

London Health Data Strategy

Data Controllers FAQ

ONE LONDON

London SECURE DATA ENVIRONMENT

Part of the NHS Research Secure Data Environment Network



Contents

01. Overview

02. Londonwide LMCs Statement

03. Common FAQs

04. FAQs - Lawfulness, Fairness and Transparency

05. FAQs - Purpose Limitation

06. FAQs - Data Minimisation

07. FAQs - Accuracy

08. FAQs - Storage Limitation

09. FAQs - Integrity and Confidentiality (Security)

10. FAQs - Accountability

11. Glossary



Overview

We're pleased to share that preparations for the London Secure Data Environment (SDE) are well underway, with a planned go-live in Spring 2025.

Once it is live, the London SDE will provide enhanced tools to support more proactive, data-driven care across the city.

In some areas, this will include new data flows and patient flags within the London Care Record, as well as proactive care dashboards that will allow you to view in-depth details of patients under your care. These improvements will help streamline workflows, improving decision-making and patient outcomes.

To support this launch, we've created a series of resources to address frequently asked questions and provide a clear overview of how the London SDE will function and impact your work.



Londonwide LMCs Statement

There has been broad public and professional engagement in relation to the London Secure Data Environment including extensive and continued involvement with Londonwide LMCs, who have been particularly focused on GP practices' data protection obligations and provided the below statement to explain their involvement.

Londonwide LMCs recognises the importance of effective information sharing and the benefits that shared data can realise for patients and GPs. That is why we 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.

We 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.

ONE LONDON

London SECURE DATA ENVIRONMENT

Part of the NHS Research Secure Data Environment Network



Londonwide LMCs Statement

We 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.

We will continue to support practices and work with OneLondon in regard to this.



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.

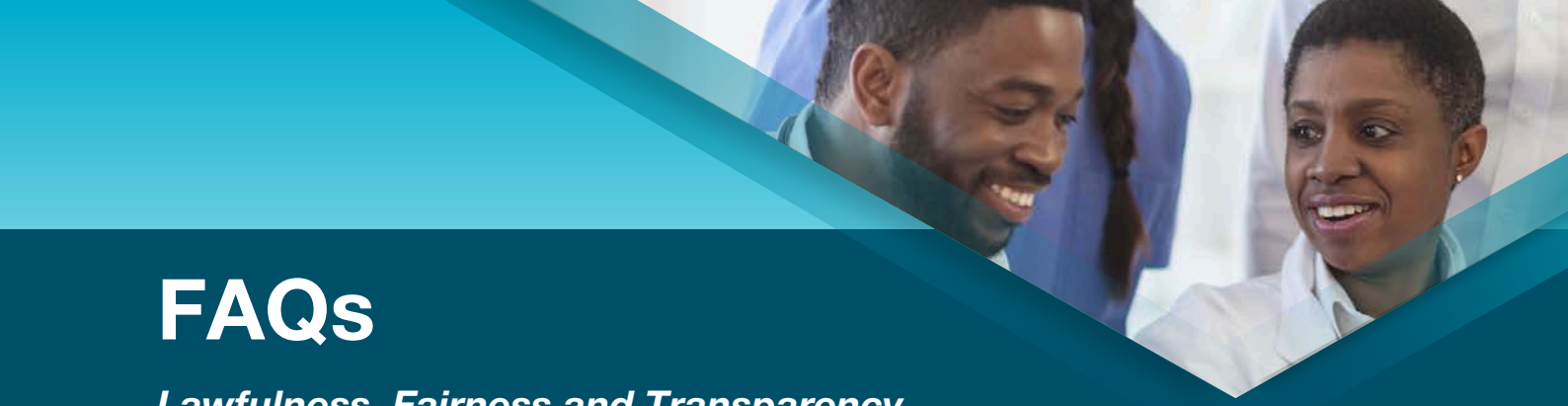


Common FAQs

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

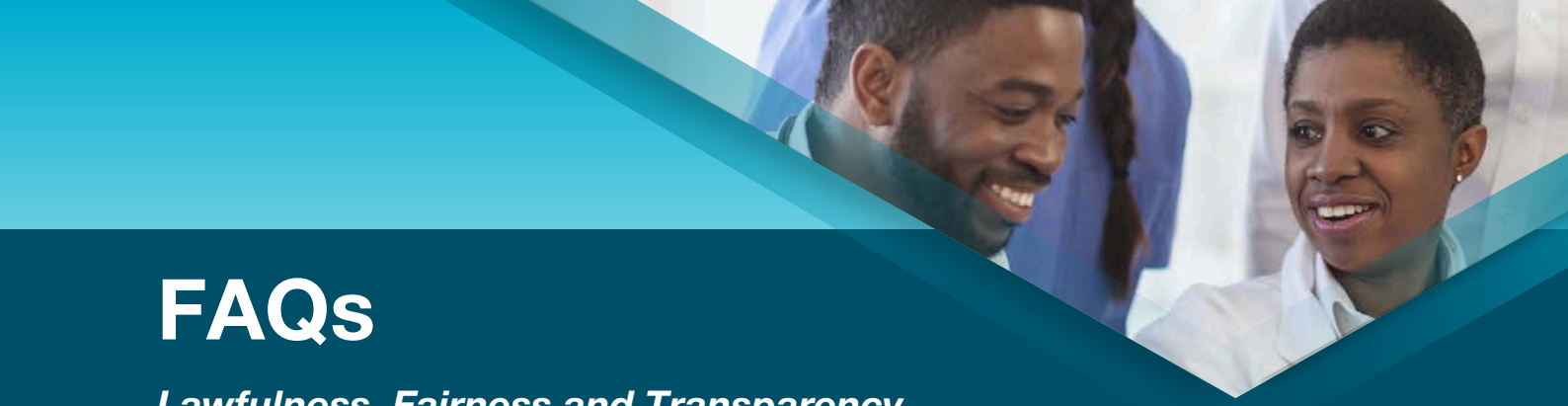


FAQs

Lawfulness, Fairness and Transparency

List of FAQ - Lawfulness, Fairness and Transparency Questions:

- What is the London Data Service (LDS)?
- What is the London sub-national secure data environment?
- Why does London need a sub-national secure data environment?
- What is the London Data Analytics platform?
- What data will be in the London Secure Data Environment (SDE)?
- Will data in the London SDE be used for research?
- What is the lawful basis for the data to be processed in the London SDE/London Analytics Platform (LAP) and how is the common law of confidentiality met for the data processed in the SDE?
- Does the processing of data in the London SDE (London Data Service and London Analytics Platform together) meet the GMC guidance on confidentiality?
- Kings Counsel (KC) Opinion - a. What is the conclusion of the KC opinion?



FAQs

Lawfulness, Fairness and Transparency

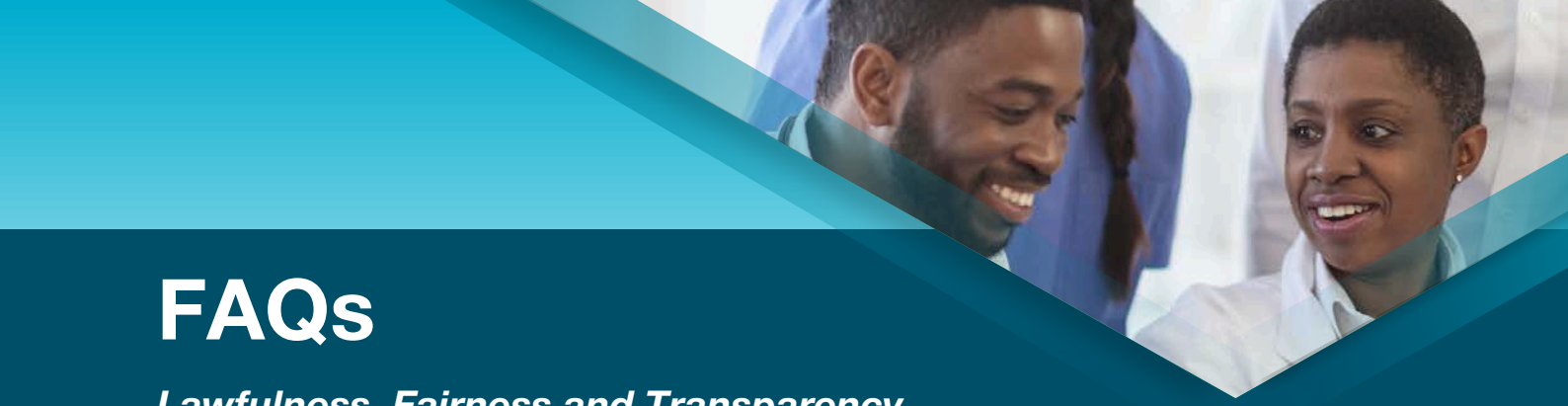
- Kings Counsel (KC) Opinion - b. Has there been any consideration of taking this to the high court for a conclusive legal view?
- Kings Counsel (KC) Opinion - c. GMC code of confidentiality
- Kings Counsel (KC) Opinion - d. Is there still a risk that a patient might sue a practice if they felt that their confidentiality had been breached?
- What are the lawful bases for the use of the data in the London Analytics Platform?
- 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?
- Is there a centralised dissent/opt out/objection service/team to avoid transfer of workload to GP practices and how will this work?
- Will existing local opts be applied to the data and its use, how and when will these be applied?
- Has the National Data Guardian been consulted on the SDE and what was their response?



FAQs

Lawfulness, Fairness and Transparency

- Has the BMA & GPCE (General Practitioners Committee England) been consulted on the SDE and what was their response?
- What patient consultation has there been with the development of the platform and the London Health Data Strategy?
- What are the plans for the communications for patients? What does this campaign look like?
- Are there materials available for patients now?
- If a GP has a query from a patient on the SDE who can they direct them to answer the query?
- Is there a layered privacy notice available for patients that a GP can link to from their practice website and links to both the IIAG and local data access group decisions?



