

An aerial photograph of London, showing the city skyline with the Shard as a prominent feature. The bottom half of the image is covered by a semi-transparent teal overlay.

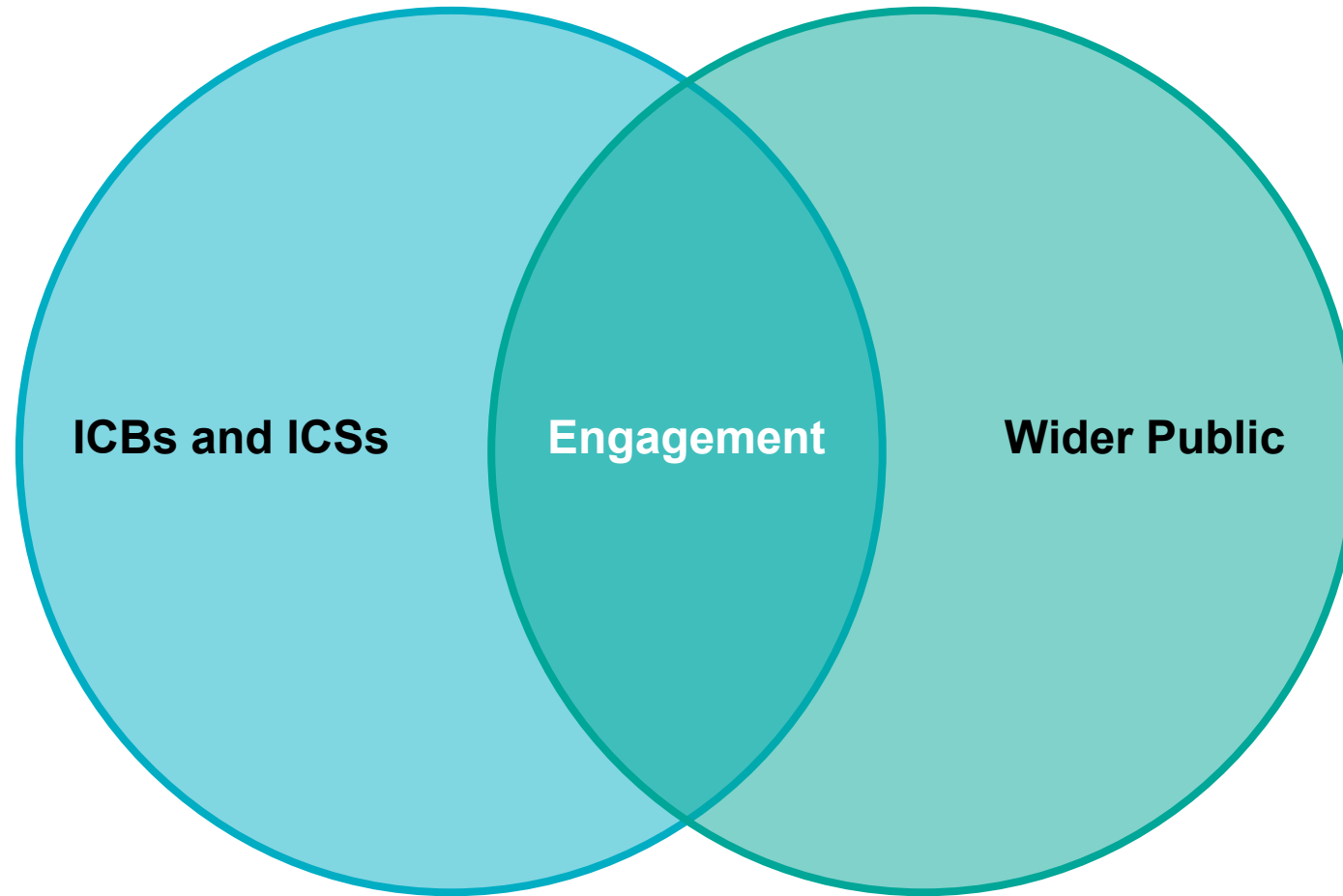
The OneLondon Secure Data Environment (OneLondon SDE)



The SDE has two foundational elements: **London Data Service** (LDS) and London Analytics Platform (LAP).

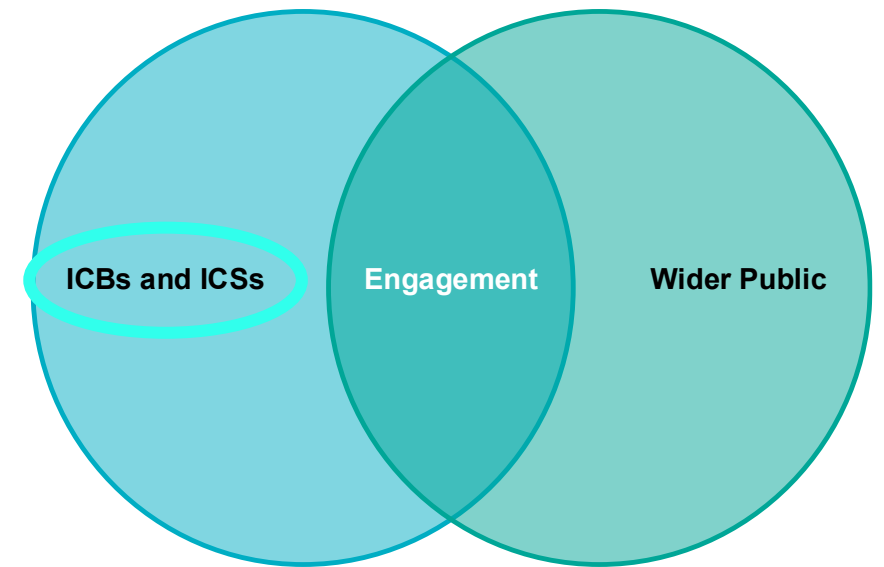
The LDS and Analytics Platform can perform a range of uses, including:

- direct care;
- system planning;
- population health management;
- and research and development



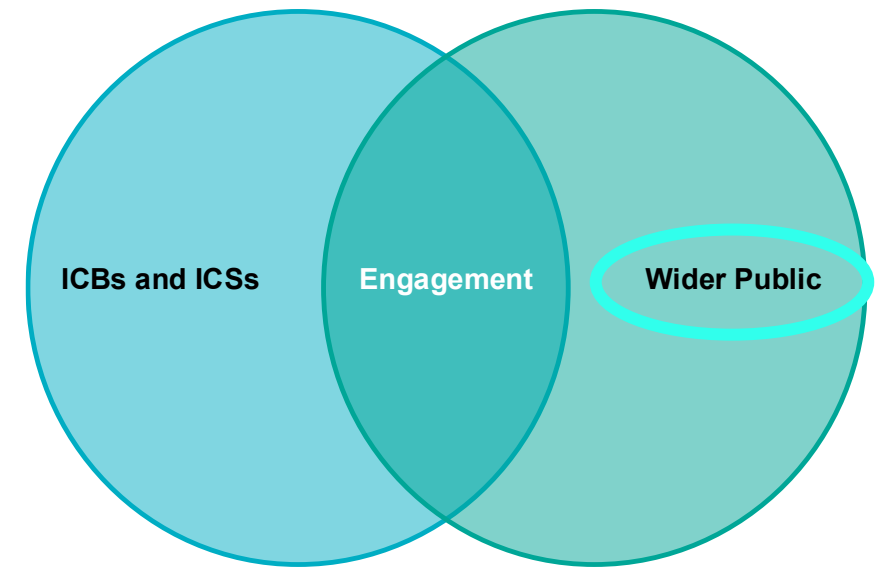
ICBs and ICSs

- We have conducted various conversations over several years with ICBs about the best way in which London manages and curates data to be used for multiple use cases including patient care, operational management, service management, and research.
- Furthermore, Information Governance Leads from each of the four London ICSs, representing nearly 1.5k NHS organisations acting as data controllers, have been collaborating for the development of the SDE Programme.



