

Common FAQs

List of Common FAQ Questions:

- What is the London sub-national secure data environment?
- Why does London need a sub-national secure data environment?
- What are the benefits to me as a GP and to my practice?
- What are the benefits for my patients of their data flowing to the London Data Service?
- What are the benefits for my borough, my ICS and for London?
- Have the Londonwide Local Medical Committees (LMCs) been involved?
- Do I still have control over my patients' data? How will data be used and shared?
- How does the data access approval process work?
- If I get a Data Subject Access Request (DSAR) as a GP, how can I see how the patient's data has been used in the London Data Service?



Common FAQs

- What are the access and audit controls on identifiable patient data?
- How can I be reassured that there are no re-identification risks for my patients' data when it is pseudonymised or anonymised? And who/what process checks this?
- If a GP withdraws the data sharing agreement for the SDE – what happens to the patient identifiable data (including the pseudonymised data)?
- Is there assurance that the data held in the London Data Service will not be used to performance manage GPs and their practices?
- Can a patient opt out (object to) of their data flowing into the London Data Service? Will existing local opts be applied to the data and its use, how and when will these be applied?
- What is the difference between the London Data Service and the London Care Record?
- What data sharing/processing documents for the London Data Service and the London Analytics platform are my practice being asked to sign and why?



Common FAQs

- What is the London Independent Access Group?
- Is there a Data Access Committee for my ICS area?
- How do I as an individual GP practice get a say on how the data of my patients is being used?
- What does it mean to me as a GP that the documents state I am a joint controller and have delegated my responsibilities to a data access committee? Does this absolve me of any responsibility if there is a legal challenge?
- Will all data requests go via the London Independent Access Group, even aggregate data ones?
- Who are the GP representatives on the London Independent Access Group? If it is GP data and SUS data, then there should be a number of GP representatives alongside the citizen reps.
- Does each ICS Data Access/Usage groups have lay members (patient representatives)?
- Does the London Information Governance Advisory Group have patient representatives?
- How would an individual GP practice or PCN request for a local dashboard to be set up, would this be centrally or via a subscription request?



Common FAQs

- What is the timeline for the GP analytics dashboard to be live for individual GP Practices to utilise?
- If there is a data breach with the OneLondon SDE, how would I know as an individual controller? Would the data breach be reported to the DSPT incident reporting tool/ICO/NHSE centrally or would each GP Practice be expected to report individually?
- When would a GP practice be liable if there is a data breach in the OneLondon SDE?
- What are the risks for a GP and their practice in signing the data sharing/processing documents?
- Has my DPO been consulted on the documents I am being asked to sign?
- Has a clinical safety assessment (DCBO129 and DCB0160) been completed for the London Data Service and the London Analytics Platform?
- Do NHS Resolution Schemes cover everything?
- Is it possible that an individual controller is liable for breach another controller is responsible for?
- Could a claimant still sue my practice even if we weren't responsible?



Common FAQs

- Will the Information Commissioner's Office (ICO) fine my practice for someone else's incident?
- What should we expect if there is a breach?
- Where can I find the legal documents that protect my practice?



Common FAQs

What is the London sub-national secure data environment?

The SDE has two foundational elements: a London Data Service (LDS), and a London Analytics Platform (LAP). The LDS and Analytics platform can perform a range of uses, including direct care, system planning, population health management, and research and development. It provides a compliant infrastructure in which health care data (from all settings) can be ingested, cleaned, curated, and shared (either as identifiable or de-identified) to other approved applications; and then analysed in approved projects.

Why does London need a sub-national secure data environment?

There are many things that improve through Secure Data Environments, including:

- **Patient privacy** - Secure Data Environments must apply techniques to remove personal details. This makes sure that patient information remains confidential.



Common FAQs

- **Security** - As NHS data will only be hosted on systems that can prove they have high levels of protection.

- **Efficiency** - The process of preparing data so it is ready for analysis research can take time.

Secure Data Environments enable many different sources of data to be linked, so prepared data can be more easily accessed if needed again. This means that researchers and analysts can access bigger sets of data faster. This will speed up how quickly the NHS can make decisions and the discovery of new treatments.

What are the benefits to me as a GP and to my practice?

It will provide better tools to support you to deliver more proactive care. In some parts of London, this will include new data flows and flags in the London Care Record, and it will also include proactive care dashboards allowing clinicians to drill-down to identifiable patients in their care.