FAQs

Lawfulness, Fairness and Transparency

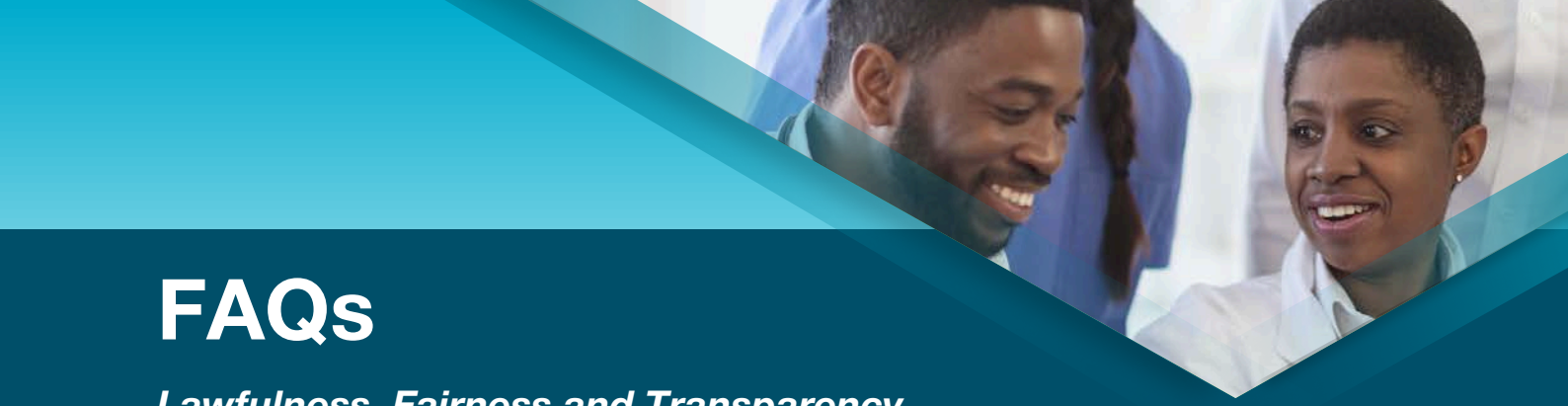
1. What is the London Data Service (LDS)?

The LDS is part of the OneLondon Secure Data Environment (SDE). 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 or the London Analytics Platform within the OneLondon SDE. North East London ICB is developing the LDS on behalf of all of London's ICSs so it covers the whole of London's population.

2. 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). Data ingestion is when data is collected and imported into a database.

The LDS provides a compliant infrastructure in which healthcare data (from all settings) can be ingested (data is collected and imported ito a database), cleaned (removing incorrate, duplicate and/or corrupt data), curated (data is maintained and organised) and shared with LAP.



FAQs

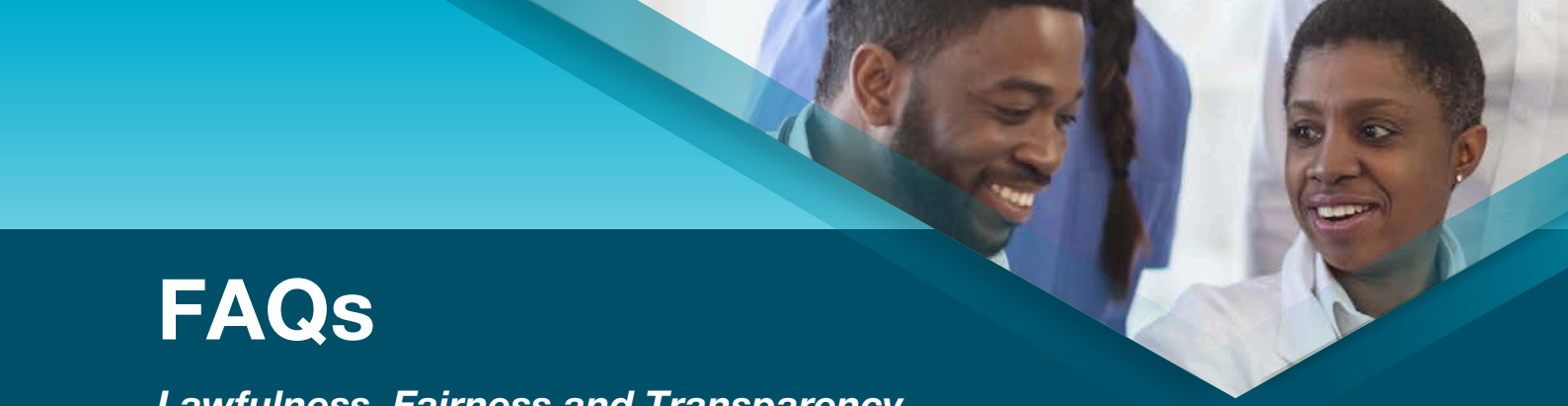
Lawfulness, Fairness and Transparency

The LAP receives identifiable data from LDS and performs a range of uses, including direct care, provision of proactive health and care (population health management), commissioning, assessing and improving health and care and research. Identifiable data is only used for direct care purposes. It is pseudonymised for any other purpose.The data for listed purposes will be accessed by approved individuals for approved projects.

3. 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.
- **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.



FAQs

Lawfulness, Fairness and Transparency

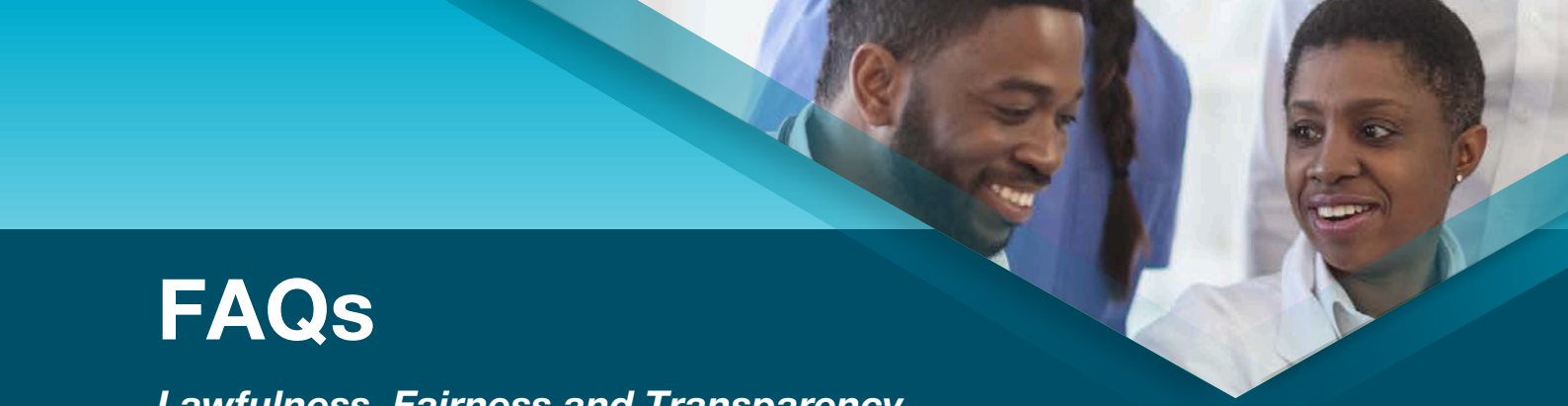
Secure Data Environments enable many different sources of data to be linked, so prepared data can be more easily accessed if needed again. This means that researchers and analysts can access bigger sets of data faster. This will speed up how quickly the NHS can make decisions and discover new treatments.

4. What is the London Data Analytics platform (LAP)?

The LAP subscribes identifiable data from the LDS and uses this to provide tools for clinical teams to provide direct care, provision of proactive health and care (population health management), and interrogate the data for commissioning, assessing and improving health and care, and research. Identifiable data is only used for direct care purposes. It is pseudonymised for any other purpose.

5. What data will be in the London Secure Data Environment (SDE)?

Initially routinely collected structured data will be from NHS providers (acute, mental health, community) and primary care. These may be added to in the future including social care where data controllers agree.



FAQs

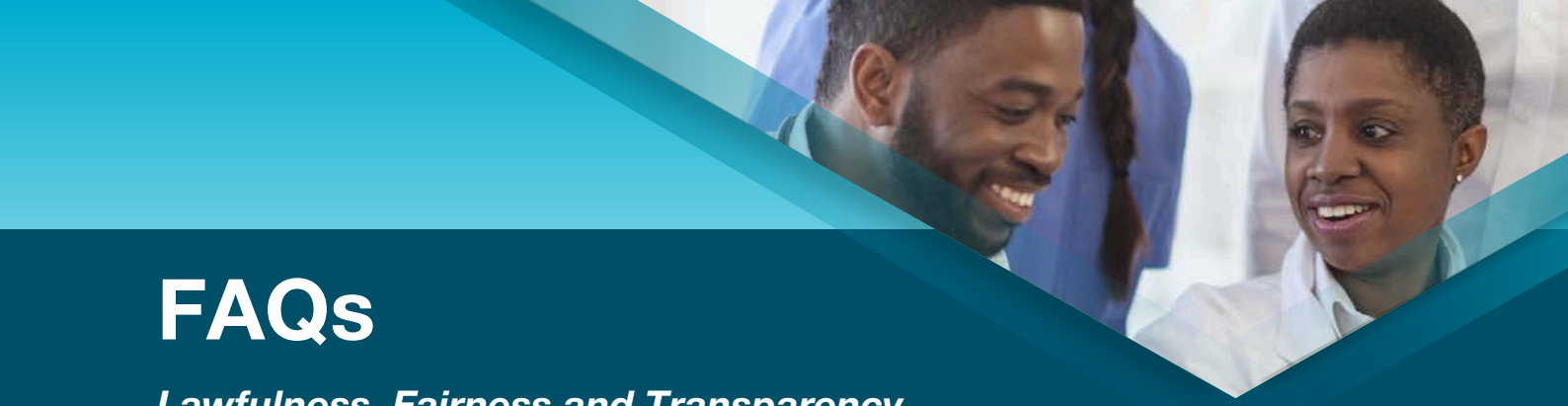
Lawfulness, Fairness and Transparency

6. Will data in the London SDE be used for research?

Where data controllers sign up, data will be accessible within the SDE for direct care provision of proactive health and care (population health management), and to interrogate the data for commissioning, assessing and improving of health and care, and research purposes. 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. Confidential Patient Information wil only be used for direct care and under roles-based access controls (similar to the London Care Record). Only pseudonymised data will be made accessible for research.

7. What is the lawful basis for the data to be processed in the London SDE/London Analytics Platform (LAP) and how is the common law of confidentiality met for the data processed in the SDE?

There are two main legal considerations when processing data in the London SDE: requirements under UK GDPR, and expectations based on the Common Law Duty of Confidentiality (CLDC).



FAQs

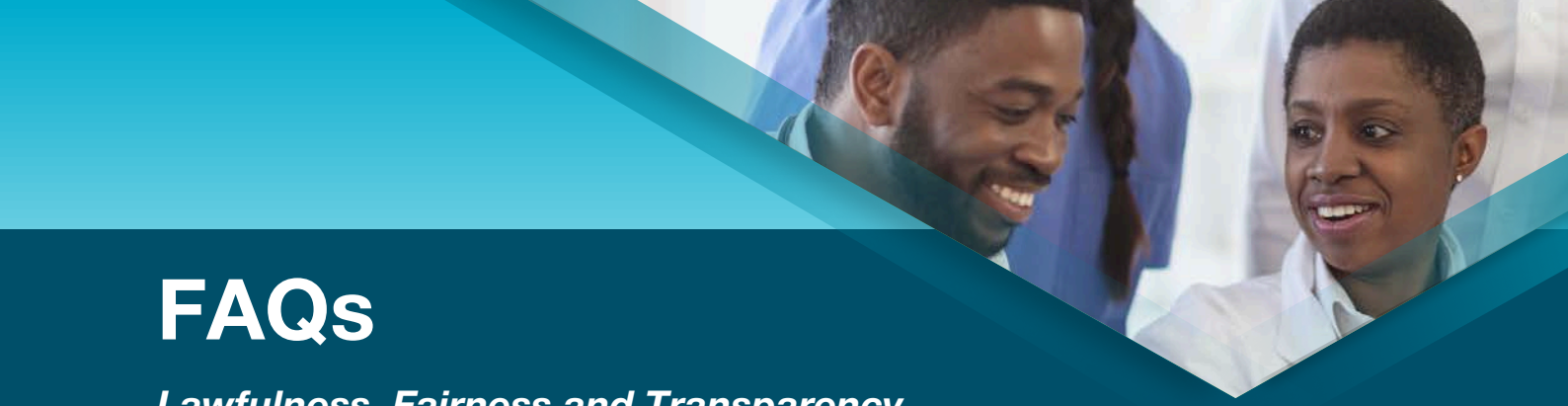
Lawfulness, Fairness and Transparency

Under the UK General Data Protection Regulation, the SDE will rely on the following lawful bases for processing data:

- 6(1)(e) necessary for data controllers to perform their tasks in the public interest;
- 9(2)(h) necessary for the provision of health or social care, including preventative or occupational medicine,
- 9(2)(i) necessary for reasons of public interest in the area of public health,
- 9(2)(j) necessary for archiving purposes in the public interest, scientific or historical purposes.

These lawful basis will be relied on because the SDE will process data on behalf of the NHS providers and local commissioners' from the five London Integrated Care Systems, acting as public authorities.

In doing so, the SDE will serve to provide a London-wide solution for standardisation, restructuring and storage of data to support a range of interoperability projects in London for different public interest purposes that include provision of direct and proactive healthcare, planning and commissioning, improving healthcare services, and enabling research.



FAQs

Lawfulness, Fairness and Transparency

Under the CLDC, where data is used for direct care purposes we assume implied consent; and where data is linked and accessed for secondary purposes we operate under Secretary of State directions granted under the s251 powers (see Q52 &53 for answers relating to s251).

8. Does the processing of data in the London SDE (London Data Service and London Analytics Platform together) meet the GMC guidance on confidentiality?

Yes, it does.

The data processed in the SDE meets the eight principles under the General Medical Council's guidance on confidentiality because of the 'Data Protection by Design and Default' approach and the robust technical and organisational measures applied.

Data Controllers will be provided all the necessary information about the Data Access Committees and their responsibilities through extensive and comprehensive stakeholder engagement.



FAQs

Lawfulness, Fairness and Transparency

- **Use the Minimum Necessary Personal Information -** At the point of extraction of data from the SDE environment, the principle of Data Minimisation will be applied by the Data Controllers as part of the necessary due diligence and assurance. It is only at that point that the Data Controllers, by concretely defining the purpose for which the data will be used and determine the nature of the data that needs to be processed in order to achieve that concretely defined purpose, will be able to assess what data is strictly necessary for the envisaged purpose.

- **Be Aware of Your Responsibilities** - Only members of staff that have completed all mandatory Information Governance training will have access to the data processed as part of the SDE. They will also have confidentiality clauses in their contracts. Those regular Information Governance Trainings will cover their responsibilities around handling confidential data.

- **Comply with the Law** - The OneLondon programme has assured itself around legalities by taking advice from IGS, a specialist information governance consultancy, a King's Counsel, and continues to collaborate with stakeholders such as the Information Commissioner's Office, the National Data Guardian.



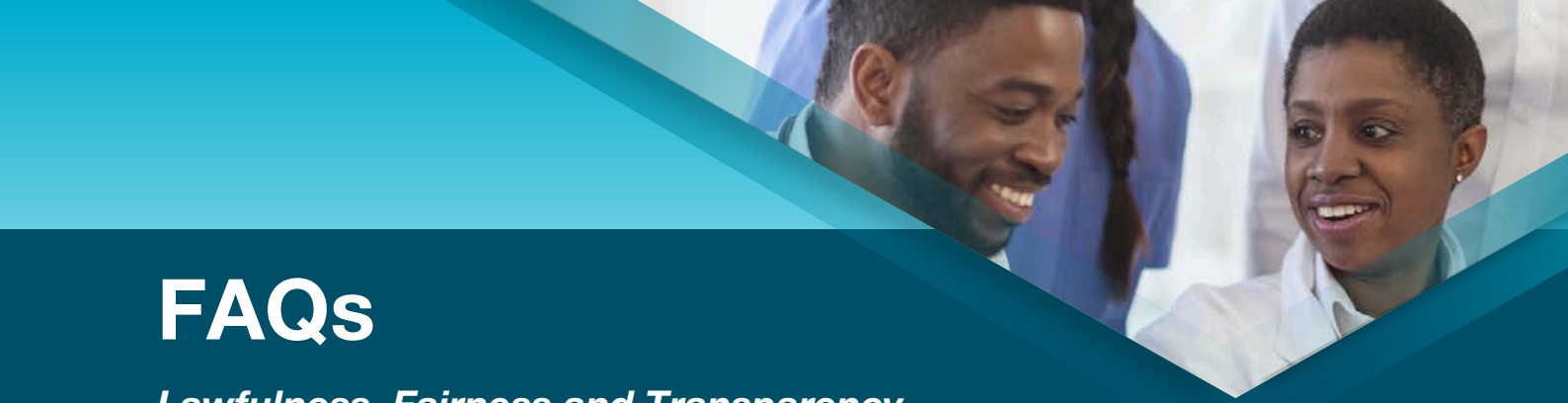
FAQs

Lawfulness, Fairness and Transparency

- It has also received support from the Confidentiality Advisory Group under s251 of the NHS Act (2006). Participating data controllers are involved through stakeholder engagement and can review all documentation for their due diligence purposes, thus ensuring their compliance as well.

- **Share Relevant Information for Direct Care -** At the point of extraction of data from SDE, all direct care use cases will be first approved by the Data Controllers, either individually or collectively through a comprehensive due diligence exercise via Data Access Committees. OneLondon SDE Programme applies all dissent and opt-out requests recorded in their registers.

- **Ask for explicit consent to disclose identifiable information other than direct care -** All use cases where SDE will be approved by the Data Controllers, either individually or collectively through a comprehensive due diligence exercise which includes an assessment of how confidentiality is satisfied.

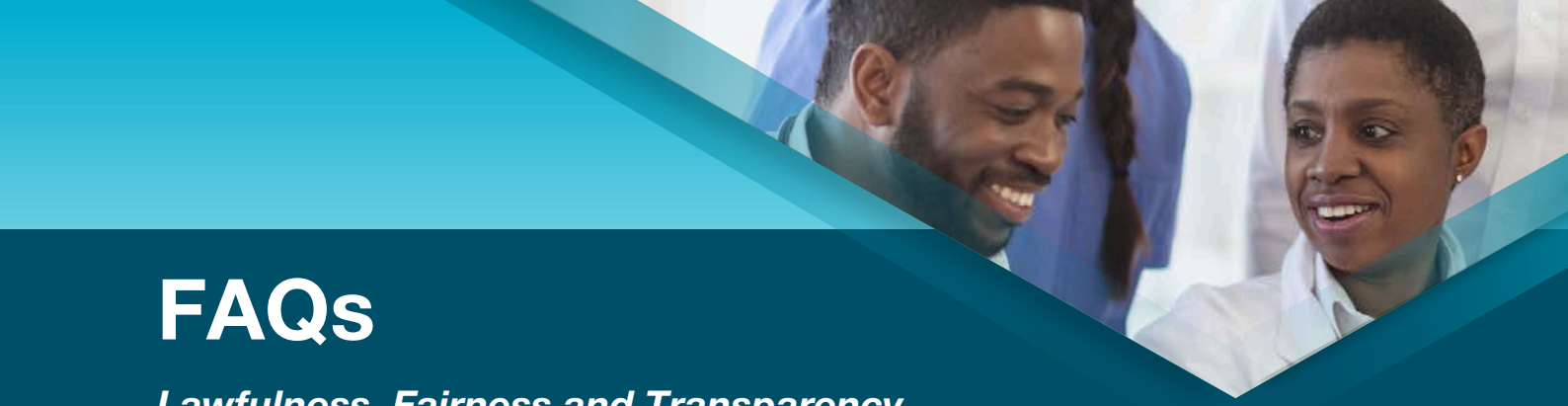


FAQs

Lawfulness, Fairness and Transparency

- **Tell Patients -** Extensive and unparalleled public deliberation has been taking place since the start of the programme, including the OneLondon Citizens' Summit. Londoners have expectations that the OneLondon SDE will improve the delivery of direct care. Additionally, for each interoperability project for which data will be extracted from SDE, a programme-specific Privacy Notice, in compliance with the UK General Data Protection Regulation, will be provided. Other transparency and communication materials such as posters, leaflets etc, will be developed and distributed.

- **Support patients to access information -** Insofar as they are required by law, all Data Subject Rights will be upheld. OneLondon Programme has been advised by IGS, a specialist information governance consultancy, to implement a centralised mechanism for complying with data access requests. Patients will be informed about their data subject rights and how they can exercise them through transparency and communication materials, including privacy notices, posters and leaflets etc.



FAQs

Lawfulness, Fairness and Transparency

9. Kings Counsel (KC) Opinion - What is the conclusion of the KC opinion?

The KC was of the opinion that the data sharing carried out under SDE is "*unlikely to involve an actionable breach of confidence*" and "*unlikely to involve a breach of national opt-out*s".Therefore, the KC was of the opinion that the probability of a breach of confidence occurring is very low. We have further minimised the risk of a breach by obtaining section 251 support.

a. Has there been any consideration of taking this to the high court for a conclusive legal view?

No, the programme has concluded that legal due diligence and stakeholder engagement to date is sufficient to confirm an appropriate approach to data processing, and further expenditure would not represent good use of public funds.

The OneLondon Health Data Board reviews and directs the SDE program. These are made after consulting the stakeholdes in the programme and relying on independent advice. The risk would be carried by the data controllers who are jointly involved in OneLondon SDE.



FAQs

Lawfulness, Fairness and Transparency

b. GMC code of confidentiality

This was referenced in the position paper and KC opinion and the approach was seen to be compliant. "*We are fortified in our conclusions by the relevant publicly available guidance from the DHSC, General Medical Council (GMC) and the British Medical Association "BMA) on the question of implied consent. As set out at page 27 of the Position Statement, these organisations have published various guidance documents relating to confidentiality and implied consent.*"

c. Is there still a risk that a patient might sue a practice if they felt that their confidentiality had been breached?

The KC was of the opinion that data sharing carried out under the SDE is "*unlikely to involve an actionable breach of confidence*". To further minimise the risk we have received support from Confidentiality Advisory Group under section 251 of the NHS Act 2006.

- CAG Reference for research is 24/CAG/0155
- CAG Reference for non-research is 24/CAG0156



FAQs

Lawfulness, Fairness and Transparency

The CAG registers for research and non-research projects can be found **here**.

10. What are the lawful bases for the use of the data in the London Analytics Platform?

This has been answered in **Question 8**.

11. 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?

The OneLondon SDE Programme has conducted extensive and comprehensive public engagement deliberations and is planning to continue to engage and involve the public in the future. Dissent and opting out were and will be a topic of discussion where members of the public can voice their opinions and concerns. Overall, the OneLondon SDE will comply with the right to dissent, national data opt-out, Type 1 opt-out, right to object and local data opt-out. This will further inform our approach.



FAQs

Lawfulness, Fairness and Transparency

12. Can a patient opt out (object to) of their data flowing into the London Data Service?

The OneLondon SDE Programme has conducted extensive and comprehensive public engagement deliberations and is planning to continue to engage and involve the public in the future. Dissent and opting out were and will be a topic of discussion where members of the public can voice their opinion and concerns. Overall, the OneLondon SDE will comply with the right to dissent, national data opt-out, Type 1 opt-out, right to object and local data opt-out. Once the process of opting-out is set up, the patients will be informed through transparency and communications materials, such as privacy notices, posters, leaflets etc. We are told that the SDE programme, at national level, are going to also carry out a deliberative workshop on opt-outs. This will further inform our approach.

13. Will existing local opts be applied to the data and its use, how and when will these be applied?

Please view the answer to the above question.



FAQs

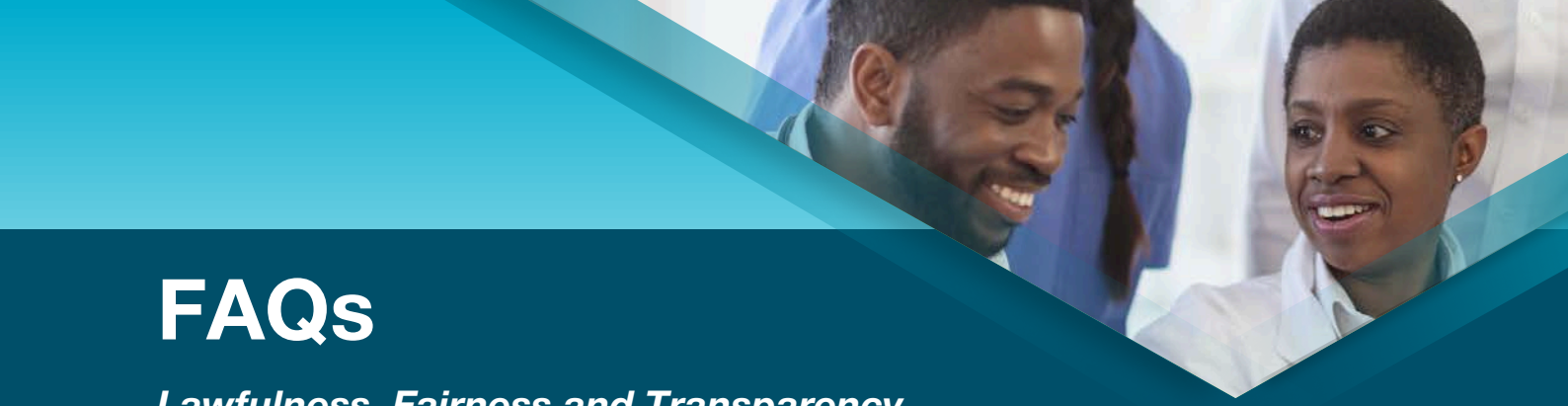
Lawfulness, Fairness and Transparency

14. Is there a centralised dissent/opt out/objection service/team to avoid transfer of workload to GP practices and how will this work?

The OneLondon SDE Programme has conducted extensive and comprehensive public engagement deliberations and is planning to continue to engage and involve the public in the future. Overall, the OneLondon SDE will comply with the right to dissent, national data opt-out, Type 1 opt-out, right to object and local data opt-out. Once the process of opting-out is set up, the patients will be informed through transparency and communications materials, such as privacy notices, posters, leaflets etc. We are told that the SDE programme, at national level, are going to also carry out a deliberative workshop on opt-outs. This will further inform our approach.

15. Has the National Data Guardian been consulted on the SDE?

We have consulted the National Data Guardian (NDG) and their views have been acted on including seeking a s251 CAG support for use of confidential patient information for secondary purposes.



FAQs

Lawfulness, Fairness and Transparency

16. Has the Information Commissioner's Office (ICO) been consulted on the SDE and what was their response?

We have been informed by the ICO that they are supporting regional SDEs at national level by working with NHS England's Information Governance (IG) policy team. Since then, we have liased with the IG policy team at NHS England and agreed all further engagement with the ICO for the purposes of the OneLondon SDE will be carried out by NHS England, on behalf of the OneLondon programme. Any feedback will be acted upon.

17. Has the BMA & GPCE (General Practitioners Committee England) been consulted on the SDE and what was their response?

The BMA (which includes the GPCE) has been contacted and we have requested a meeting with them to discuss the work undertaken by the SDE programme. Thus far, we have shared briefing notes and documents with them for senior members of the BMA to review. Once their review is complete, we will arrange a meeting. No objections have been raised.



FAQs

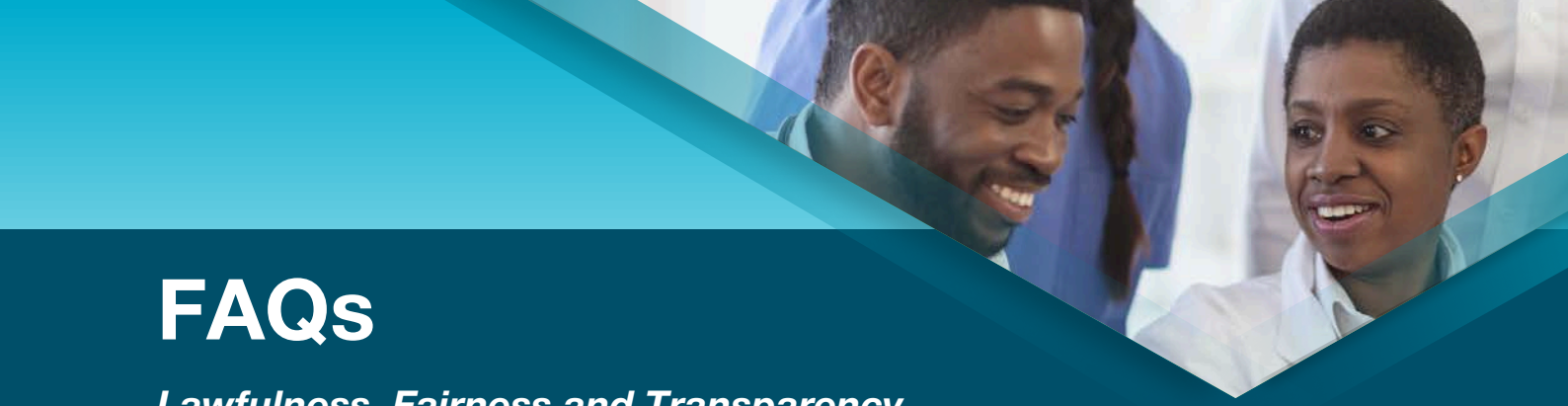
Lawfulness, Fairness and Transparency

18. What patient consultation has there been with the development of the platform and the London Health Data Strategy?

Since 2020, there have been three London-wide public deliberation events which have asked representative groups of Londoners for their views on access to identifiable health and care data for direct care purposes, access to anonymised health and care data for reasons beyond direct care, deciding who has access to health and care data and for what purposes, charging for health and care data access and the value exchange and how they feel the public should be engaged with.

These results have been used to shape the role of citizens in the programme and design the approval process of accessing data e.g., establishing the Independent Information Access Group (IIAG).

The programme also has citizen representatives who inform pilot projects (known as the pathfinder projects). These projects also included public engagement and involvement.



FAQs

Lawfulness, Fairness and Transparency

19. What are the plans for the communications for patients? What does this campaign look like?

In 2024/25 there is national engagement taking place which London patients are feeding into. There has been one event in north London on the role of health and care data and there is due to be a second event in south London focused on the role of the data held by GPs (most SDEs have one event, some have none). The report from the first engagement is due to be published in November. The third engagement will centre on the national opt out. This work is being led by NHS England and we are planning to use the insights from this to inform public communications, with the aim to start planning a wider public facing campaign in Q4. We are currently reviewing public facing campaigns from Greater Manchester and the North East.

20. Are there materials available for patients now?

Yes. Please view the infographic and public deliberation summaries.



FAQs

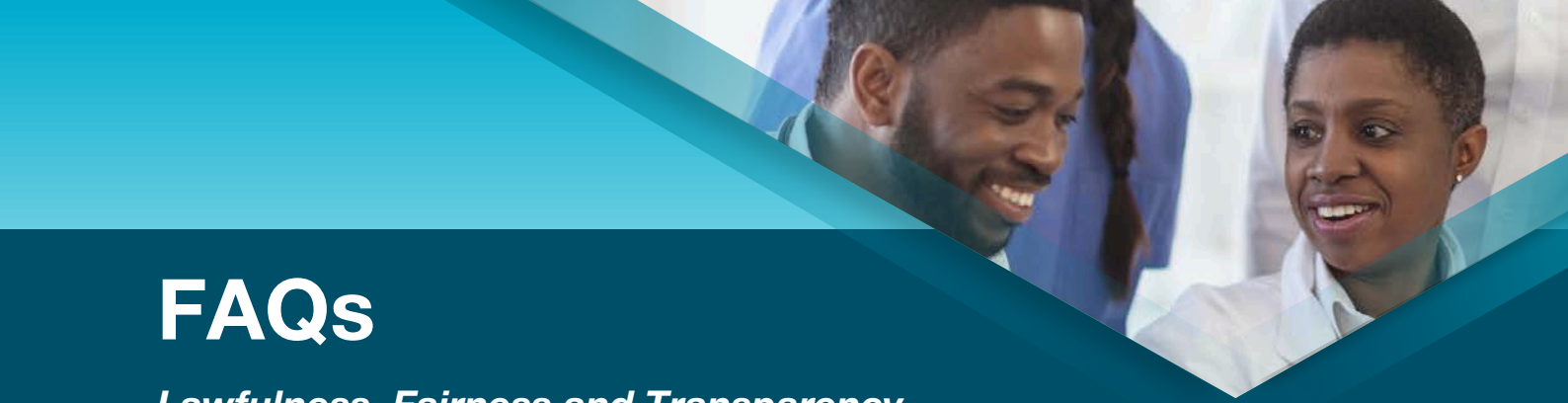
Lawfulness, Fairness and Transparency

21. If a GP has a query from a patient on the SDE who can they direct them to answer the query?

For general queries we will have full information available on the OneLondon website. For specific queries on opting-out, the patients will be informed of the details of a central mailbox and telephone number through transparency and communications materials, such as privacy notices, posters, leaflets etc.

21. Is there a layered privacy notice available for patients that a GP can link to from their practice website and links to both the IIAG and local data access group decisions?

We have developed exemplar privacy notices for both the London Data Service and the London Analytics Platform for all GPs who want to sign up to the OneLondon Data Sharing Framework, which supports the sharing of data amongst the healthcare organisations across the London region, which GPs can use on their website. Additionally, the privacy notices will be made available on the OneLondon SDE website as well to which patients can be referred.



FAQs

Lawfulness, Fairness and Transparency

The privacy notices were drafted in line with the legal requirements under the UK General Data Protection Regulation and Information Commissioner's Office guidance. As such, they provide the reader with all necessary information on the programme, the purposes, their rights and how to exercise them.

It will enable them to understand what is going to happen to their data and they will be able to make informed decisions. This can be layered in a digital format. Easy read, plain English and translated versions are also being drafted to make the information accessible for all.



FAQs

Purpose Limitation

List of FAQs - Purpose Limitation Questions:

- The lawful basis is reliant on the data being processed for direct care. What are the direct care priorities for each London ICS area and the London region now and planned?
- What are the benefits for my patients of their data flowing to the London Data Service?
- What are the benefits to me as a GP and to my practice?
- What are the benefits for my borough, my ICS and for London?
- As a GP, I am a controller for the data of the patients registered at my GP practice, who makes the decision on how their data will be processed/used?
- As a GP, I am content for data to flow to the London Data Service for direct care, but I am not comfortable with the data being effectively contextually anonymised to be used for research purposes. Can I just sign up for the direct care purposes for now?



FAQs

Purpose Limitation

- What is the definition of proactive care for the SDE (London Data Service and London Analytics) platform?



FAQs

Purpose Limitation

22. The lawful basis is reliant on the data being processed for direct care. What are the direct care priorities for each London ICS area and the London region now and planned?

While the London ICSs are developing their proirities, the programme has been working on a number of direct care dahsboards that will be availble once the SDE is live, an example of which is the CVD Action tool which has been widely piloted across London.

23. 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.



FAQs

Purpose Limitation

24. 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. It will also include proactive care dashboards allowing clinicians to drill down to identifiable patients in their care.

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

It will:

- Make 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;

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



FAQs

Purpose Limitation

- 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.

26. As a GP, I am a controller for the data of the patients registered at my GP practice, who makes the decision on how their data will be processed/used?

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 through the ICS level Data Access Committees (DACs). All five ICSs will also be represented on a pan-London Independent Information Access Group (LIIAG).

All DACs will keep a public log of the requests that they have considered. Each DAC can collectively reject or object to a request but each GP practice will not be able to at practice level.



FAQs

Purpose Limitation

27. As a GP, I am content for data to flow to the London Data Service for direct care, but I am not comfortable with the data being pseudonymised to be used for research purposes. Can I just sign up for the direct care purposes for now?

No.

The London SDE implements the recommendations of the London Citizens' Assembly, where residents expressed an expectation that GPs share data about them for both direct care and secondary purposes, under the safeguards of the 'six safes' framework.

Much of the development of the SDE has been funded through national taxpayer investment that specifically includes obligations to support research. There is therefore no general mechanism for participating data controllers to decline the whole class of research uses; but GP practices will be able to turn down any specific research proposals that they object to through the local Data Access Committees that appraise all research requests.



FAQs

Purpose Limitation

28. What is the definition of proactive care for the SDE platform?

Proactive (or anticipatory) care is an activity undertaken by clinical teams to assure themselves that patients under their care are receiving safe, timely, and high-quality care; and to support action in cases where there are opportunities to improve care for a named individual.

Typically, proactive care employs analytical methods to review information about a person and the care they have received. This helps to indicate opportunities for early interventions related to the prevention, investigation, and treatment of illness, or to confirm where no care gaps are identified for a person and therefore no intervention is required.

Examples include 'care gap analysis', where individuals with a relevant clinical traits (such as a diabetes diagnosis) are identified and information about events they have recorded (such as date of last care plan review) are compared against the agreed standards of care (such as the diabetes care processes). The aim is to help inform clinical teams about possible actionable opportunities for prevention, diagnosis, or treatment.



FAQs

Purpose Limitation

Other examples include the identification of patterns that are characteristic signals of concerning undiagnosed pathologies, disease progressions, or exacerbations. These approaches typically use validated computer programmes (i.e algorithms) to assign a risk score (or indices of suspicion) to everyone in the dataset, operating as a Clinical Decision Support tool. Examples include tools such as QRisk or QCancer.

Where individuals have risk factors above a clinical threshold, clinical teams can identify individuals for whom early intervention would likely be beneficial. These methods have the potential to diagnose an underlying pathology earlier (achieveing 'stage shift' in cancer diagnosis), or ameliorate the suffering caused by potentially avoidable disease progression or exacerbation.

In the London SDE, these analytical tools are managed using roles-based access controls to ensure that information is only accessible to regulated health or socal care professionals and their team, with whom the individual has a legitimate relationship for their care. Critically, proactive care is likely to be enhanced when the information used for analysis is a more complete picture of a person's whole care record, rather than relying on any single silo of information within a single care setting.



FAQs

Purpose Limitation

This more integrated and holistic approach requires access to a health record that is linked across care settings.

The use of similar analytical methods, used at the population level rather than for named individuals, is not proactive care. Whilst these are vitally important activities of population health management, these constitute indirect care activites and (where possible) these should not be undertaken using confidential patient information.

In the London SDE, these types of indirect care processes do not use confidential patient information - instead a anonymised dataset is used, operating under the controls of the 'six safes' framework. This implements the recommendations made by Londoners in citizens' assemblies that have considered the specific uses and protections of health and care information.



FAQs

Data Minimisation

List of FAQs - Data Minimisation Questions:

- Please can you provide clarity on when data is anonymised and when it is pseudonymised in the London Data Service?
- Is the data pseudonymised when it first flows to the London Data Service?
- 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?
- What are the access and audit controls on the identifiable patient data?
- Does the data in the SDE include sensitive codes and legally excluded data flow to the SDE and if so, what is the policy on processing these?
- Is it lawful to hold them in the SDE London Data Service if they are not being used?



FAQs

Data Minimisation

32. Please can you provide clarity on when data is anonymised and when it is pseudonymised in the London Data Service?

The data that flows into the London Data Service (LDS) will be in identifiable format. Once it is ingested into the LDS, it will be pseudonymised as soon as practically possible, before being subjected to further processing activities.

In practice, the pseudonymisation of the data will be carried out as soon as the processes of 'NHS tracing and validation', 'NHS number checking against National Data Opt-out repository' and 'associated geographical data derivation' take place, as these, by their very nature, require the processing of identifiable data. After this, pseudonymisation process will take place and all core-processing including data standardisation, cleansing and other geographical data derivations will be performed on the Pseudonymised Data.

The identifiable data will be kept separate and access to the identifiable data will be restricted to those System Administrators who absolutely require it to perform their duties.



FAQs

Data Minimisation

33. Is the data pseudonymised when it first flows to the London Data Service?

No, the data ingested into the London Data Service (LDS) from the Data Controllers will be in identifiable format. It will only then be pseudonymised in the LDS environment as part of LDS's services on behalf of, and under instructions from, the Data Controllers.

34. 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. One core element of the Six Safes Framework is the implementation of safeguards against the risk of re-identification.

The datasets that flow into the database will be pseudonymised. 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.



FAQs

Data Minimisation

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. 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 obtained Section 251 CAG approval considering the richness of the data.

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

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



FAQs

Data Minimisation

36. Does the data in the SDE include sensitive codes and legally excluded data flow to the SDE and if so, what is the policy on processing these?

We will routinely exclude legally restricted codes (previously referred to as 'sensitive records') from any further processing in LDS including any data flow to London Analytics Platform unless there is a legal provision to include them e.g. disease epidemic.

37. Is it lawful to hold them in the SDE London Data Service if they are not being used?

Please refer to the answer above.



FAQs

Accuracy

There is only one FAQ under the FAQs - Accuracy section, which is shown below.

41. A presentation shown in SWL on slide 20 states that the tools cannot be used to make changes to the patient record. Can you confirm that the GP data integrity, including QOF and other metrics, is protected?

The SDE works by ingesting data, from a data controller, where a data sharing agreement has been signed. This is achieved through a national mechanism once the permission has been updated in the local GP practice system. The flow of data is one-way, and there is no facility to write-back into the GP record, though data items can be made visible to clinical teams through the London Care Record.



FAQs

Storage Limitation

List of FAQs - Data Minimisation Questions:

- There are concerns over the large data set in the SDE London Data Service and the risk of re-identification. What are the controls to manage the risk of re-identification?
- Is it possible to filter/restrict the data flow to the SDE London Data Service to only the data that is needed for the agreed use cases now?
- If a GP withdraws the data sharing agreement for the SDE London Data Service and the London Analytics platform – what happens to the patient identifiable data (including the pseudonymised data) in the SDE two platforms? Is it put beyond use or deleted?
- What happens to the patient identifiable data of patients who move out of the London region and what happens to the contextually effectively anonymised data for those patients?



FAQs

Storage Limitation

42. There are concerns over the large data set in the SDE London Data Service and the risk of re-identification. What are the controls to manage the risk of re-identification?

The SDE programme has set up the SDE in line with the Six Safes Framework. One core element of the Six Safes Framework is the implementation of safeguards against the risk of re-identification. As explained above, the datasets that flow into the database will be pseudonymised.

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.

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. They are stricly prohibited to attempt to re-identify anyone through the access that they receive.



FAQs

Storage Limitation

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 obtained Section 251 CAG approval considering the richness of the data.

43. Is it possible to filter/restrict the data flow to the SDE London Data Service to only the data that is needed for the agreed use cases now?

It is not possible for the SDE to receive a narrower set of records than those sent from the source system for a given data controller. The data flow is 'all-or-nothing' from the source system.

However, it is possible to filter the data flow on SDE to ensure that only the data needed for each approved project is accessed by approved users. Section 251 CAG approval was obtained to support the considerations around proportionality.



FAQs

Storage Limitation

44. If a GP withdraws the data sharing agreement for the SDE London Data Service and the London Analytics platform – what happens to the patient identifiable data (including the pseudonymised data) in the SDE two platforms? Is it put beyond use or deleted?

If a GP withdraws the data sharing agreement for the SDE then the 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.

45. What happens to the patient identifiable data of patients who move out of the London region and what happens to the contextually effectively anonymised data for those patients?

We will retain information in line with the Record Management Code of Practice and the retention schedules of the programme.



FAQs

Storage Limitation

If a patient moves out of the London region and registers with a new GP practice outside of London, then the SDE will from that point not receive any further GP practice record updates. The historic data will be retained in effectively pseudonymised form. This is in order to ensure that an accurate history of the patient's activity while registered with a London practice is maintained, for example to enable accurate historic population health management analysis.

Should the patient be treated within the bounds of London again at a later date, there will also be a benefit to the patient's record of care being retained in that use case also.



FAQs

Integrity and Confidentiality (Security)

List of FAQs - Integrity and Confidentiality (Security) Questions:

- What is a secure data environment?
- What are the six safes and how do these ensure the data is safe?
- Will the data only be processed within the UK?
- Who are the processors and sub-processors involved in the London Data Service?
- Who are the processors and sub-processors involved in the London Analytics platform?
- Is the London Data Service part of the Federated Data platform?
- What is Section 251/a s251?
- Is there a s251 for the London Data Service?
- There will be a lot of valuable data in one place, how do I know that this will be safe?
- What safeguards are in place to protect the data from unauthorised access?
- What safeguards are in place to protect the data from cyber-attacks?



FAQs

Integrity and Confidentiality (Security)

- Has there been an independent cyber security assessment completed on the London Data Service and the London Analytics platform?
- Were there any high risks identified that can't be mitigated?
- Did this include penetration testing of the platforms?
- Will regular penetration testing be undertaken?
- Is there assurance that the data held in the London Data Service will not be used to performance manage GPs and their practices?
- My ICB has a sandpit environment. How does data flow from the London Data Service to an ICB sandpit and who controls/authorises this?



FAQs

Integrity and Confidentiality (Security)

46. What is a secure data environment?

The OneLondon SDE provides a six-safes compliant infrastructure in which health care data (from all settings) can be ingested, cleaned, curated, and accessed by approved users (either as patient identifiable or pseudonymised) to be used for other approved applications/projects using powerful tools for direct care, provision of proactive health and care (population health management), and to interrogate the data for commissioning, assessing and improving of health and care, and research.

47. What are the six safes and how do these ensure the data is safe?

Data processed and stored for the purposes of the OneLondon SDE will be protected by a combination of robust technical and organisational measures, in line with the Six Safes Framework.

- **Safe People** - Only members of staff that have completed all Information Governance training, and who have necessary credentials and authorisation will have access to patient-level data on a need-to-know basis.



FAQs

Integrity and Confidentiality (Security)

- There will be auditing capabilities to prevent abuse of authorised access by the Data Processors. For the purposes of the SDE, identifiable data will be made available only through dashboard visualisation technology to healthcare professionals with legitimate relationship with the patients. Users (e.g. analysts, researchers) who wish to obtain access to access to pseudonymised data (both pseudonymisation and anonymisation techniques will be applied to the pseudonymised dataset) will need to be reviewed by London-level recommending bodies and approved by Integrated Care Systems-level Data Access Committees before they are granted access, subject to strict requirements including completion of Data Access Request Form and Acceptable Use Policy.

- **Safe Projects** - There will not be blanket approval or extraction of data for any Interoperability Project in the SDE. The Data Controllers, independently or jointly, will instruct the Data Processor and carry out necessary due diligence and assurance process before any such transfer of data takes place. As above, in the SDE, users wishing to access pseudonymised datasets will be granted access to data required for their project subject to approval by the relevant bodies.



FAQs

Integrity and Confidentiality (Security)

- **Safe Settings** - The Data Processors will comply with key cyber-security standards set by the National Cyber Security Centre UK.

- **Safe Data** - After the point of data ingestion into SDE for the purposes of the OneLondon SDE, data will be standardised, restructred, cleansed and validated to avoid inconsistencies in the data that would otherwise arise.

- **Safe Outputs** - At the point of extraction from SDE, Data Controllers, independently or jointly, will instruct the Data Processor and carry out necessary due diligence and assurance before any such transfer of data takes place e.g. to other NHS SDEs. For the purposes of research, no data will be extracted unless it is anonymised aggregate data.

- **Safe Return** - Exclusively, in the context of population health management programmes that involve carrying out risk stratification for case finding purposes, the Data Processor for the SDE will re-identify the patients categorised as 'at risk' and make available only to corresponding GP practices. For this purpose, no data will be extracted instead, this information will be provided via purposefully built dashboards that allow the re-identification of these patients.



FAQs

Integrity and Confidentiality (Security)

48. Will the data only be processed within the UK?

Yes. The OneLondon SDE will be comprised of two complementary infrastructures, namely, the London Data Service hosted by North East London Integrated Care Board (NEL ICB) and the London Analytics Platform hosted by North West London Integrated Care Board (NWL ICB). The data processed for the purpose of the OneLondon SDE will be processed by the respective ICBs hosting the infrastructures. In doing so, they will utilise Microsoft Azure and Snowflake, cloud data storage and warehouse service providers, and store all patient-level identifiable and pseudonymised data in the UK South datacentre region.

49. Who are the processors and sub-processors involved in the London Data Service?

The North East London ICB (NEL ICB) will carry out the role of a Data Processor for the purpose of the London Data Service (LDS) and will discharge its role through the work of Intelligence Solutions for London (ISL) team which is hosted by North East London Integrated Care Board (NEL ICB).



FAQs

Integrity and Confidentiality (Security)

By being sub-contracted by the Data Processor, on behalf of the Data Controllers, multiple Sub-Processors will be used to deliver the LDS:

- **Microsoft** will act as a Sub-Processor and provide Azure cloud-based data storage solution.
- **Snowflake** will act as a Sub-Processor and provide SaaS-Built Data Warehousing and analytics service.
- **Zendesk** will act as a Sub-Processor and provide support desk system for service provision and incident mnagement. Interworks will act as a Sub-Processor and provide project management technical advisory and data engineering services.
- **Answer Digital Limited** will act as a Sub-Processor and provide technical advisory, data engineering, analytical and project management services.



FAQs

Integrity and Confidentiality (Security)

50. Who are the processors and sub-processors involved in the London Analytics platform?

The North West London Integrated Care Board (NWL ICB) will carry out the role of a Data Processor for the purpose of the London Analytics Platform (LAP). By being sub-contracted by the Data Processor, on behalf of the Data Controllers, multiple Sub-Processors will be used to deliver the LAP.

- **Imperial College Healthcare NHS Trust (ICHT)** will act as a Sub-Processor and provide the infrastructure and secure environment within which the LAP will operate.
- **Microsoft** will act as a Sub-Processor and provide Azure cloud-based data storage solution.
- **Snowflake** will act as a Sub-Processor and provide SaaS-built data warehousing, data management and analytics service.
- **Accenture** will be sub-contracted by ICHT and act as a Sub-Processor to support the managed service provision and help development of capabilities and row-level security.



FAQs

Integrity and Confidentiality (Security)

51. Is the London Data Service part of the Federated Data platform?

This is a joint data controller environment. Data only flows on explicit documented instructions from data controllers. Data will not flow into the FDP unless data controllers give us a specific direction to do this.

52. What is a Section 251/s251?

This is a shorthand term and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002 (Section 251).

Section 251 was established because it was recognised that the NHS's essential activities and important medical research required the use of patient-identifiable information where anonymised information was not possible and obtaining consent was not practical.



FAQs

Integrity and Confidentiality (Security)

Section 251 allows the Common Law Duty of Confidentiality to be lifted temporarily to enable the use and disclosure of Patient Identifiable Information for medical purposes without breaching the principles of confidentiality. The Confidentiality Advisory Group (CAG) reviews research and non-research applications under Section 251 and advises under the framework of Regulations 2002 whether there is sufficient public interest to temporarily lift the common law duty of confidentiality in the context of the application made.

53. Is there a s251 for the OneLondon SDE?

The trust and confidence between a patient and clinician is central to any health and care programme involving data. Our programme has been designed to maximise patient confidentiality: traditional approaches to data sharing disseminate data to users, but in this programme approved users come to the data and access it in a controlled environment.

We conducted several extensive public deliberations with Londoners, who told us they expect the London SDE to provide data for direct care and other secondary purposes (such as planning and research) to improve the delivery of their care.



FAQs

Integrity and Confidentiality (Security)

These deliberations have been commended nationally as examples of best practice. As a result of this we have undertaken two key approaches to the design of the SDE:

- A 'Data Protection by Design and Default' approach whereby patient identifiable information will be pseudonymised as soon as practicable, and all core-processing will take place on pseudonymised data.

- All use of data within the London SDE will be for public interest purposes. This includes supporting the provision of direct care, based on implied consent of the patient, and using pseudonymised data for the provision of proactive health and care (population health management), and to interrogate the data for commissioning, assessing and improving of health and care, and research. Data Controllers, through their local Data Access Committees, will assess each application. Only those projects which serve the public interest will be approved.

We have engaged widely to test and refine our proposals.

This includes independent legal advisors and a leading King's Counsel.



FAQs

Integrity and Confidentiality (Security)

It also involved detailed discussion with the National Data Guardian, the Information Commissioner's Office, NHS England, the Confidentiality Advisory Group (CAG), the Londonwide Local Medical Committee, and the BMA. Through this extensive engagement, we have been able to finalise our approach.

We have applied for and received support under Section 251 of the National Health Service Act 2006 and the Health Service (Control of Patient Information) Regulations 2002.

Although our approach is based on privacy by design, s251 directions will allow us to eliminate the risk of breaching confidentiality when pseudonymised datasets are used for secondary purposes. This approach aligns London with the other SDE programmes across the country.

- CAG Reference for research is 24/CAG/0155
- CAG Reference for non-research is 24/CAG0156

The CAG registers for research and non-research projects can be found **here**.



FAQs

Integrity and Confidentiality (Security)

54. There will be a lot of valuable data in one place, how do I know that this will be safe?

Data processed and stored for the purposes of the OneLondon SDE will be protected by a combination of robust technical and organisational measures, in line with the Six Safes Framework.

Safe People - Only members of staff that have completed all Information Governance training, and who have necessary credentials and authorisation will have access to patient-level data on a need-to-know basis. There will be auditing capabilities to prevent abuse of authorised access by the Data Processors. For the purposes of the SDE, identifiable data will be made available only through dashboard visualisation technology to healthcare professionals with legitimate relationship with the patients. Users (e.g. analysts, researchers) who wish to obtain access to access to pseudonymised data (both pseudonymisation and anonymisation techniques will be applied to the pseudonymised dataset) will need to be reviewed by London-level recommending bodies and approved by Integrated Care Systems-level data access committees before they are granted access, subject to strict requirements including completion of Data Access Request Form and Acceptable Use Policy.



FAQs

Integrity and Confidentiality (Security)

Safe Projects - There will not be blanket approval or extraction of data for any Interoperability Project in the SDE. The Data Controllers, independently or jointly, will instruct the Data Processor and carry out necessary due diligence and assurance process before any such transfer of data takes place. As above, in the SDE, users wishing to access pseudonymised datasets will be granted access to data required for their project subject to approval by the relevant bodies.

Safe Settings - The Data Processors will comply with key cyber-security standards set by the National Cyber Security Centre UK.

Safe Data - After the point of data ingestion into SDE for the purposes of the OneLondon SDE, data will be standardised, restructred, cleansed and validated to avoid inconsistencies in the data that would otherwise arise.

Safe Outputs - At the point of extraction from SDE, Data Controllers, independently or jointly, will instruct the Data Processor and carry out necessary due diligence and assurance before any such transfer of data takes place, e.g., to other NHS SDEs. For the purposes of research, no data will be extracted unless it is anonymised aggregate data.



FAQs

Integrity and Confidentiality (Security)

Safe Return: Exclusively, in the context of population health management programmes that involve carrying out risk stratification for case-finding purposes, the Data Processor for the SDE will re-identify the patients categorised as 'at risk' and make available only to corresponding GP practice. For this purpose, no data will be extracted instead, this information will be provided via purposefully built dashboards that allow the re-identification of these patients.

55. What safeguards are in place to protect the data from unauthorised access?

We comply with the six safes framework.

This consists of:

- **Safe Data** - Data is collated, cleansed, checked and pseudonymised - this is where any identifiable personal information such as names are replaced with artificial information.

- **Safe Research** - All research is pre-approved to ensure they are of benefit to health and social research.



FAQs

Integrity and Confidentiality (Security)

- **Safe People** - Users of the SDE are vetted.

- **Safe Settings** - People can only gain access to the SDE once they have been approved and been through an induction process; it is cloud-based, data is encrypted on rest and processing, and access via VDI.

- **Safe Outputs** - There are strict rules on what can be removed from the SDE.

- **Safe Return** - Any members of the public whose data has been used for research can benefit from the learnings sooner rather than later.

56. What safeguards are in place to protect the data from cyber-attacks?

The Data Processors and Sub-Processors for the OneLondon SDE are accredited and conform to cyber security standards endorsed by the National Cyber Security Centre UK. In addition to this, there will be independent audits and regular penetration testing.



FAQs

Integrity and Confidentiality (Security)

North West London Integrated Care Board (NWL ICB) which hosts the London Analytics Platform holds Cyber Essentials Plus Certification and has achieved 2023-2024 Standards Exceed in DSPT submission. North East London Integrated Care Board (NEL ICB) which hosts the London Data Service holds Cyber Essentials Plus Certification and has achieved 2023-2024 Standards Exceed in DSPT submission.

The sub-processor, Microsoft Limited,which they will both utilise as the storage solution, holds ISO 27001 and Cyber Essentials certifications. It has also achieved 2023-2024 Standards Exceeded in DSPT submissions.

The other main sub-processor, Snowflake Computing U.K. holds ISO 27001 and Cyber Essentials Plus certifications. It has also achieved 2023-2024 Standards Exceeded in DSPT submissions.



FAQs

Integrity and Confidentiality (Security)

57. Has there been an independent cyber security assessment completed on the London Data Service and the London Analytics platform?

Yes. As answered in Question 56, the Data Processors and Sub-Processors, processing patient-level data for the OneLondon SDE, conform to cyber security standards by the National Cyber Security Centre UK and implement the National Cyber Security Centre's Cyber Assessment Framework (CAF). Please see the answer to the previous question for further details.

a. Were there any high risks identified that can't be mitigated?

