Londonwide LMCs
The professional voice of London general practice

Data Sharing Agreement/Document Checklist and Guidance for GPs and Practices

Londonwide LMCs is aware of the increasing complexity and number of information and Data Sharing Agreements and documents (DSAs) which practices are receiving to review and sign. Whilst Londonwide LMCs cannot endorse, support or approve any information sharing or DSAs/documents, we have put together this checklist and guidance to help GPs and practices in reviewing the agreements they receive in order to be able to make an informed decision on whether to sign them or not. If you are unfamiliar with what constitutes a DSA, please read through the guidance section first and then use the checklist.

Please note this checklist does not constitute legal advice and is guidance only.

There may be other considerations/processes and documents that you may have to take into account or have in place to fully comply with all the requirements of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)/Data Protection Act 2018 (DPA 2018) and other data protection legislation.

You should liaise with your Data Protection Officer (DPO) and/or the CCG provided DPO and DPO support service, and other parties to the DSA, including taking legal advice where appropriate to ensure that you are compliant with GDPR/DPA 2018 and other data protection legislation.

This checklist has been produced with advice from LMC Law Ltd and Protecture.

Londonwide LMCs
The professional voice of London general practice

Checklist for GPs and Practices reviewing a Data Sharing Agreement (DSA)/Document

Review the DSA using the questions provided in the checklist below. The checklist is divided into three parts: essential information, necessary information, and your role.

For each question, record the answer.

If the answer is 'partly' or 'no', request clarification from the owner of the agreement. Keep a record of the information provided, if the DSA itself has not been amended to include it.

You can download an Excel version of the checklist here.

Essential information			
Does the DSA...	**Yes, clearly**	**Partly/ ambiguously/ vaguely**	**No**
Have a start date, specify review dates and any termination date?			
Contain a list of the categories of personal data which will be shared in the dataset, including any 'special category' data and any de-identified data?			
Identify or describe the group of data subjects whose personal data will be shared and how they are expected to be identified?			
Describe the objective(s) of the sharing, how the sharing supports and is necessary for those objectives?			
Explain the intended benefits to individuals and society in the sharing of this data?			
Contain a visual or descriptive map of the data flows between the organisations?			
Explain the purpose(s) of the sharing and justify why the sharing is necessary to fulfil those purposes?			
Explain the lawful basis for the sharing activities, including specific lawful bases for 'special category' personal data? (NB: 'consent' is unlikely to be a suitable lawful basis for any direct care purpose.) Make clear the lawful basis for each processing purpose or data flow identified as a requirement of the sharing activity.			

State which organisations are Data Controllers and whether there is a Joint Data Controller relationship? This includes making clear which parties are the disseminators and recipients of which data sets – the relationship must be clearly defined.			
If you have answered 'partly/ambiguously/vaguely' or 'no' to any of these questions, you must seek clarification on these essential points before signing the agreement.			
Necessary information			
Does the DSA...	**Yes, clearly**	**Partly/ ambiguously/ vaguely**	**No**
Identify which organisation(s) will be responsible for providing privacy information about the sharing, and at what stage (and how, where, and to whom this information will be provided)?			
(for Joint Data Controller relationships) Identify which organisation(s) will take the lead on handling data subject rights requests and incidents, and the process by which data subject rights will be addressed?			
Describe the systems and locations where the shared data will be stored, transmitted and accessed from?			
Outline clearly the measures required to ensure adequate security of the data?			
Make clear the process to be relied upon for effective deletion of data?			
Outline the common period for which data will be retained and the method by which data should be deleted?			
List and justify the roles or categories of individuals who will be allowed to access the shared dataset?			
Set out the boundaries of confidentiality and purpose limitation for the shared data, setting restrictions on its onward disclosure and/or reuse for other purposes?			
Differentiate between data sharing for direct care and for secondary purposes?			
(if Data Processors are involved) Designate the organisation which has issued the Data Processor			