Wider Public

- The public have been engaged through the Conversation with Londoners – the world's largest public deliberation on the use of health and care data.
- The public recommendations agreed at this Citizens' Summit provided a clear instruction from the public for how data should be used and are now being used to shape policy for London (<https://www.onelondon.online/get-involved/>).





Patient Benefit



GP/Practice Benefit

Patients

- Patients will 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.
- Their de-identified 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.



Patient Benefit

GP/Practices

- The OneLondon SDE 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.



GP/Practice Benefit

- As it is widely known, the London region is comprised of four Integrated Care Systems (ICSs)
- All four London ICSs already have **Data Sharing Frameworks** in place to support the sharing of data amongst the health and care organisations operating within their corresponding geographic areas.
- Whilst these frameworks have been quite effective in supporting **intra-ICS** data sharing, they have somewhat struggled to equally support **inter-ICS** initiatives that extend beyond their corresponding geographical boundaries and affect the London region more widely.



London Region

- It became necessary to integrate the London region and allow for the sharing of data between the health and care organisations across the four London ICSs, without prejudice to the important work that will continue to take place at ICS-level.
- The **OneLondon Data Sharing Framework** was agreed amongst the health and care organisations in London as a means to enable programmes of work that require the sharing of data at regional level.





OneLondon Data Sharing Framework

The OneLondon Data Sharing Framework will underpin the sharing of Personal Data that concurrently is:

- necessary to support **Interoperability Projects**, including those involving:
 - the exchange of Personal Data;
 - the pooling of Personal Data;
 - the integrated use of Personal Data;
- undertaken in the **public interest** for purposes that include:
 - supporting the direct provision of health and social care;
 - planning and commissioning of health and social care services;
 - assessing health and social care services;
 - improving health and social care services;
 - enabling research;
- carried out between different **Members from two or more of the London ICSs.**

OneLondon Data Sharing Protocol (ODSP)

OneLondon Data Sharing Specification (ODSS)

**OneLondon Data Sharing Agreement
(DSA)**

**OneLondon Data Processing
Agreement (DPA)**

OneLondon Data Sharing Protocol (ODSP)

- The OneLondon Data Sharing Protocol (ODSP) establishes the OneLondon Data Sharing Framework for the sharing of Personal Data between its Members in support of Interoperability Projects carried out in the public interest.
- It also sets out the general principles, standards and procedures that each Member shall adhere to and the responsibilities that each Member owes to other Members in respect of the shared Personal Data.

OneLondon Data Sharing Protocol (ODSP)

OneLondon Data Sharing Specification (ODSS)

OneLondon Data Sharing Agreement (DSA)

OneLondon Data Processing Agreement (DPA)

OneLondon Data Sharing Specification (ODSS)

- Each individual OneLondon Data Sharing Specification (ODSS) defines the specificities of each Interoperability Project that requires the sharing of Personal Data between two or more Members.
- This includes the data which will be processed, the purposes, the legal basis, the sharing type and the conditions under which the Project will be executed.

OneLondon Data Sharing Protocol
(ODSP)

**OneLondon Data Sharing
Specification (ODSS)**

OneLondon Data
Sharing Agreement
(DSA)

OneLondon Data
Processing
Agreement (DPA)

Depending on the specificities of each project:

- **OneLondon Data Processing Agreement (ODPA)**: used where a Member or a third-party organisation processes data on behalf of and under strict instructions from Members who are party to the ODSS;
- **OneLondon Data Sharing Agreement (ODSA)**: used where a third-party organisation, alone or jointly with Members, determines the purpose and means of the processing of data relevant to an ODSS.

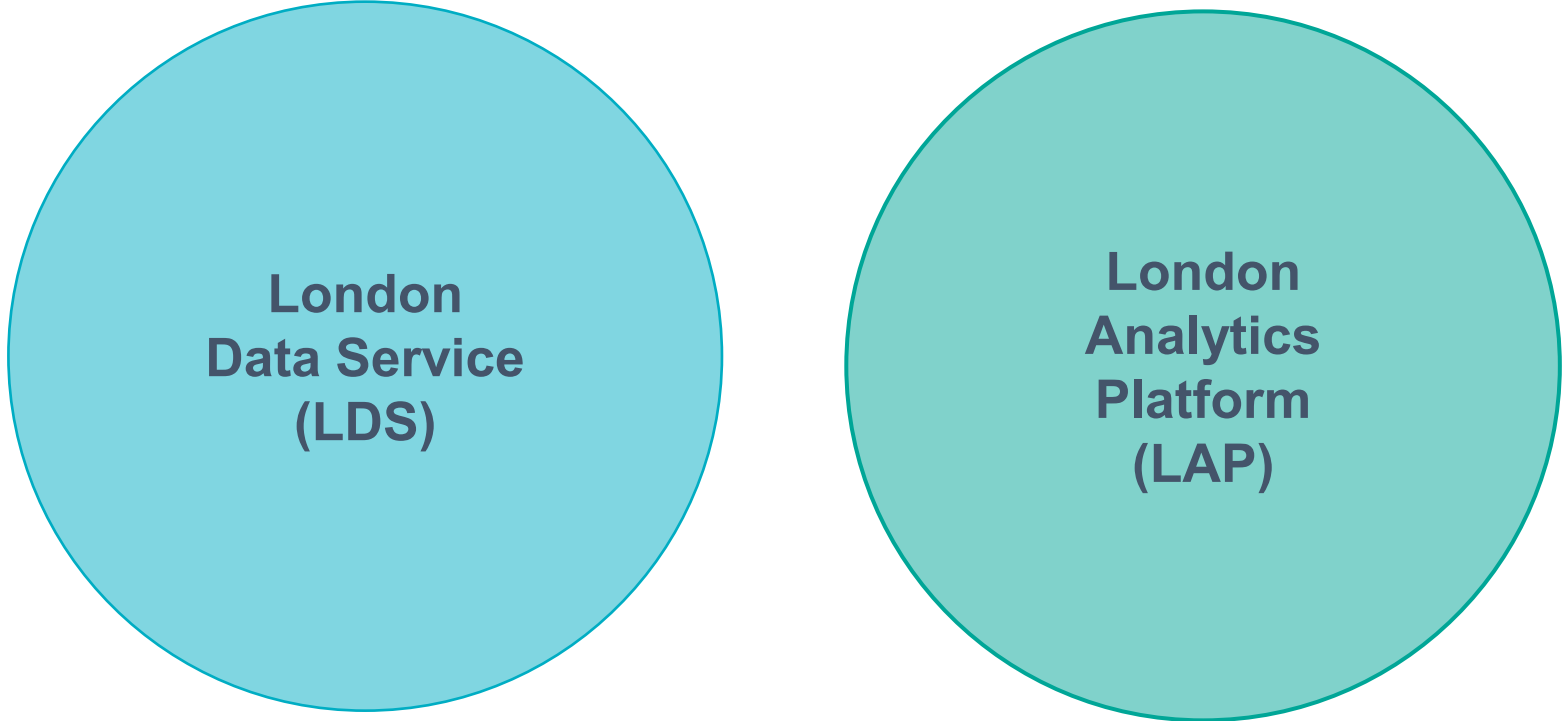
OneLondon Data Sharing Protocol
(ODSP)