Common FAQs

What are the benefits for my patients of their data flowing to the London Data Service?

For direct care it will mean patients do not have to repeat their history, medications etc and they can be confident that the clinician treating them can make critical decisions about their individual care and treatment whenever and wherever they may need it. Their pseudonymised data can also be used for research and planning - helping regional teams to better understand the health of the city and improve services as a result.

What are the benefits for my borough, my ICS and for London?

- Makes it easier for local clinically-led projects to share methods, insights and tools that they develop to understand patient care and risks – such as the Tower Hamlet's metric on domestic overcrowding;

- Makes it easier for you to get involved in research, and feel the benefits of research being done using London data



Common FAQs

- Consolidate a range of different data sharing policies and agreements within a unified OneLondon Framework, addressing the public recommendation to reduce local variation in data policies and practice.

Have the Londonwide Local Medical Committees (Londonwide LMCs) been involved?

The Londonwide LMCs recognises the importance of effective information sharing and the benefits that shared data can realise for patients and GPs. That is why they have been working collaboratively with OneLondon to ensure that queries and questions raised by London practices about the programme for the London Secure Data Environment are considered and addressed rapidly.

The Londonwide LMCs believe that the London Data Service and London Analytics Platform are important enablers to improve opportunities for proactive direct care and population health and are working with OneLondon to address and mitigate the risks with this type of sharing as far as possible as part of the London Secure Data Environment.



Common FAQs

The Londonwide LMCs encourage practices to consider carefully the opportunities presented alongside their duties and responsibilities as the data controller, including having in place necessary indemnity arrangements and sourcing independent advice on Data Sharing Agreements and Data Processing Agreements. The Londonwide LMCs will continue to support practices and work with OneLondon in regard to this.

Do I still have control over my patients' data? How will data be used and shared?

The first and most important choice is whether GPs participate in the SDE by signing data sharing and processing agreements. The use of data for any particular project will be accessed by the local Data Access Committees (DACs) and as a data controller you will be represented on your local DAC (e.g. by your GP Data Protection Officer (DPO) or by attending directly).

The GP makes the decision where they are the sole data controller. In the jointly controlled data environment, the decision will be jointly made by all the data controllers including GPs or their nominated representative.



Common FAQs

This will be done through the ICS level IG governing bodies / Data Usage Committees (DUCs) / Data Access Groups (DAGs). . All five ICSs will also be represented on a pan-London Independent Information Action Group (IIAG).

It means you remain in control and can make decisions about the use of your patients' data and can jointly make decisions about the use of the linked data set through your local Data Access Committee.

The liability sits as a joint data controller and you continue to be responsible for ensuring that the processing of personal data takes place in compliance with the UK GDPR (see Article 24 UK GDPR), and all applicable legislation and data protection provisions/regulations.

Where data controllers sign up, data will be accessible within the SDE for direct care purpose, planning purposes, and research. Only research applications that have been approved by your local Data Access Committee would be given access to the data. This implements the recommendations from Londoners, expressed at the OneLondon Citizens' Assembly.



Common FAQs

Identifiable patient information will only be used for direct care and under roles-based access controls (similar to the London Care Record). Only anonymised data will be made accessible for research.

How does the data access approval process work?

Researchers fill out a templated data access form for their project. This is reviewed by the Data Access Committees and if found to be in line with agreed access standards e.g. compliant with research for medical purposes, providing public benefit etc, will be approved.

The OneLondon SDE requires five documents to be signed by data controllers: OL Data Sharing Framework, LDS data processing agreement, LAP data processing agreement, LDS data sharing specification, LAP data sharing specification.

Signing the data processing and data sharing agreements are a necessary part of signing up to the OneLondon SDE as a project. These agreements outline the responsibilities of the relevant parties (Data Controllers and Processors) in line with Article 28 of the UK GDPR and best data protection practices.



Common FAQs

If I get a Data Subject Access Request (DSAR) as a GP, how can I see how the patient's data has been used in the London Data Service?

Access and rectification requests may be submitted by the data subjects to the individual data controllers responsible for their care, in accordance with their local processes.

Given that, to a very large extent, the data contained within the London Data Service (LDS) and London Analytics Platform (LAP) environments is a copy of the data held by the NHS organisations from across the region within their own respective local systems, the data controllers should readily be able to comply with users' request wishing to exercise those data subject rights while referencing that the data is also being processed for the purposes of the LDS and LAP and shared with organisations across the region.

