

FAQs

Accountability

List of FAQs - Accountability Questions:

- What data sharing/processing documents for the London Data Service and the London Analytics platform are my practice being asked to sign and why?
- What is the London Independent Access Group?
- Is there a Data Access Committee for my ICS area?
- How does the data access approval process work?
- 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.



FAQs

Accountability

- 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?
- What is the timeline for the GP analytics dashboard to be live for individual GP Practices to utilise?
- 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?
- 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?
- What liability is there for an individual controller on a data breach in the OneLondon SDE?
- What are the risks for a GP and their practice in signing the data sharing/processing documents?



FAQs

Accountability

- 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?
- 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?



FAQs

Accountability

60. 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.

61. 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.

62. Is there a Data Access Committee for my ICS area?

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



FAQs

Accountability

63. How does the data access approval process work?

Researchers fill out a templated data access form for their project. This is first reviewed by the pan-London recommending body, LIIAG, and then reviewed by the ICS level Data Access Committees. If found to be in line with agreed access standards e.g. compliant with research for medical purposes, providing public benefit etc, it will be approved.

64. 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).



FAQs

Accountability

65. 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 Question 64.

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.



FAQs

Accountability

66. 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.

67. 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.



FAQs

Accountability

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

Yes, all DACs must have lay members.

69. 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.

70. 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).



FAQs

Accountability

71. 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.

72. 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.



FAQs

Accountability

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.

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.



FAQs

Accountability

73. 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.

74. 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.



FAQs

Accountability

75. 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.

76. 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.



FAQs

Accountability

77. 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.



FAQs

Accountability

78. 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.

79. 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)).



FAQs

Accountability

80. 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.

81. 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.



FAQs

Accountability

82. 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 question below of where to find the ODSP.



FAQs

Accountability

83. 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