OneLondon Data Sharing
Specification (ODSS)

OneLondon Data
Sharing Agreement
(DSA)

OneLondon Data
Processing
Agreement (DPA)

Once implemented, the OneLondon Data Sharing Framework will be used to support, amongst many others, the following data sharing initiatives:

The diagram consists of two large, light blue circles positioned side-by-side. The left circle contains the text 'London Data Service (LDS)' and the right circle contains the text 'London Analytics Platform (LAP)'. At the bottom of the slide, there are several thin, light blue lines that sweep upwards from left to right, creating a sense of motion or a base for the content above.

**London
Data Service
(LDS)**

**London
Analytics
Platform
(LAP)**



London Data Service (LDS)



The London Data Service (LDS) is a service that **North East London Integrated Care Board (NEL ICB)** will provide for health care organisations across the London region.

These health and care organisations will act as **data controllers** under data protection law.

NEL ICB will carry out the role of **data processor** under the same law, processing data on behalf of and under instructions from the controllers.



At the point of ingestion, identifiable data will be processed for NHS number tracing and validation, for the purpose of application of National Data Opt-Outs and geographical data derivation.

Then, identifiable data will be **pseudonymised**, at the earliest opportunity, in line with data protection by design and default approach.

In other words, identifiable data will be processed to generate two outputs:

- a pseudonymised dataset that identifies patients only through the use of a pseudonym;
- a look-up table that links the pseudonyms to the personal identifiers.

The two outputs will be held separately under appropriate technical and organisational measures. The pseudonymised data is only re-identified when there is a specific use-case.



Once pseudonymised, the data will be **cleansed**.

This means that the data will be processed with the aim of fixing incorrect, incomplete, duplicate or otherwise erroneous data within the extracted datasets.



After that, the data will be **mapped and standardised**.

This involves processing the data in a way that converts it into one common data format (e.g. Observational Medical Outcomes Partnership (“OMOP”) common data model).