contract, identify any sub-processors, and provide procedures for engaging with the Processor?			
Identify any data flows outside the UK and if these are required; specify the destinations and the conditions for transfer? (Leave room for Brexit considerations should the UK become a third-country and new rules apply – have model clauses or EEA representatives been put in place where/when necessary?)			
Identify standards and frameworks which must also be complied with when processing the shared dataset?			
Include a version number, details of the approval process and state how any variations to the agreement, including new signatories, will be handled?			
Provide references to other documents such as contracts, over-arching protocols or standards which the DSA relies on?			
If you have answered 'partly/ambiguously/vaguely' or 'no' to any of these questions, you may wish to seek clarification on these essential points before signing the agreement.			
Your role			
Are you clear on…	**Yes**	**Partly**	**No**
The purpose, justification and necessity for the sharing?			
The location, methods of transmission and quality standards of any data which will be distributed by your practice under this agreement, and the means to ensure security?			
The methods of transmission, quality standards and minimum dataset which will be received or shared by your practice under this agreement, and the means to ensure security?			
The degree (if any) to which the sharing agreement will affect your day-to-day operations?			
Whether the sharing requirements will impose an additional workload on practice staff and, if so, how this will be funded?			

The terms of the agreement, enough to be able to explain it to patients in simple language?			
What needs to be added to/altered in your practice's privacy information as a result of the sharing agreement?			
The point(s) of contact for queries, comments and incident response relating to the sharing agreement? (This should be specifically allocated to each party with particular roles and responsibilities.)			
What arrangements need to be in place to provide individuals with access to their personal data if they request it.			
If you have answered 'partly' or 'no' to any of the questions in the checklist, you may wish to seek clarification on these essential points before signing the agreement, or to decide whether the risk to your practice and patients is acceptable. You must document this decision in your data protection records.			

What to do next

Once you have completed this checklist, if you are satisfied that the DSA is fit for purpose and that you can deliver your part in the sharing relationship without problems, and you want to sign it, then you should:

- Update your practice privacy notice with the privacy notice information provided for this DSA and ensure this is displayed/available for patients
- Update your practice data mapping with any additional data flows from the DSA and update your practice ROPA (Record of Processing Activities)
- Ensure all relevant practice staff are aware of the sharing if they are asked questions by patients.

Guidance

What is a Data Sharing Agreement?

This is a catch-all term for documents which describe the arrangements where personal data is being transferred, copied or accessed between organisations. A DSA can take different forms: it could be a separate document, it could be part of a suite or tier of documents, it may be a separate sharing agreement associated with a contract, or the data sharing terms may form part of a contract.

Whilst some organisations prefer to have legally-binding agreements to limit their liability, data sharing arrangements are not required to be legally-binding agreements, as long as all of the requirements of data protection and confidentiality law are met. However, if an agreement is intended to create legal relations, then it is a 'contract' under English law, even if it is not described that way.

What's the difference between a Data Sharing Agreement and a Data Processor Agreement?

A Data Processor Agreement is a legally-binding contract between a Data Controller and a Data Processor which sets out the instructions for processing and strict limits on what the Processor can do with the data. For example, if a GP Practice as a Data Controller wishes to use a mailing house to write to its patients, then the mailing house would require access to personal data from the GP Practice in the form of patient names and address details. The mailing house would be processing the data on behalf of the GP Practice and a data processing agreement or contract would be required, detailing the parties involved and the processing activity being undertaken. This is a legislative requirement, as Data Processors can only process on instruction from a Data Controller.

A DSA is usually an operational document which describes one-way, two-way or multiple-way distribution of personal data between two or more Data Controllers.

Why have a Data Sharing Agreement?

The purpose of a DSA is to set out the sharing relationship clearly and carefully, so that everyone involved understands how it should work and what their individual and joint responsibilities are with regard to the data. To achieve this, the DSA should be written in plain language without the use of jargon or obscure legal terms; and it should clearly describe the why, what, who, where and how of the sharing relationship so that there is no ambiguity or confusion on these points.