However, as there are particular data fields which will be derived from source data within the LDS environment (and as such contained in the LAP), a process will be implemented by the data controllers to ensure that processing of such data does not get inadvertently excluded, where it would otherwise fall within the scope of the rights of access and/or to rectification.



Common FAQs

Each controller may be able to instruct the data processor, North East London Integrated Care Board, to provide the audit logs to the data controller for the controller's review to ascertain how their patient's data has been used in LDS.

What are the access and audit controls on identifiable patient data?

Across the SDE we will implement role based access control such that only clinicians with a legitimate basis have access to identifiable data for direct care purposes and proactive care. Access is auditable and access priviledges are reviewed by each organisation's Caldicott Guardians.

How can I be reassured that there are no re-identification risks for my patients' data when it is pseudonymised or anonymised? And who/what process checks this?

The SDE programme has set up the SDE in line with the Six Safes Framework.



Common FAQs

One core element of the Six Safes Framework is the implementation of safeguards against the risk of re-identification. The OneLondon SDE programme has been following Information Commissioner's Office (ICO) draft guidance on pseudonymisation and anonymisation when finalising the design of the database. Guidance from the BMA and GMC on anonymisation have been consulted as well. Our comprehensive assessment concludes that the level of anonymisation envisaged for the SDE would be considered effectively anonymous considering the standards introduced by the ICO.

The datasets that flow into the database will be pseudonymised and stripped from identifiers. The key to the pseudonyms are kept separately and cannot be accessed by the researchers. To ensure this, technical and organisational measures including strict access controls are in place. This should ensure that there is no legal way to link the data with identifiers which would allow re-identification of patients.

Furthermore, researchers are required to sign Acceptable Use Policies when they request access to the database. This policy establishes standards which all staff and users (e.g. analysts and researchers) need to follow and puts restrictions on them on how they can use the data.



Common FAQs

They are strictly prohibited to attempt to re-identify anyone through the access that they receive. Breach of this can lead to severe consequences for them. Their access of data can be audited and if any misconduct is detected, access privileges will be revoked.

To minimise the risk to the data controllers we have specifically sought CAG's approval considering the richness of the data.

If a GP withdraws the data sharing agreement for the SDE – what happens to the patient identifiable data (including the pseudonymised data)?

Data flowing daily into the platform will stop, and all data sent by that practice will be permanently deleted. Any application with a use case relying on that data flow will no longer be able to read from the data, either for updates or for history.

A full scan will be run on the whole environment to check if any data is held in relation to the data controller to ensure that the data is removed.



Common FAQs

Signing the data processing and sharing agreements themselves may not pose risks in itself. The risks of the project are outlined in detail in each Data Protection Impact Assessment (DPIA). However, the programme has implemented appropriate technical and organisational measures aligned with the Six Safes Framework to minimise the risk of data breaches.

All data access requests that involve two or more Integrated Care Systems (ICSs) will go to the London Independent Information Access Group (IIAG) even though they only request aggregated data. If the project only involves one ICS then this access request will be progressed through the local Data Access Committees (DACs). This is to ensure clarity and consistency of the data access process. Additionally, this will help with central oversight over access applications and auditing.

Is there assurance that the data held in the London Data Service will not be used to performance manage GPs and their practices?

Yes. The data in the LDS is to be used for patient benefit, not to performance manage GPs and their practices.



Common FAQs

Can a patient opt out (object to) of their data flowing into the London Data Service? Will existing local opts be applied to the data and its use, how and when will these be applied?

There will be a local registry of dissent where a patient can object or dissent from implicit consent for all data sharing and a national data opt out will also apply for secondary uses of data.

Centralised dissent and local opt-outs to avoid transfer of workload to GP practices will be implemented when ready and are currently in development.

What is the difference between the London Data Service and the London Care Record?

The LDS is part of the London SDE which is an NHS environment. It securely extracts, transforms and stores data from across London for approved uses. This data can be directed to applications like the London Care Record (LCR) or the analytics platform within the London SDE.



Common FAQs

The LCR is a digital system that gives health and care staff an instant view of a person's health and care information when they need it at the point of care. It is an up-to-date record of their information over time and across different parts of the NHS and social care in London and some neighbouring areas.

The LDS supports the analysis of patient populations, improving the delivery of health and care (e.g. population health management, groups with similar care requirements and/or those diagnosed with the same illnesses). It speeds up how quickly the NHS can make decisions and the discovery of new treatments.