No.

b. Did this include penetration testing of the platforms?

Yes.



FAQs

Integrity and Confidentiality (Security)

c. Will regular penetration testing be undertaken?

Yes, annually. The London Data Service (LDS) carries out penetration testing to ensure it is meeting cyber security standards of the National Cyber Security Centre UK (NCSC). The LDS carried out penetration testing in the early development stage and a second penetration testing is scheduled to be carried out in the next months. Thereafter, penetration testing will be carried out annually.

Similarly, the London Analytics Platform carries out regular penetration testing to ensure it is meeting cyber security standards of NCSC. The most recent penetration testing was completed in August 2024.

58. Is there assurance that the data held in the SDE will not be used to performance manage GPs and their practices?

The data in the SDE will not be used to performance manage GPs and their practices. The data held in SDE will be processed to support range of public interest purposes.



FAQs

Integrity and Confidentiality (Security)

59. My ICB has a sandpit environment. How does data flow from the London Data Service to an ICB sandpit and who controls/authorises this?

The data flow from the LDS to ICB sandpits are not covered under the OneLondon SDE programme and the Section 251 approval obtained.

Therefore, a separate data protection review and data controller sign off is required for the data flow from LDS to ICB sandpits using the OneLondon data sharing framework templates, in line with public expectations.



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



Glossary

Anonymised Data

Data that can no longer be attributed to an identified or identifiable individual.

Commissioning Data Sets

Patient level, secondary use data sets that provide information about NHS-provided and NHS-funded secondary care activity. It re-uses clinical and operational data for purposes other than direct care.

Common Law Duty of Confidentiality

A right developed by the Courts which requires there to be a lawful basis for the use or disclosure of personal information that is held in confidence.

The personal information must have been received under circumstances which warrant a duty of confidence, which will regularly be the case between healthcare providers and their patients.



Glossary

Confidentiality Advisory Group ("CAG")

An independent body created by the Health and Social Care Act 2012 which provides expert advice on the use of patients' confidential data by reviewing requests on behalf of the Health Research Authority and the Secretary of State for Health and Social Care.

Data Access Committee ("DAC") and Data Usage Committee ("DUC")

ICS-level governing bodies that make formal decisions on data access requests. They are the entities that decide whether access to data should be granted for the data sourced from data controllers in their respective areas.

Data Breach

A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It is broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.



Glossary

Data Controller

A person or entity that determines the purpose and means of the use of personal data. This means that they decide why and how personal data is processed. They are the main responsible entity under data protection legislation.

For the OneLondon SDE Programme, all healthcare providers within the London region who sign up to the OneLondon Data Sharing Framework and the local commissioners from the five London ICSs will be acting as independent or joint data controllers, whereby they will independently or jointly determine the purposes and means of the processing.

Data Minimisation

A core data protection principle under the UK GDPR. It requires data controllers to ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.



Glossary

Data Processor

The person or entity that processes the personal data on behalf of the data controller. They follow the instructions of the data controller and do not have their own purpose for processing the personal data.

For the OneLondon SDE Programme, the data processors will be North East London ICB (for the London Data Service) and North West London ICB (for the London Analytics Platform).

Data Protection by Design and Default

Data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of the project at an early stage.

Data protection by default is the implementation of appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.



Glossary

Data Protection Impact Assessment ("DPIA")

A risk assessment. By completing a DPIA, the potential risks of a project or activity are identified, assessed and mitigated. It is a requirement under data protection legislation to complete a DPIA in certain circumstances, namely when the project or activity could result in a high risk to the affected individuals.

Data Protection Officer ("DPO")

In certain circumstances, the UK GDPR requires controllers appoint a Data Protection Officer (DPO). DPOs assist in monitoring internal compliance, informing and advising on data protection obligations and act as a contact point for data subjects and the Information Commissioner.

Data Subject

The identified or identifiable living individual to whom personal data relates.



Glossary

Data Subject Rights

Under the UK GDPR, individuals are granted a number of rights which controllers need to comply with. For example, individuals have the right to be informed, the right of access, the right to be forgotten, and the right to object.

Data Sub-Processor

A third-party service provider that the processor engages to process the personal data of the controller for the controller's purposes.For the OneLondon SDE Programme, NWL ICB's and NEL ICB's engaged third-party service providers are the data sub-processors, such as Microsoft Limited and Snowflake Computing U.K. Limited.

Direct Care

Any clinical activity concerned with the prevention, investigation and treatment of ilness and the alleviation of suffering of individuals. It includes risk stratification in so far it is for case finding purposes which involves health professionals identifying patients who may benefit from targeted interventions for their individual care (as per the National Data Guardian, "Review of Data Security, Consent and Opt-Outs" at 3.2.10)



Glossary

Information Commissioner's Office ("ICO")

The independent regulatory office regarding data protection of the UK.

Information Governance ("IG")

The internal framework that ensures that the entity in question remains compliant with the data protection legislation and ensures good data protection practices across its organisation. This includes policies and training of staff.

Integrated Care Board ("ICB")

NHS organisations that are responsible for planning health services for their local population. There is one ICB in each Integrated Care System area.

Integrated Care Systems ("ICS")

Systems that bring together the health and care organisation in a specific area to deliver joined-up health and care services. Each ICS is responsible for planning health and care services in the area that it covers.



Glossary

Interoperability Projects

An Interoperability Project is a project that involves the ability of different systems implemented by different organisations to communicate with one another and, in doing so, allow for the exchange of personal data, the pooling of personal data or the integrated use of personal data.

King's Counsel's Opinion

Information Governance Services Ltd (a consultancy firm engaged by the OneLondon SDE Programme for their services in data protection), acting on behalf of NHS England-London and the Programme, obtained advice from a King's Counsel about whether the London Data Service and the London Analytics Platform could be said to breach patient's confidentiality or the national policy on opt-outs.

The term *"King's Counsel's Opinion"* is referencing the opinion that was received.



Glossary

London Analytics Platform ("LAP")

The Analytics Platform is one integral part of the OneLondon Secure Data Environment. It consists of two separate databases. The first one contains identifiable patient information and is solely used for direct care purposes. This data will be anonymised and ingested into the second database. The second database is used for secondary purposes such as population health management and health-related research. Researchers will only be able to view the anonymised data and will not be able to identify anyone.

This way, the LAP will be bringing both depth and diversity of healthcare data and expertise in leveraging this data to transform patient outcomes and benefit patient care and create a source of information for researchers whilst maintaining the security of the data and safeguarding patient confidentiality.

London Data Service ("LDS")

London Data Service is one of the complementary infrastructures that sits under the OneLondon SDE which will provide a London-wide solution for standardisation, cleansing, restructuring, pseudonymisation and storage of data, reducing the costs and preventing inconsistencies that would otherwise arise.



Glossary

London Independent Information Access Group ("IIAG")

The IIAG is a governing body of the OneLondon SDE Programme with the London Information Governance Steering Group. They are responsible for overseeing the processing of personal data at a regional level.

They are recommending bodies, meaning that they will undertake a preliminary review of the requests to determine whether they meet the standards set by the framework, assess their substance and merits and make recommendations to the five London Integrated Care System's Data Access Committees who are the bodies making the formal decision about granting access.

London Information Governance Steering Group ("LIGSG")

The LIGSG is a governing body of the OneLondon SDE Programme with the Independent Information Access Group. They are responsible for overseeing the processing of personal data at a regional level.



Glossary

National Data Opt-Out

Introduced by the UK Government to replace "Type 2" Opt-outs and enable patients to opt-out from the use of their data for research or planning purposes. This means that in certain circumstances, patients will be able to let the NHS know that they do not wish their personal data to be used for purposes beyond direct care. As indicated, the National Data Opt-Out does not always apply.

OneLondon Data Sharing Framework ("the Framework")

The OneLondon Data Sharing Framework is a suite of overarching documents that underpins the sharing of personal data carried out between different Members of the Framework. The Framework establishes the framework, specifies its scope and purpose, regulates the membership to the Framework and introduces the governance structure and decision-making process on matters relating to the Framework.

The OneLondon Data Sharing Framework consists of the OneLondon Data Sharing Protocol, the OneLondon Data Sharing Specification, the OneLondon Data Processing Agreement and the OneLondon DataSharing Agreement.



Glossary

Patient Identifiable Information

Any information that relates to an identified or identifiable patient.

Pseudonymised Data

Personal data that has undergone a procedure where direct identifiers are replaced by pseudonyms. A so-called "key" or "look-up table" with the identifiers and the used pseudonyms are kept separately. Without this key, the data that has been processed can no longer be linked to the individual.

Role-Based Access Controls ("RBAC")

Security measures that restrict access to a network/database based on a person's role within an organisation.

SaaS-built Data Warehousing Technology

SaaS means Software as a Service. SaaS allows access to complete user application which the cloud user accesses through a web browser or other software. They can be accessed online via a subscription. A data warehouse centralises and consolidates large amounts of data from multiple sources. They are central repositories of data integrated from different sources.



Glossary

Secure Data Environment (SDE)

Data storage and access platforms which uphold the highest standards of privacy and security.

Six Safes Framework

Office of National Statistics's 'Five Safes Framework' sets principles and best practices for safe governance of data access, and comprises of the following principles; safe data, safe projects, safe setting, safe output.

The standards in the Five Safes Framework has been established as a policy by the Department of Health and Social Care. It has since been developed further by Health Data Research Alliance UK, becoming known as the 'Six Safes Framework', which also includes 'safe return'.

The UK General Data Protection Regulation ("UK GDPR")

The UK GDPR is the EU's General Data Protection Regulation (GDPR) retained in domestic law. It sits alongside an amended version of the DPA 2018.



Glossary

Virtual Desktop Infrastructure ("VDI")

A technology that enables users to access a virtualised desktop environment from any device with an internet connection. They are IT infrastructure that lets users access enterprise computer systems from any device.