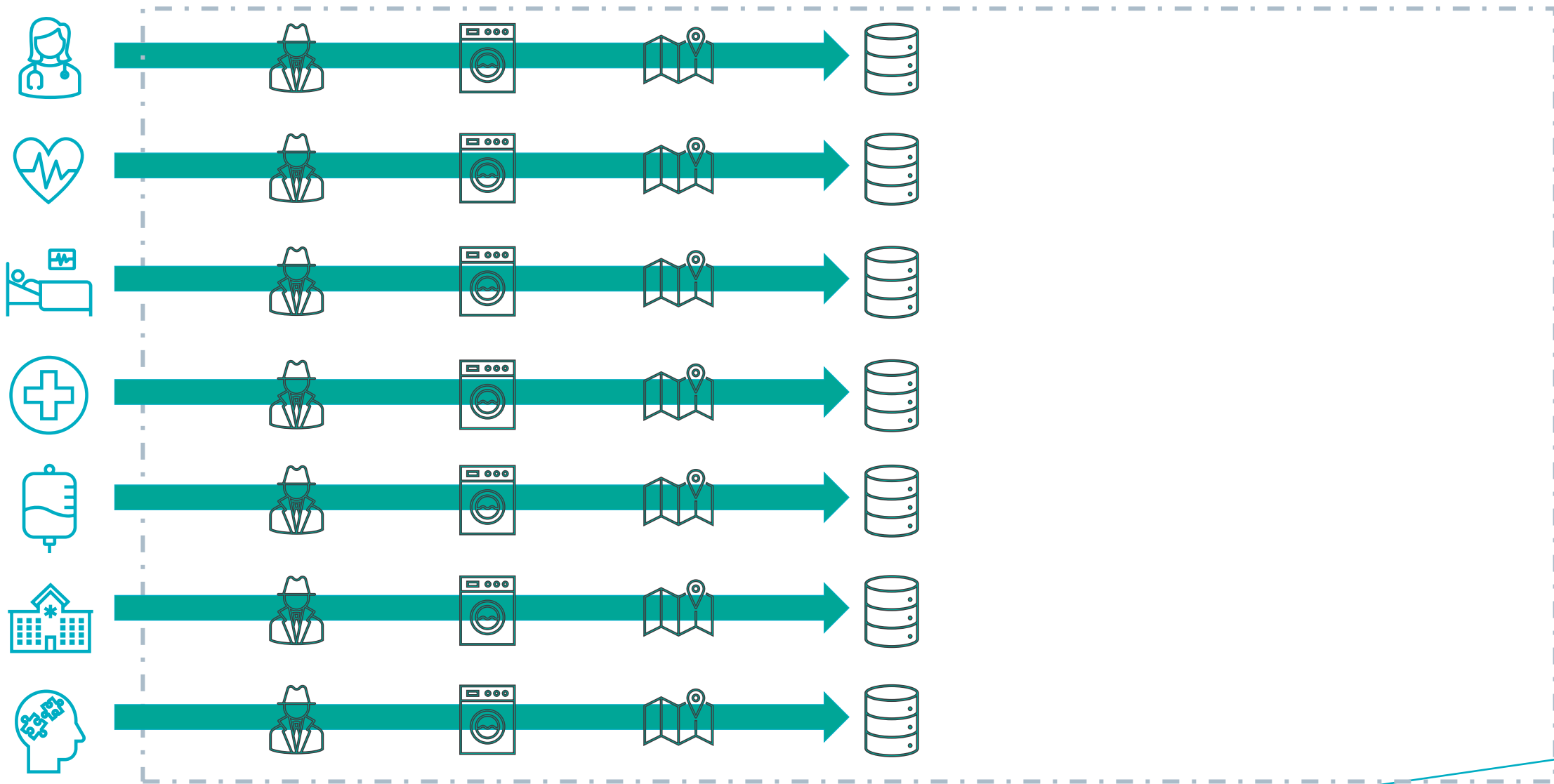


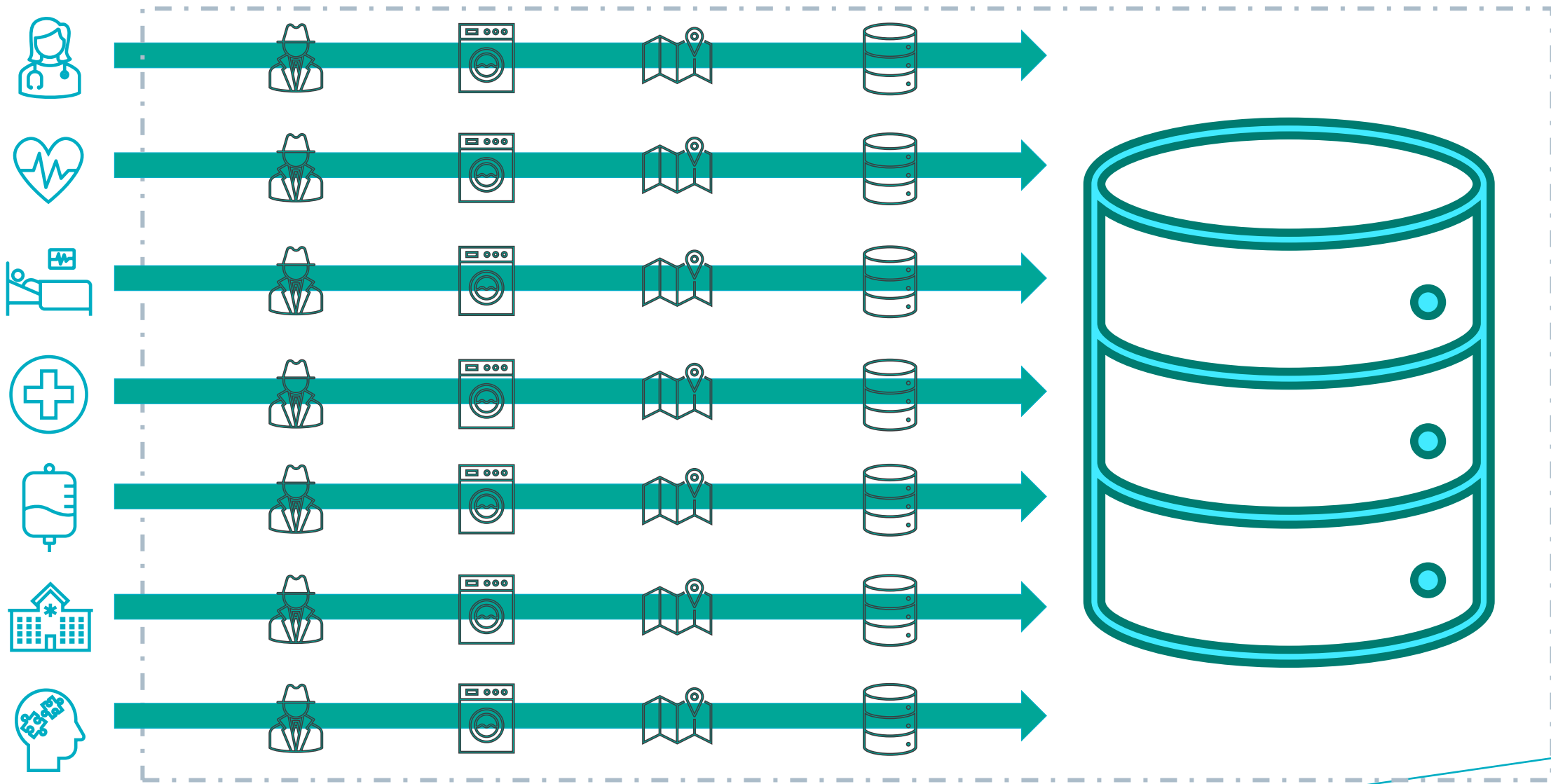
The pseudonymised, cleansed, standardised data will be **securely stored** and made available to the corresponding NHS organisation using the service.

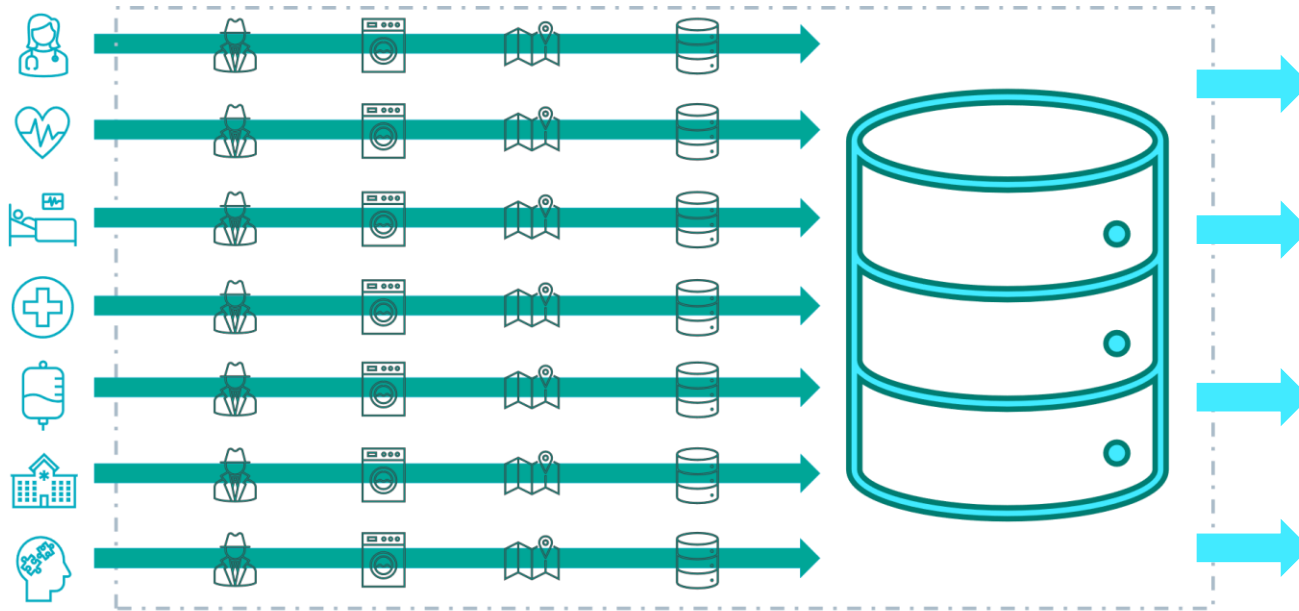
As sole data controller, the NHS organisation may instruct NEL ICB to:

- **re-identify** the pseudonymised, cleansed, standardised data, as required;
- **transfer** the cleansed, standardised data, whether in pseudonymised or identifiable form, back to the them or to a third-party;

It will be the responsibility of the data controller to carry out the necessary due diligence before any such transfers of data take place, ascertaining whether additional technical and organisational measures need to be put in place to ensure the security of the data and protect patients' confidentiality.







Under a **joint controllership agreement**, data held by the different health and care organisations will be linked together, stored and as instructed by them, extracted by NEL ICB, whether in identifiable or pseudonymised form, for public interest purposes that include:

- supporting the provision of direct care;
- planning and commissioning of services;
- assessing and improving services;
- enabling research.

Any such transfer, however, will need to be approved by the joint data controllers via participation in the governing bodies established under the joint controllership agreement.

At that point, the NHS organisations will need to ascertain whether additional technical and organisational measures need to be put in place to ensure the security of the data and protect patients' confidentiality.

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

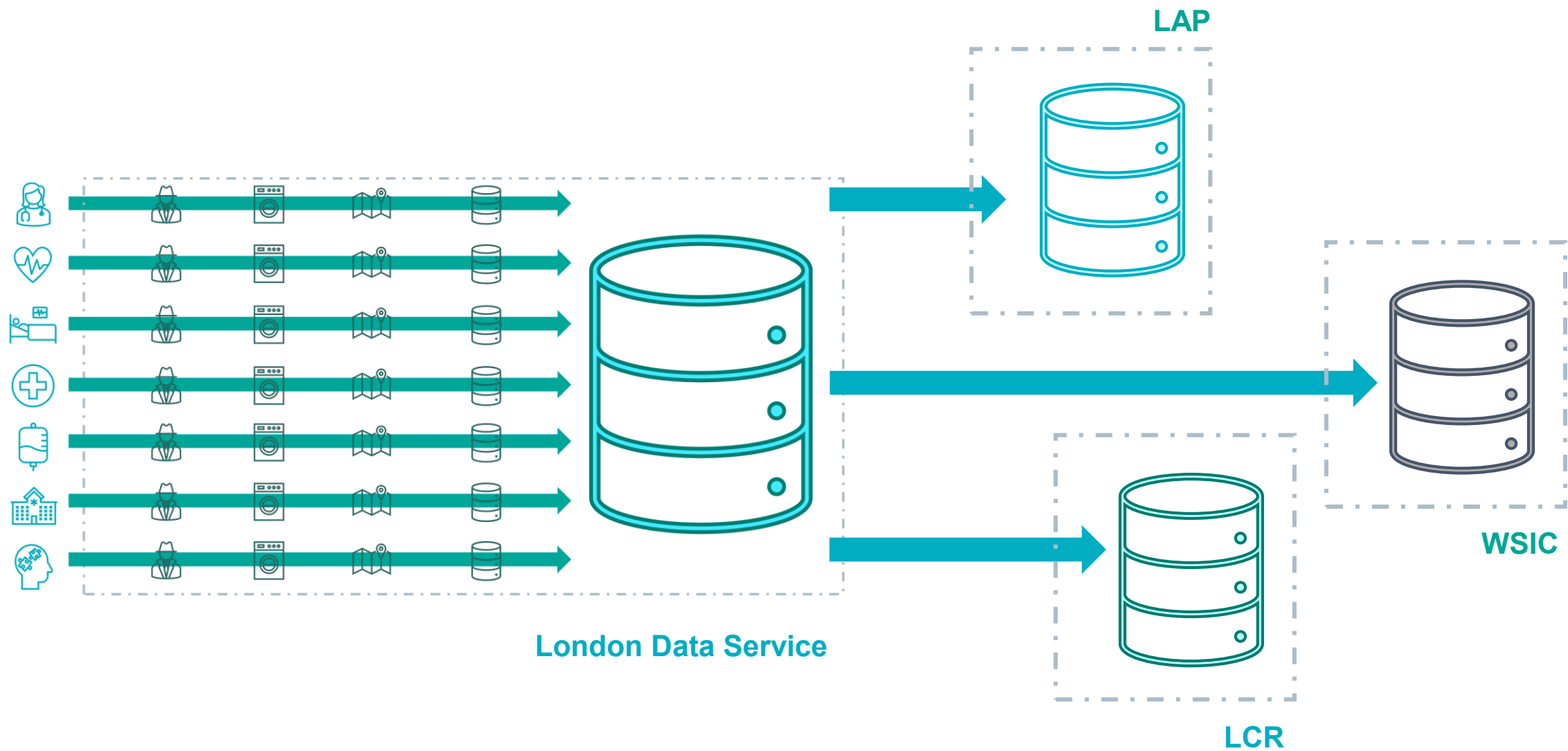
9(2)(j) necessary for archiving purposes in the public interest, scientific or historical purposes

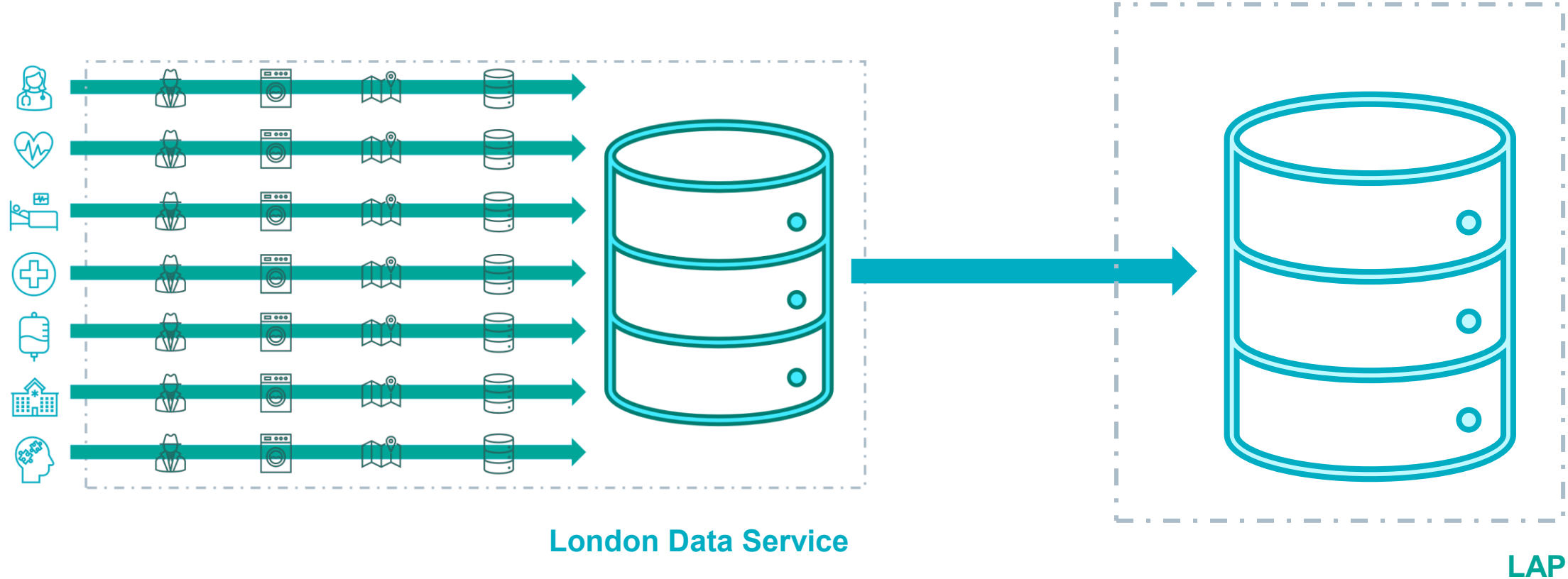


Direct Care Programmes

It is envisaged that data initially processed under the LDS will be further processed to underpin a wide array of programmes, at both regional and ICS levels, conceived to support the provision of direct care to patients by healthcare organisations in London. Notable examples include:

- **London Care Record (LCR)**: shared care record in operation for many years which enables healthcare professionals, under strict access controls, to securely view the records relating to their patients that are held by other healthcare providers across the region;
- **Care Information Exchange (CIE)**: portal that allows patients to access their consolidated health record from anywhere in the world, contribute to the formation of these records, and share them with other institutions, professionals, family members or carer;
- **Whole Systems Integrated Care (WSIC)**: integrated record created via the pooling of data from different healthcare providers which allows clinicians to obtain a holistic overview of a patient's healthcare record across the whole pathway and provides dashboards which can be used for case finding and management of patients who require more targeted and proactive care;
- **OneLondon SDE Programme**: creating a patient-level linkable longitudinal record to support the creation of a research database that will support research and other secondary care purposes including planning, risk stratification and commissioning. Additionally, identifiable patient-level data will be used to support the delivery of direct care.







London Analytics Platform (LAP)



The London Analytics Platform is a service that **West and North London Integrated Care Board (NWL ICB)** will provide for health and care organisations across the London region.

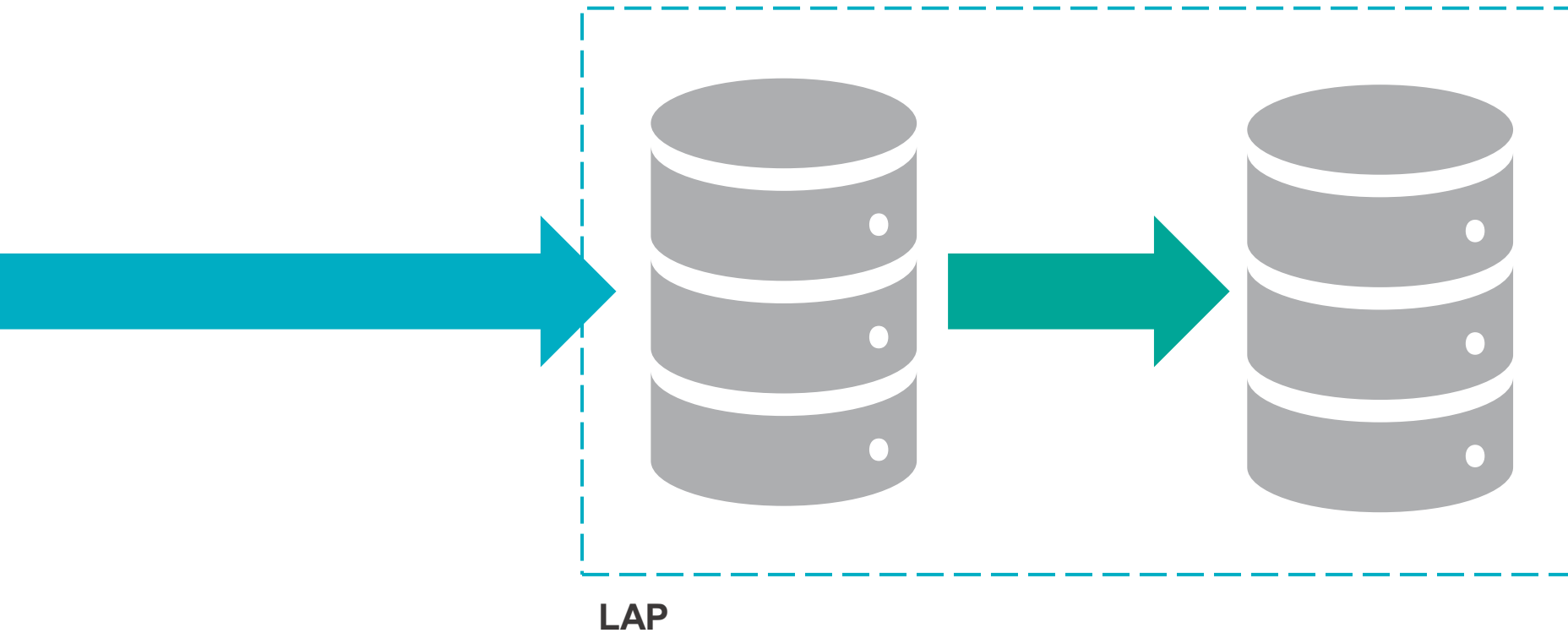
These health and care organisations will act as **data controllers** under data protection law.

In turn, W&NL ICB will carry out the role of **data processor** under the same law, processing data on behalf of and under instructions from the controllers.

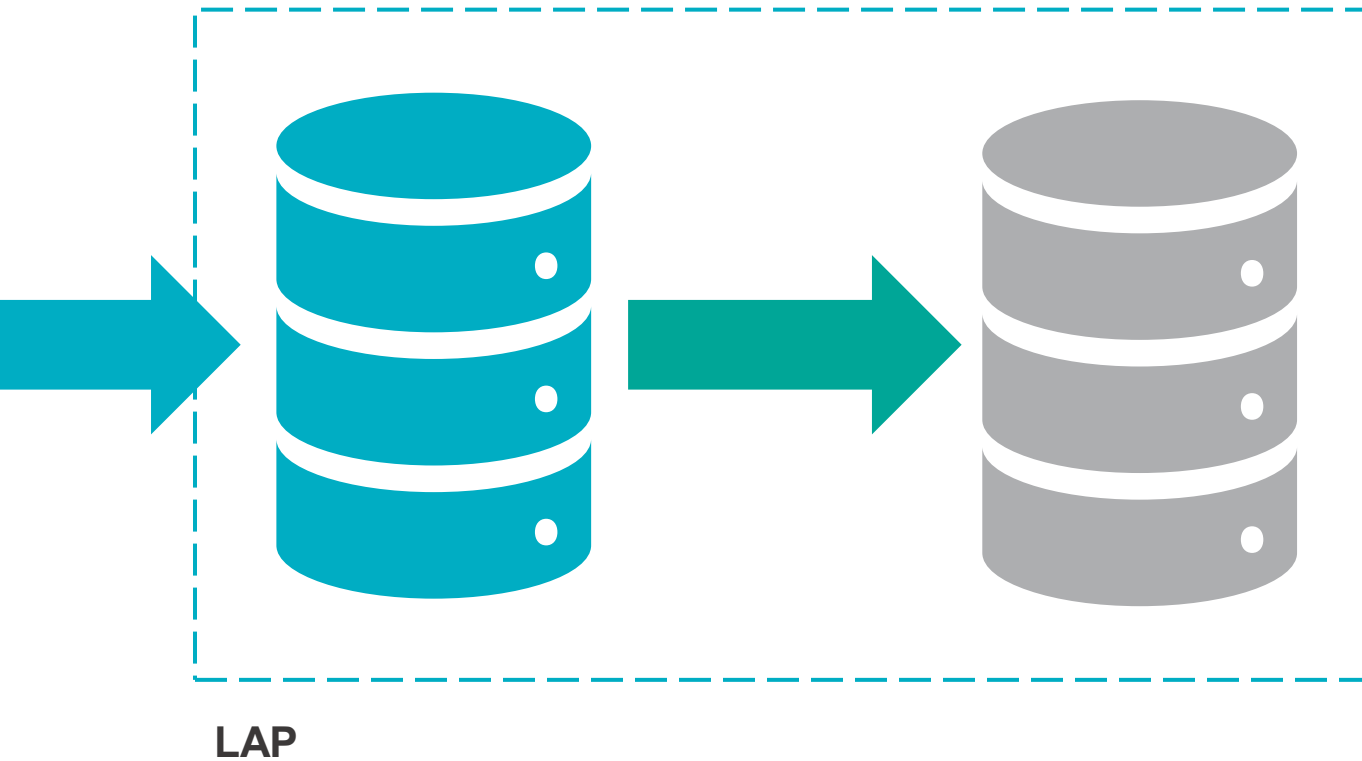
The creation of the London Analytics Platform will require the ingestion of data obtained from the different health and care organisations across the region via the London Data Service (LDS).



In the model which we currently seek to implement in London, the secure environment would be comprised of **two separate databases** held by W&NL ICB on behalf of the data controllers.



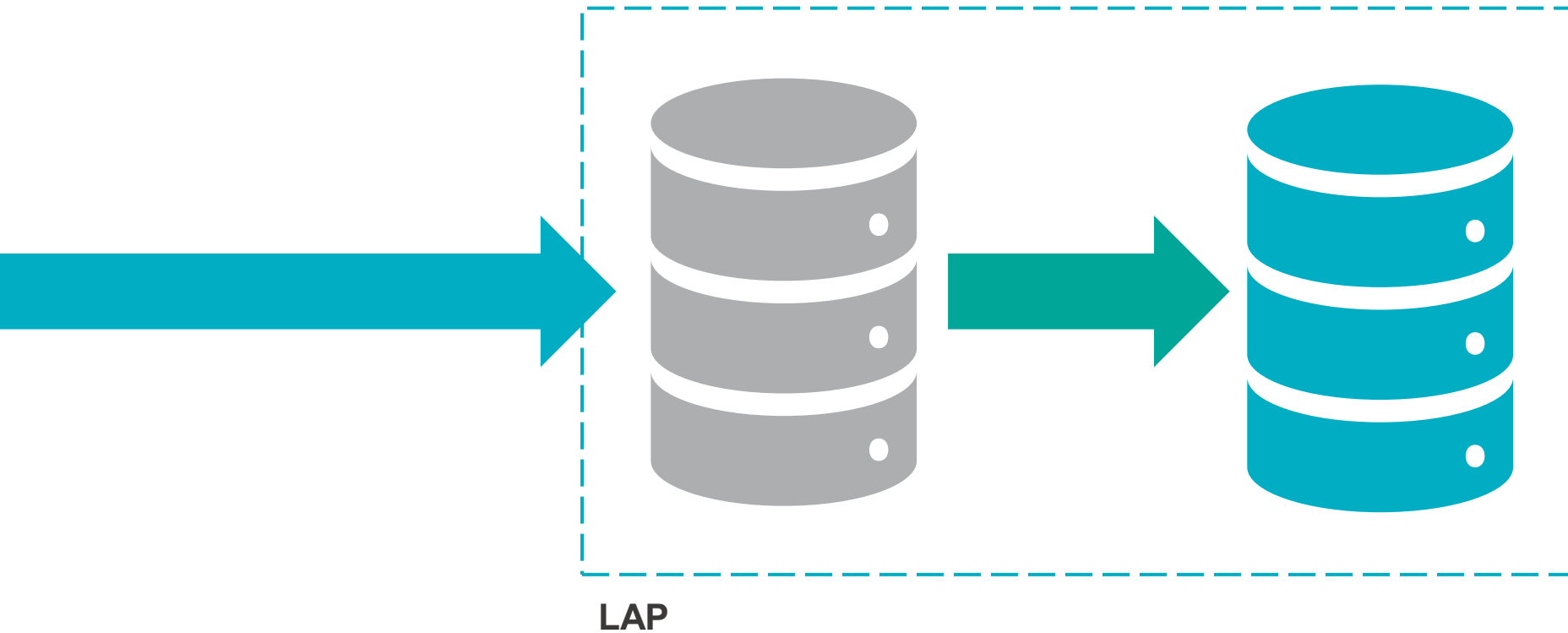
Under a joint controllership model, the first database will receive **identifiable information** from the LDS and will be used for the purpose of **providing direct care to patients**.



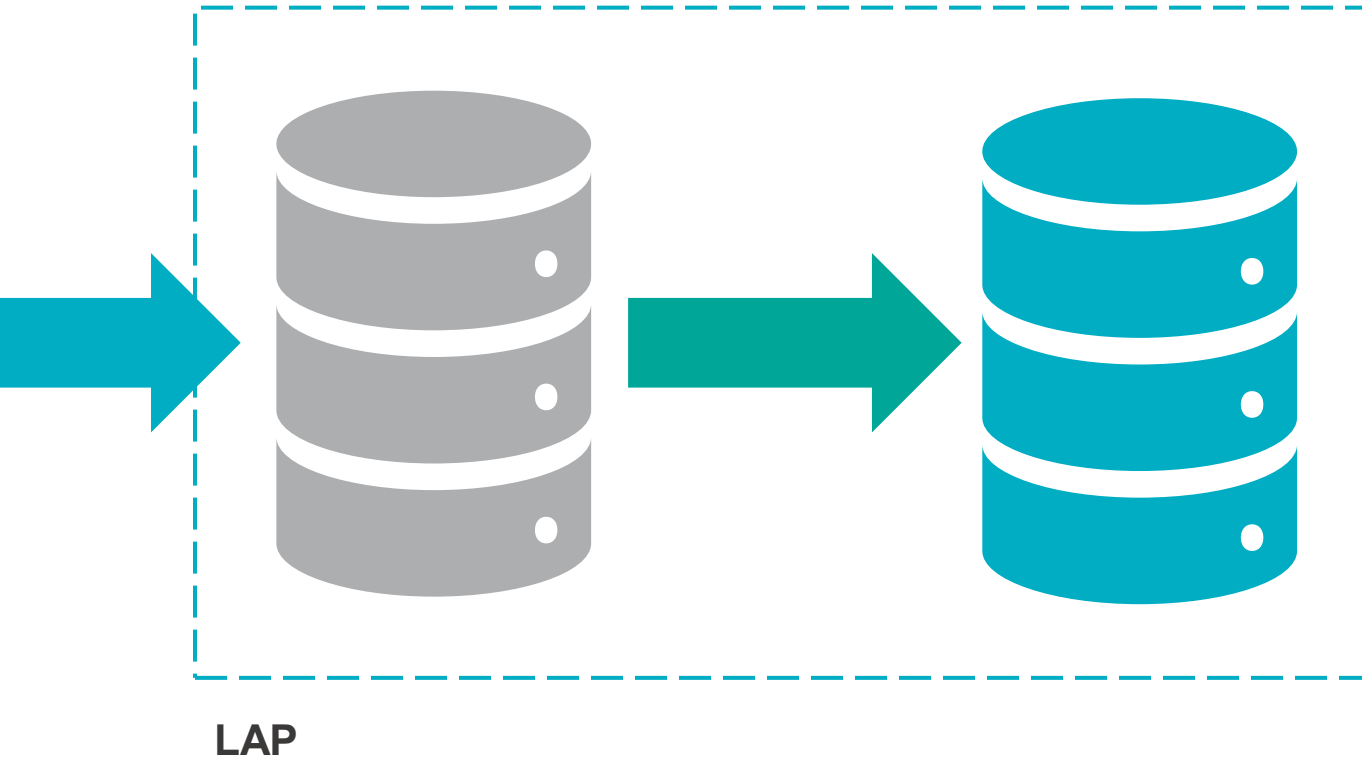
The database will consist of an integrated record created via the pooling of data from different healthcare providers.