What data sharing/processing documents for the London Data Service and the London Analytics platform are my practice being asked to sign and why?

The OneLondon SDE requires five documents to be signed by data controllers: OL Data Sharing Framework, LDS data processing agreement, LAP data processing agreement, LDS data sharing specification, LAP data sharing specification.



Common FAQs

What is the London Independent Access Group?

Each ICS area will have its own Data Access Committee (DAC) that makes decisions about improving projects that use patient data.

Operating across all five DACs is a pan-London Independent Information Access Group (LIIAG) which acts as a recommending body and is the first port of call to review and triage pan-London applications before they are received by each DAC.

Is there a Data Access Committee for my ICS area?

Yes. It is being set up as part of the implementation.



Common FAQs

How do I as an individual GP practice get a say on how the data of my patients is being used?

The first and most important choice is whether GPs participate in the SDE by signing data sharing and processing agreements. The use of data for any particular project will be accessed by the local Data Access Committees (DACs) and as a data controller you will be represented on your local DAC (e.g. by your GP Data Protection Officer (DPO) or by attending directly).

What does it mean to me as a GP that the documents state I am a joint controller and have delegated my responsibilities to a data access committee? Does this absolve me of any responsibility if there is a legal challenge?

It means you remain in control and can make decisions about the use of your patients' data and can jointly make decisions about the use of the linked data set through your local Data Access Committee. For more information, please refer to the answer to the above question.



Common FAQs

The liability sits as a joint data controller and you continue to be responsible for ensuring that the processing of personal data takes place in compliance with the UK GDPR (see Article 24 UK GDPR), and all applicable legislation and data protection provisions/regulations.

Will all data requests go via the London Independent Information Access Group, even aggregate data ones?

Yes. All data access requests that involve two or more Integrated Care Systems (ICSs) will go to the pan-London Independent Information Access Group (LIIAG) even though they only request aggregated data. If the project only involves one ICS, this access request will be progressed through the local Data Access Committees (DACs).

This is to ensure clarity and consistency of the data access process. Additionally, this will help with central oversight over access applications and auditing.



Common FAQs

Who are the GP representatives on the London Independent Access Group? If it is GP data and SUS data, then there should be a number of GP representatives alongside the citizen reps.

There is currently GP representation on the pan-London Independent Information Access Group (LIIAG). There will be an expectation for the local London DAC groups to have appropriate GP and GP DPO representation.

Does each ICS Data Access/Usage groups have lay members (patient representatives)?

Yes, all DACs must have lay members.

Does the London Information Governance Steering Group (LIGSG) have patient representatives?

The LIGSG will not have any patient representatives. Pan-London Independent Information Access Group (LIIAG) will have patient representatives. This is part of the respective LIIAG Terms of Reference.



Common FAQs

How would an individual GP practice or PCN request for a local dashboard to be set up, would this be centrally or via a subscription request?

This would happen centrally. The individual GP practices or PCN would need to liaise with their local ICB. The ICB team would implement this through their central shared service (the London SDE).

What is the timeline for the GP analytics dashboard to be live for individual GP Practices to utilise?

We are intending some dashboards will be available from April 2025. The detailed timeline depends on two factors:

- The time required for practices to sign-up to LDS and LAP will determine when all the GP data will be available in the analytics platform.
- Intent from all five ICBs to commission a London-wide GP analytics dashboard as a London-wide dashboard would need to be commissioned by all five ICBs via the London Data Delivery Board for the LAP team to develop the dashboard. This intent has been expressed by all five ICBs.



Common FAQs

If there is a data breach with the OneLondon SDE, how would I know as an individual controller? Would the data breach be reported to the DSPT incident reporting tool/ICO/NHSE centrally or would each GP Practice be expected to report individually?

If there is a breach the OneLondon team will notify all data controllers. We would analyse the breach and advise on the next steps a GP would need to take. OneLondon would co-ordinate and liaise with NHSE and the ICO as appropriate.

When would a GP practice be liable if there is a data breach in the OneLondon SDE?

If your practice didn't cause the breach, you're not liable for it. Each party remains responsible for its own obligations; you are not liable for another organisation's breach. If the issue is with OneLondon's systems, OneLondon leads the investigation and regulatory steps. You will only be liable if the breach involved your own practice (e.g. an incorrect upload or inappropriate access by your staff). UK GDPR Article 82(3) confirms fault-based liability.



Common FAQs

What are the risks for a GP and their practice in signing the data sharing/processing documents?

Signing the data processing and data sharing agreements are a necessary part of signing up to the OneLondon SDE as a project. These agreements outline the responsibilities of the relevant parties (Data Controllers and Processors) in line with Article 28 of the UK GDPR and best data protection practices.

Signing the data processing and sharing agreements themselves may not pose risks in itself. The risks of the project are outlined in detail in each Data Protection Impact Assessment (DPIA). However, the programme has implemented appropriate technical and organisational measures aligned with the Six Safes Framework to minimise the risk of data breaches.

Has my DPO been consulted on the documents I am being asked to sign?

Yes, we have met the GP Data Protection Officers across the five ICSs and discussed the project, received their feedback and implemented it where necessary.



Common FAQs

Has a clinical safety assessment (DCBO129 and DCB0160) been completed for the London Data Service and the London Analytics Platform?

For the London Data Service, North East London Integrated Care Board (NEL ICB) is working with SafeHand who are acting as the Clinical Safety Officer. They are working towards a DCB0129 assurance for the solution itself and DB0160 for the implementation of the Clinical Risk Management. The work began with Hazard workshops and a Clinical Safety Plan was created. Relevant meetings, workshops are held and documentation drafted which should enable SafeHand to make a detailed assessment on the London Data Service (LDS).

This work continues until the LDS is ready to go live as there are some parts (like testing reports) that cannot be delivered until that work has been carried out. Beyond that point, in Live Service, the governance processes will be followed for enhancements to LDS and the Clinical Safety Officers either at SafeHand or with internal NEL ICB governance will be engaged to make sure any new functionalities are compliant.



Common FAQs

Do NHS Resolution Schemes cover everything?

No, the General Practice Indemnity Scheme (NHS Resolution) does not currently provide indemnity cover for the OneLondon SDE for GP Practices. Nor is there cover through Medical Defence Organisations, as that is linked to clinical indemnity, not public liability or data.

GP Practices are encouraged to check their current practice insurance policies as to whether they provide cyber and data cover.

Is it possible that an individual controller is liable for breach another controller is responsible for?

Generally, no. You are not liable for another organisation's breach. You could only be liable if your practice did not follow the processes it should have.

For example, sharing data beyond the agreed scope or not applying safeguards in your systems. Liability under UK GDPR is fault-based (Article 82(3)).



Common FAQs

Could a claimant still sue my practice even if we weren't responsible?

A Claimant might name your practice, but if you didn't cause the breach, you can show you weren't responsible. If it is shown that you were not responsible, but the other parties have had to pay compensation to the Claimant, you can recover your share of the compensation paid from the party that was at fault. Since you were not responsible if one party pays compensation, you can recover your fair share from the party at fault. The UK GDPR Article 82 allows full compensation from one party, with recovery from the responsible party.

Will the Information Commissioner's Office (ICO) fine my practice for someone else's incident?

No. The ICO looks at your conduct. If you met your duties and didn't cause the incident, you won't be fined for another party's failure.



Common FAQs

What should we expect if there is a breach?

- **If there is a breach in the OneLondon SDE, or in OneLondon's Systems:** OneLondon investigates and informs the Data Controllers through Data Access Committees (DACs) – there is one for each London ICS. If the breach is reportable to the ICO, OneLondon will report this on behalf of all the Controllers and update the Controllers through the DACs that it has been reported and inform the DACs if there are any actions for any Controller(s).

- **If it's in your practice and involved the OneLondon SDE:** Follow your normal breach process including contacting your DPO (contain, assess risk, notify the ICO within 72 hours if required, and inform affected patients where needed) and inform the Secretariat and London Information Governance Steering Group (LIGSG).

For more detail on the OneLondon data breach process please see 4.9.1.2 of the OneLondon Data Sharing Protocol (ODSP) – see this question of where to find the ODSP.



Common FAQs

Where can I find the legal documents that protect my practice?

See the documents on the Data Controller Console via your ICB DPO:

- **OneLondon Data Sharing Protocol** – principles, standards, and responsibilities between members
- **LAP OneLondon Data Processing Agreement, LDS OneLondon Data Processing Agreement** – provides instructions to NEL ICB and NWL ICB, respectively, when they process data on your behalf. NEL ICB and NWL ICB can only act on the instructions given
- **LDS OneLondon Data Sharing Specification and LAP OneLondon Data Sharing Specification** – sets out the details of each infrastructure project, including what data is shared and on what basis