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.

GPs are familiar with protecting patient information they hold 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. If the patient is generally aware of the sharing and not objecting then for their care, records can generally be shared. 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 NHS Digital 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 (GAG HRA).

## Lawful basis for processing data and consent

### Implied Consent

Implied consent can be relied on where there are very strong grounds for believing that the patient is generally aware of the data sharing and hasn't raised any concerns. 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 requires data on childhood immunisation coverage and invitation letters are sent out. 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

The revised Data Protection Legislation (including the General Data Protection Regulation – GDPR) emphasize that consent is one of a number of lawful basis to process data on, but it should only be the basis where the patient has genuine choice and control over the use of their data. It highlights that if consent is to be used to process data then it must be explicit. It is important to note that a patient consenting to being referred is not consenting to their data being used for the referral. Consent cannot be the basis to process data for the referral because the patient's only choice is to have the referral or not. If they want the referral then data has to be shared, they cannot have the referral without the sharing of data, so in terms of genuine choice and control over their data alone, they do not have that. That is why there are other basis to process data where the data is necessary for the provision of a service. The patient must be aware the data is being shared and can object, but you should not be asking for their explicit consent.

In circumstances where the use of data is not necessary and if the patient refused, the data would not be used, then explicit consent is the best option to base the processing of data on.

# 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 very useful 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.

Under revised Data Protection legislation if data is to be shared ‘in the public interest’ then an ‘appropriate policy’ is required and a DSA is likely to be the sort of documentation needed.

Please note, 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, as follows, provides a practical and pragmatic 'working' list of points to incorporate into any data sharing agreement and is derived from existing legislation and guidance.

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

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

## Checklist:

GPs 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. A clear lawful basis to share the data
5. Data Quality – accuracy, relevance, completeness and usability etc
6. Data security – accessibility
7. Retention of shared data – how long will data be retained and under what circumstances
8. Patient’s 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

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:

## 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.

## 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).

## 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.

## What is the lawful basis for sharing the data?

As detailed above, revised Data Protection Legislation is shifting the position on consent. For the provision of care to the patient, then in simple terms, the patient should be informed about the sharing. If they have concerns they have the right to object. This meets the common law duty of confidentiality and links to processing conditions in legislation such as ‘exercise of official authority’ and the ‘provision of health and social care or treatments’.

Where the sharing is not directly related to the care of the patient, then whilst the lawful basis for processing under Data Protection legislation is likely to be the same or similar, the issue is whether the common law duty of confidentiality will be breached. This can be addressed by anonymizing or pseudonymising the data as far as possible. A good DSA will set out how this is to be done and address whether it is sufficient to put aside concerns about the common law duty of confidentiality. Where the potential to re-identify the data is very small without the tightly controlled ‘key’ to the data, then the likelihood of a confidentiality breach affecting individuals is very low.

## 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.

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).

## 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.

## 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.

## 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.

### 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?

### 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?

### Do I need to update my notification?

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

## References


- Data Sharing Code of Practice.
- "NHS confidentiality code of practice". Department of Health. 2003-11-07
- "The Caldicott Review ". Department of Health. 26 April 2013
- National Data Guardian Report 2017.
- General Data Protection Regulation 2018.
- Data Protection Act 2018.


## 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.
- Thanks to Londonwide LMCs for sharing this information.


**Reviewed and updated by Wessex LMCs, September 2018.**

# 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 individua ls 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 nonclinical 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:

- Protect patient and service user confidential data from inappropriate use and disclosure.
- Address the unhelpful "culture of anxiety" that surrounds sharing patient confidential data that is often detrimental to care.
- 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 datafiow, current or proposed, should be tested against basic principles of good practice. Continuing fiows should be re-tested regularly.

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

- 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.

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

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

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

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

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

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

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

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

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

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

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

- 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 Data Protection Principles (General Data Protection Regulation)

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

See website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/