Although there is no law that explicitly says a DSA must be put into place, the Accountability Principle of the General Data Protection Regulation (GDPR) requires that reliable records are created for all data processing activities. Therefore, having DSAs in place for data sharing relationships is a necessary part of demonstrating compliance with data protection law.

Do I have to sign this Data Sharing Agreement?

If your practice is party to a DSA which you don't fully understand or don't agree with you may be placing the practice and your patients at risk by proceeding. To protect yourselves and your patients, you should always ask for clarification on any aspects within the agreement which are missing, inappropriate or not properly explained before you sign. By signing the agreement, you are accepting a degree of responsibility (and possibly legal liability) for the data sharing relationship, so it is important to make sure you understand and can deliver your part.

How do I make sense of this Data Sharing Agreement document?

Ideally, a DSA should be easy to read, understand and interrogate. However, this is not always the case, especially where the DSA forms part of a contract. In its most basic form, a DSA should tell the reader the following:

- Why the sharing will happen:
    - The purpose of the sharing activities and the lawful basis for each purpose or sharing activity
    - The objectives of the sharing, and why the sharing of personal data is necessary to meet those objectives. (It must demonstrate that this sharing activity is proportionate to the objectives, which could not be achieved otherwise)
    - The power to share: the functions or powers of your organisation and any legal obligation to share.

- What personal data is being shared:
    - What categories of personal data are involved, and which of these are 'special category' personal data
    - Which particular group or set of patients will be affected
    - What you need to tell people about the data sharing and how you will communicate that information.

- How the sharing works:
    - The journeys that the data will take between/among the organisations
    - The systems and processes for collecting, storing, sending/receiving and using the data
    - The relationships between the organisations: whether they are independent Data Controllers (independently decide the why, what and how of processing) or Joint Data Controllers (jointly decide the why, what and how of processing) , and the boundaries of these relationships
    - Which organisation is responsible overall for the sharing agreement
    - Who in each organisation is accountable for making sure that the terms of the sharing agreement are met

- Who needs to be informed about the terms of the sharing agreement
- How changes to the agreement or the relationships will be managed
- What arrangements need to be in place to provide individuals with access to their personal data if they request it
- Measures to ensure adequate security are in place to protect the data
- Agreed common retention periods for the data
- Processes to ensure that secure deletion takes place, where appropriate.

To be able to evaluate and understand the terms of a DSA, you will need to have an understanding of data protection and confidentiality law. If you are not familiar with any of the following terms, you should brush up on your knowledge of the following before tackling the DSA:

- Data Subject
- Data Controller
- Data Processor
- Joint Data Controllers
- Data Protection Principles
- Subject Access Requests
- 3rd country/conditions for transfer
- Lawful basis of processing.

Why can't Londonwide LMCs or my LMC review and approve the Data Sharing Agreement for my practice?

Londonwide LMCs cannot endorse, support or approve any information sharing or DSAs/documents, and we don't have the resources or expertise to review each DSA/document in detail. However, we do wish to ensure that commissioners/providers give assurance to practices that the key requirements are in place and in a format that is accessible and readable. So, in addition to this checklist and guidance for GPs and practices, Londonwide LMCs has also developed, with legal assistance, an assurance checklist for commissioners/providers. This will be provided to the organisation/author of the DSA and they will be asked to review the checklist against their proposed DSA and to sign that the DSA covers the items specified in the checklist and that the DSA meets current data protection requirements. A copy of the completed assurance checklist for commissioners/providers, along with a copy of the Data Protection Impact Assessment (DPIA) for the DSA, should accompany/or be made available to practices when the DSA is sent to them. The DPIA will identify any risks that can't be fully addressed and as part of the process these should be highlighted to practices.

Useful References

- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr
- https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
- https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality