Londonwide LMCs
The professional voice of London general practice

Data sharing agreement checklist and guidance for GPs and practices

Version 1.0 | Published May 2026

Londonwide LMCs is here to support you and your practice team in operating safely.

As part of agreed Collective Action, GPC England is urging GP partnerships and practices across England to act collectively to stay safe and sustainable in the face of the 2026/27 imposed GP contract.

GPC England is recommending (on their website) that the first action practices take is around reviewing the GP patient data they are expected to share outside the practice, with the wider NHS and other organisations. Writing to your local ICB provides a "housekeeping" opportunity to ensure that the practice is fully up to date and that all active DSAs have all necessary Data Protection Impact Assessments (DPIAs) in place from an information governance perspective to support informed and safe decisions to be made if Collective Action progresses. The letter is to enable you to contact your local ICB Chief Clinical Information Officer (CCIO) requesting a comprehensive review of all DSAs across the system to which the ICB's constituent NHS general practices are a signatory, including requesting information in writing.

Whilst not mandatory, our DSA audit guidance is intended to support this, should practices wish to use this as an opportunity to review their existing arrangements, demonstrate compliance with the UK GDPR accountability principle, and make sure the right documents are in place to support the practice's approach to data sharing under data protection law.

Londonwide LMCs has produced this guide to help you: identify where your practice's data sharing information is held; check whether each data sharing agreement is clear and justified; record whether data sharing is for direct care or secondary purposes, and; record practice actions.

The guide starts with a quick checklist to help you identify the purpose of the data sharing in each DSA and check relevant data protection and information governance requirements are in place, then you can use the full audit template if more details or follow-up are needed. A downloadable excel workbook containing the quick checklist, the full audit checklist and the audit decision log can be accessed here. A downloadable PDF of the quick checklist, the full audit checklist and the DSA audit decision log can be accessed here. There is a glossary of data protection terms at the end of the document for ease of reference.

Please note this guidance and 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 UK 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 ICB provided GP DPO and DPO support service, and other parties to the DSA, including taking legal advice where appropriate to ensure that you are compliant with UK GDPR/DPA 2018 and other data protection legislation.

Londonwide LMCs
The professional voice of London general practice

Contents

Brief introduction

What is a data sharing agreement (DSA)?

This is a broad term used for documents that describe arrangements under which personal data is transferred, copied, or accessed between organisations. A DSA can take different forms: it may be a stand-alone document, part of a wider suite of documents, a separate agreement linked to a contract, or data-sharing terms within a contract.

Some organisations prefer legally binding agreements to manage risk and liability. However, data-sharing arrangements do not have to be legally binding, provided the requirements of data protection and confidentiality law are met. If an agreement is intended to create legal relations, it is likely to be treated as a contract under English law, even if it is not labelled as one.

What's the difference between a data sharing agreement and a data processing agreement (DPA)?

A data processing agreement is a legally binding contract between a data controller and a data processor. It sets out the instructions for processing and the limits on what the processor can do with the data. For example, if a GP practice uses a mailing house to write to patients, the mailing house would need access to personal data such as names and addresses. As the mailing house would be processing data on behalf of the GP practice, a data processing agreement or contract would be required. This is a legal requirement because a processor can only process personal data on the controller's instructions.

A data sharing agreement is usually an operational document that describes the sharing of personal data between two or more data controllers. It may cover one-way, two-way or multi-way sharing.

Why have a data sharing agreement?

The purpose of a DSA is to explain the sharing arrangement clearly so that everyone involved understands how it works and what their individual and joint responsibilities are. To do this well, the DSA should use plain language, avoid jargon or obscure legal terms, and clearly describe the why, what, who, where and how of the sharing arrangement.

There is no specific law that says a DSA must always be in place. However, the accountability principle in UK GDPR requires organisations to keep reliable records of their processing activities. In practice, having DSAs in place for data sharing arrangements is an important way to demonstrate compliance with data protection law.

Where to find information on data sharing agreements for your practice

- **Your practice's clinical system**

SystmOne (TPP)

- Enhanced Sharing Training Document.pdf
- Check the ***Enhanced Data Sharing Model (eDSM)*** settings in ***Setup > Users & Policy > Share In Rules*** to review how record sharing is configured for your practice.
- Review any organisation-wide sharing rules, including whether other organisations require verification before accessing shared records.
- Check whether there is an associated local information sharing agreement or eDSM information sharing agreement covering the organisations involved and compare this with your Record of Processing Activity (ROPA)/information asset register.
- Practices in the NWL area who use SystmOne – there is a whitelist set up which controls how external organisations can access patient records. Further details on the allowed list are in this document Importing_the_allowed_list_v24.docx, including the allowed list of organisations who have signed up to the NHS NWL Data Sharing Agreement.

EMIS (Optum)

- EMIS Web - Data Sharing Manager
- Open ***Data Sharing Manager*** from ***Configuration > Data Sharing Manager***, then use ***My Agreements (and Enterprise where available)*** to review the sharing agreements configured for your practice.
- Check the agreement categories such as ***Care Record, Reporting, CrossOrgTasks***, ***Appointments and Data Distribution***, and note whether each agreement is active or inactive.
- Open each agreement to review the current activation status, the organisations that may be sharing or viewing data, and whether the arrangement matches your practice's Record of Processing Activity (ROPA)/information asset register and any local DSA.

Medicus

- Enabling a Bulk Data Extract – Medicus Help Centre – this article explains how to see which bulk data extractions have been agreed.

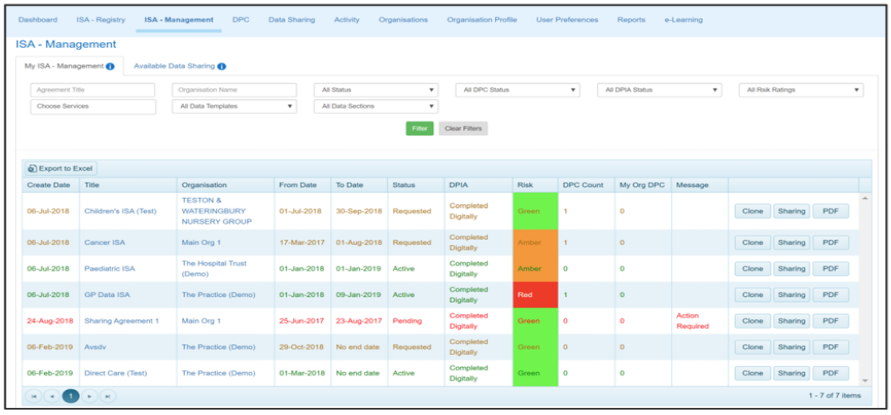
- **Your practice's Record of Processing Activity (ROPA) and/or information asset register will list the data flows for the practice.**

- **Data Controller Console (DCC) – is a central repository for DSAs in London**
  - Data Controller Console – Log in for the DCC.
  - Issues with logging in contact Support : OneLondon ServiceDesk
  - Documentation and help guides - Data Controller Console
  - Active user guide , page 17 section 6.5 provides details of how to search for and view Information Sharing Agreements (ISAs)/DSAs your organisation is participating in. See screenshot below.
  - From the ***My ISA – Management tab*** for each ISA/DSA it will show the creation date, the title, the organisation hosting the ISA/DSA, from and to dates, status, if there is a Data Protection Impact Assessment (DPIA), if there is an associated data processing agreement/contract (DPC). To create and save a PDF of the DSA for your practice records, you can click on the PDF button.

6.5 Search for and view ISAs your organisation is participating in

Under 'ISA Management > My ISA – Management' tab, you will see the ISAs that you have been invited to or requested access to. The 'ISA – Management' tab shows all of the ISAs you are participating in.

1. Select 'ISA – Management' from the navigation bar. The 'ISA - Management' screen is displayed with the 'My ISA - Management' tab in focus listing the ISA's that your organisation has been invited to or requested access to



Direct care and secondary purposes

Use this quick comparison to help decide whether a DSA supports individual patient care or a purpose beyond direct care.

Direct care	Secondary purposes
Definition: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes safe and high-quality care delivered by professionals who have a legitimate relationship with the person for their care.	**Definition:** Uses of confidential patient information for purposes beyond individual care, such as wider service planning, research, commissioning, analytics, audit across organisations, and innovation for public benefit.
Typical examples: Shared care records, referrals, diagnosis and treatment, medicines management, safeguarding, local clinical audit linked to care.	**Typical examples:** Population health management, service planning, research studies, commissioning analysis, risk stratification outside direct care, and wider system reporting.

Common indicator: Usually relies on implied consent for confidentiality because the patient would reasonably expect the information to be shared for their care.	**Common indicator:** Often needs explicit consent, anonymisation, or another legal basis such as statutory support where confidentiality would otherwise prevent the use.
Ask yourself: Is this sharing necessary for the care, treatment or safety of identifiable individuals by professionals involved in that person's care?	**Ask yourself:** Is this sharing mainly to benefit the wider service or population rather than direct care of individual patients whose data is shared?

Some DSAs do not draw a clear line between direct care and secondary purposes, particularly where they refer to proactive care or population health management. These labels do not by themselves determine whether a purpose is direct care; the legal and operational context still needs to be assessed. If you are unsure whether a DSA is for direct care or secondary purposes, seek advice from your Data Protection Officer (DPO) before making a final decision on the use and purpose of the DSA.

Information governance and data protection checks

One-page quick checklist

Use this checklist as a quick review to determine use and purpose of the data sharing and that key data protection and information governance requirements are in place, before working through the full audit template if required. An editable PDF version of the quick checklist is available here.

Name of document	[Click here to enter document name]
Date reviewed	[Click here to enter review date]
Yes/No	**Quick review question**
[Select: Yes / No]	Is the purpose of the sharing clear and necessary?
[Select: Yes / No]	Is the amount of data shared limited to what is necessary for the stated purpose?
[Select: Yes / No]	Is it clear whether the sharing is for direct care, secondary purposes, or both?
[Select: Yes / No]	If both apply, are the two elements clearly separated?
[Select: Yes / No]	Is there an UK GDPR Article 6 basis and, for health data, an UK GDPR Article 9 condition?
[Select: Yes / No]	Is the confidentiality position clear (for example implied consent, explicit consent, statutory support or Clinical Advisory Group (CAG) support)?
[Select: Yes / No]	Are the parties, controllers and any processors clearly identified?
[Select: Yes / No]	Is there a DPIA, or at least completed DPIA screening questions where appropriate, and if the DPIA has identified any risks are you content that these have been addressed?
[Select: Yes / No]	Are the patient information materials, privacy notice content, and any relevant rights or opt-outs covered in the documentation and in the practice's patient-facing information?
[Select: Yes / No]	Is the DSA clear on how the data is shared from start to end user, that there are clear access controls in place for the accessing the data at any point, with appropriate security measures in place throughout the data sharing and the retention period for the data is clear?
[Select: Yes / No]	Are DSA review dates, termination arrangements and points of contact recorded?
[Select: Yes / No]	Has the practice recorded its decision on the use and purpose of the data sharing, justification and any follow-up actions?

If any answer is unclear or incomplete, use the full audit template and seek DPO advice before making a final decision.

Full audit template

Use this full audit template/or sections of it and seek DPO advice if any of the answers to the quick checklist are unclear. An editable PDF version of the full audit checklist is available here.

Name of document:	[Click here to enter document name]	
Check	**Yes/No**	**Details/Comment**
Is the purpose of the sharing clear, and is it necessary to achieve that purpose? The document should explain why the sharing is proportionate and why the objective could not reasonably be achieved in another way.	[Select: Yes / No]	[Add comments here]
Is the amount of personal data shared limited to what is necessary for the stated purpose, including the categories of data and the number of records or patients covered?	[Select: Yes / No]	[Add comments here]
Is it clear whether the data sharing is for direct care, secondary purposes, or both?	[Select: Yes / No]	[Add comments here]
If the sharing covers both direct care and secondary purposes, does the document clearly separate the two?	[Select: Yes / No]	[Add comments here]
Is the lawful basis stated for each processing purpose or data flow identified as a requirement of the sharing activity? For personal data, there should be a lawful basis under UK GDPR Article 6 basis (1) and for health data (special category data) a condition under UK GDPR Article 9 (2).	[Select: Yes / No]	[Add comments here]
Is the sharing required or supported by a contract, statutory duty, or other formal arrangement?	[Select: Yes / No]	[Add comments here]
Is the sharing consistent with the lawful basis relied on?	[Select: Yes / No]	[Add comments here]
Is the confidentiality position clear? For example, does the sharing rely on implied consent, explicit consent, statutory support, or CAG support to set aside the common law duty of confidentiality where appropriate?	[Select: Yes / No]	[Add comments here]
Are the confidentiality boundaries and purpose limits clear, including any restrictions on onward disclosure or reuse for other purposes?	[Select: Yes / No]	[Add comments here]
Can you identify all organisations involved in the data sharing? The DSA should clearly show which parties are sharing data, which are receiving or accessing it, and which organisation is responsible overall for the agreement.	[Select: Yes / No]	[Add comments here]

Is it clear which organisations are data controllers, and whether there is a joint data controller relationship? If the practice is a joint data controller, is there a joint data controller agreement in place?	[Select: Yes / No]	[Add comments here]
Are any data processors involved in the sharing? If so, is there a data processing agreement or contract with the relevant clauses in place, is it clear which organisation issued it, and are there procedures for controllers to engage with the processor?	[Select: Yes / No]	[Add comments here]
Is it clear what personal data is being shared, including the categories involved, which data is special category data, and which patients or groups of patients are affected if this is not the whole patient list?	[Select: Yes / No]	[Add comments here]
Is there a DPIA, or at least completed DPIA screening questions where appropriate? If risks have been identified, is it clear that they have been addressed?	[Select: Yes / No]	[Add comments here]
Is it clear how the sharing works, including the data flows between organisations, where the data will be stored, transmitted and accessed, what security measures apply, and whether a data flow map is available?	[Select: Yes / No]	[Add comments here]
Is it clear which roles or groups of staff can access the shared data, why that access is needed, and what role-based access controls are in place?	[Select: Yes / No]	[Add comments here]
Are the points of contact for queries, comments and incident response clearly identified for each party, with roles and responsibilities defined?	[Select: Yes / No]	[Add comments here]
Are the start date, review dates and any end or termination date clearly recorded?	[Select: Yes / No]	[Add comments here]
Are the patient's rights in relation to the sharing clear, including whether any right to object or opt-out applies or does not apply?	[Select: Yes / No]	[Add comments here]
Are the retention period and the method for secure deletion, where appropriate, clearly set out?	[Select: Yes / No]	[Add comments here]
Have you considered the likely benefits to patients, the risks of sharing and not sharing, the impact on day-to-day practice operations, and the effect on workload?	[Select: Yes / No]	[Add comments here]

If you have answered 'no' to any of the questions in the checklist, you may wish to seek clarification from your GP DPO on these points.

If you identify any risk(s) to your practice and/or patients that have not been mitigated for this data sharing, contact your GP DPO and document any decision made.

Actions after completing the audit

We are actively engaging with One London to understand the specifics of GP data flows in London.

Once the audit is complete, use the actions below to record your decision on the use and purpose of the DSA, identify any risks, and note any follow-up steps.

These are practical prompts only. Consider them alongside DPO advice, contractual (national/local), (e.g. within the GMS contract, PCN DES or activity to support local commissioning arrangements); statutory requirements (e.g. serious case reviews or safeguarding); or mandated Government data Directions; and any local clinical safety or patient safety considerations.

- **For DSAs that cover both direct care and secondary purposes:** separate and document the two purposes clearly.
- **For DSAs that are only for secondary purposes:** document the use and purpose.
- Check that your practice privacy notice covers all of the data sharing described in the DSAs, and that it is published on your website and otherwise available to patients.
- Update your practice data mapping with any additional data flows identified through the DSA review and update your ROPA. If the practice does not have a ROPA or IAR, you can develop one with the ICO's template and guidance.
- Make sure relevant practice staff understand the practice's data sharing and what to say to patients. Where appropriate, plan how you will communicate any changes to patients, including through your Patient Participation Group.

DSA audit decision log

Use this log for each DSA reviewed. Duplicate as needed. An editable PDF version of the DSA audit decision log is available here.

DSA audit log	
DSA name / reference	[Click here to enter DSA title or reference]
Date reviewed	[Click here to enter review date]
Reviewer / approver	[Click here to enter reviewer name and role]
Decision	[Select outcome: Proceed / Do not proceed / Seek clarification / Escalate]
Legal / confidentiality basis	Record whether the sharing is for direct care, secondary purposes, or both. If both apply, record the two elements separately. Include the Article 6 basis, any Article 9 condition, confidentiality position, and DPIA status if relevant.
Justification	Record the key reason for the decision, including any patient benefit, legal concern, operational impact, or identified risk.
Actions / owner / target date	Record any follow up actions needed, owner and target date.
Sign-off / next review due	[Click here to enter sign-off name, role, and date] [Click here to enter next review due date]

Seek DPO advice where the legal basis, confidentiality position or purpose of the sharing is unclear.

Glossary of data protection terms

Term	Description
Caldicott Guardian Principles	A set of eight principles that guide how patient information is kept confidential and used appropriately.
Data controller	The body(ies) which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Controller Console (DCC)	A London-based repository and workflow tool used to store, view and manage data sharing agreements and related governance information.
Data processing agreement (DPA)	A written contract between a data controller and a data processor that sets out how personal data will be processed, including roles, responsibilities, and safeguards.
Data processing deed (DPD)	A deed used instead of a standard contract to set out processor obligations and safeguards where the parties choose that legal form.
Data processor	A body which processes personal data on behalf of the controller.
Data protection impact assessment (DPIA)	A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.
Data Protection Officer (DPO)	The person appointed to advise on and monitor compliance with data protection law, provide guidance on data protection risks and obligations, and act as a point of contact for data protection matters.
Data Protection Principles	The data protection principles are a set of seven core rules under UK GDPR that require personal data to be processed lawfully, fairly and securely, for specific purposes, kept accurate and limited, retained only as needed, and with accountability, forming the foundation of all good data protection practice.
Data sharing agreement (DSA)/ Information Sharing agreement (ISA)	A document that sets out the purpose of the sharing and helps all parties understand their roles, responsibilities, and safeguards.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Direct Care	A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes safe and high-quality care delivered by professionals who have a legitimate relationship with the person for their care.

Health Research Authority Confidentiality Advisory Group	An independent group that advises if confidential patient information can be used without consent in limited circumstances, where this is justified in the public interest; UK GDPR requirements still apply.
Information Commissioner Office (ICO) Data Sharing Code	This is a statutory code of practice made under section 121 of the Data Protection Act 2018.
Individual Rights	Individual rights are the legal entitlements that give people control over how their personal data is collected, used, and managed by organisations.
Information Asset Register (IAR)	A broader organisational tool that catalogues all information assets, including those that do not contain personal data. It captures details about asset ownership, storage locations, security classifications, retention periods, and business continuity requirements. Some organisations integrate their ROPA in the IAR.
Joint data controllers	If two or more controllers jointly determine the purposes and means of processing the same personal data, they are **joint controllers.**
National data opt-out	A choice that allows a patient to stop their confidential patient information being used for research and planning purposes outside their individual care, where the National Data Opt-out applies.
Proactive care	Personalised and co-ordinated multi-professional support and interventions for people living with complex needs, intended to delay deterioration, maintain independence, and reduce avoidable unplanned care.
Record of Processing Activity (ROPA)	A document that keeps a record of all the processing activities of personal data within an organisation to ensure transparency, accountability, and compliance.
Secondary purposes	Secondary purposes are uses of confidential patient information "unrelated to, and beyond, direct medical care", including examples such as healthcare planning, audit, population analytics, risk stratification, research, and commissioning.
Subject Access Requests (SAR)	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
Type 1 opt-out	A request by a patient to stop their GP practice sharing their confidential patient information for purposes beyond their individual care, where the Type 1 opt-out applies.

Useful references

- ICO guide to UK GDPR·
- GMC confidentiality guidance
- GPCE Resources and template letter