The aim is to allow clinicians to obtain a holistic view of a patient's healthcare record across the whole pathway, by providing dashboards which can be used for case finding and management of patients who require more targeted and proactive care.

Identifiable data contained in the first database will be **pseudonymised** and made available to Users (e.g., analysts, researchers etc.) for purposes beyond the provision of direct care to patients.



Identifiable data contained in the first database will be **pseudonymised** and made available to Users (e.g., analysts, researchers etc.) for purposes beyond the provision of direct care to patients, including:

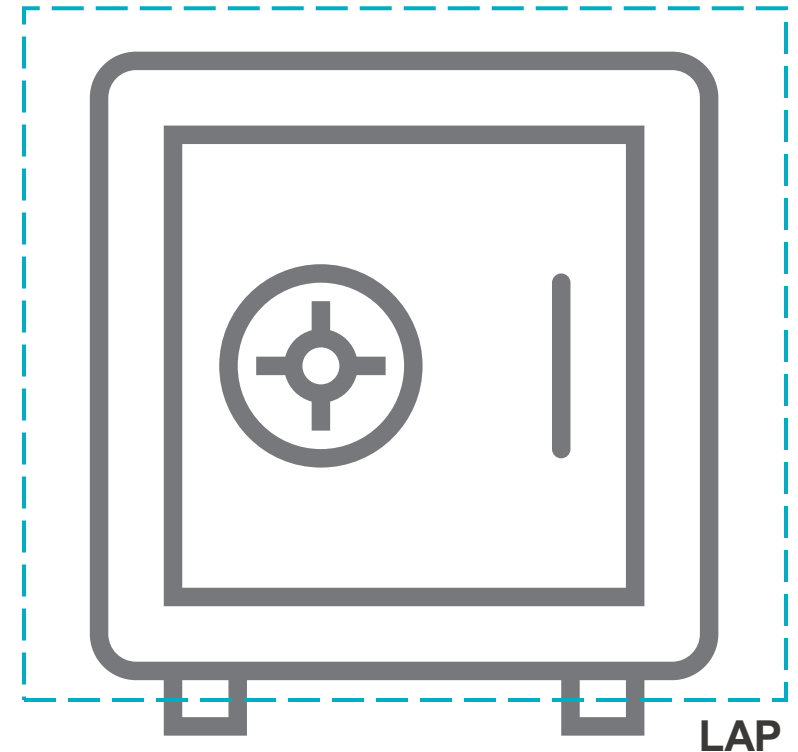


- health related research;
- population health management (proactive care);
- planning and commissioning of services;
- assessing and improving services.

Data will be stored in a secure environment compliant with the 6 Safes Framework, a set of principles and best practices established and recommended by the Office of National Statistics (ONS), the 'Goldacre Review' and the Health Data Research UK (HDRUK) and mandated by the DHSC policy.

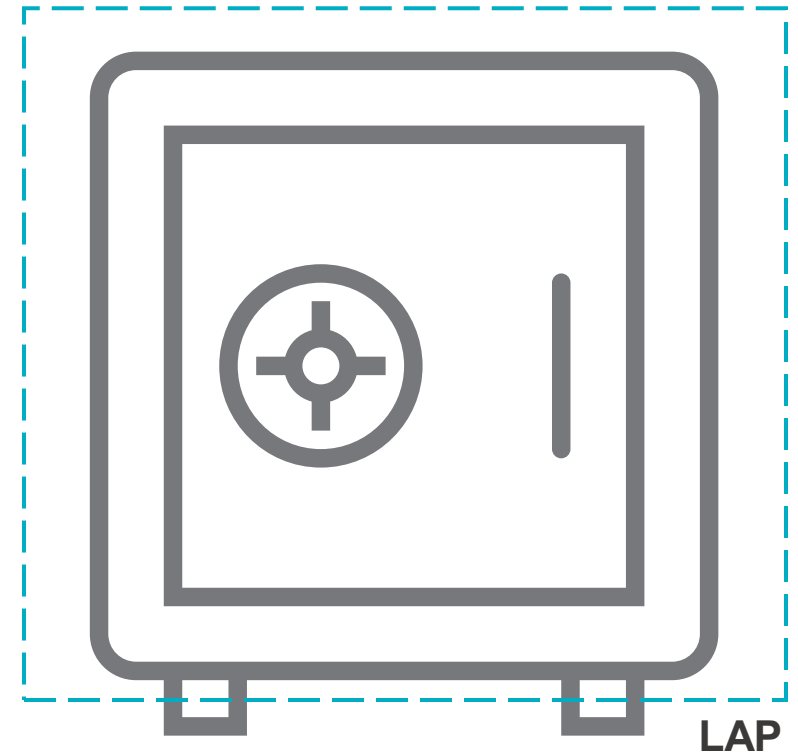


- Users who wish to obtain access to the environment to carry out their projects will need to complete a **Data Access Request form**.
- The form will capture project-specific information, including the purpose of the project, the data required for its completion, the names and affiliations of those undertaking the data analysis, the expected duration of access etc.





- Each User will be required to sign the **Acceptable Use Policy**, undertaking to a set of contractual obligations around access to the data within the secure environment.
- Similar obligations will be placed on the organisation that employs the lead User, via the **Data Access Contract**.

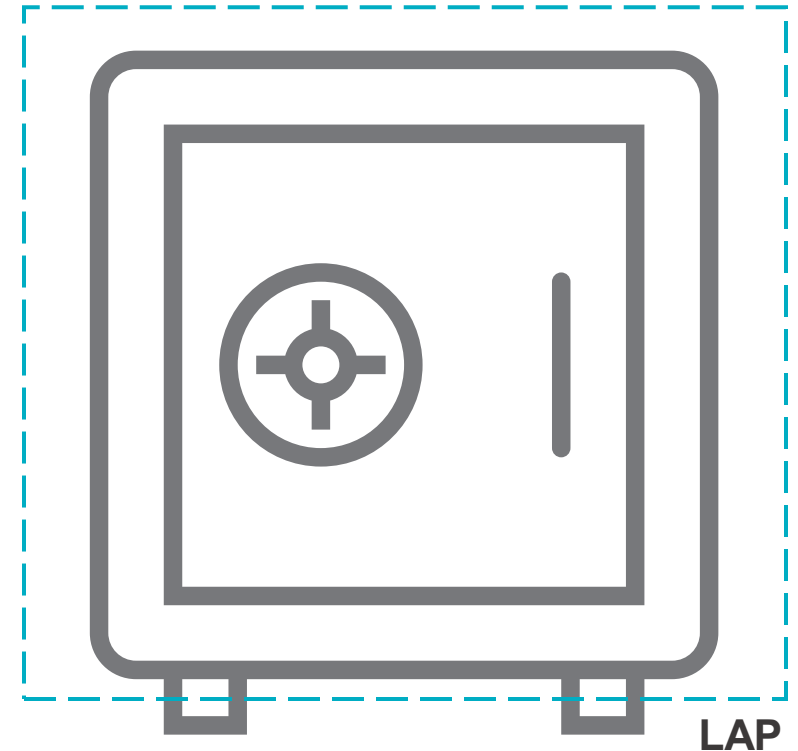




Data Access Committee

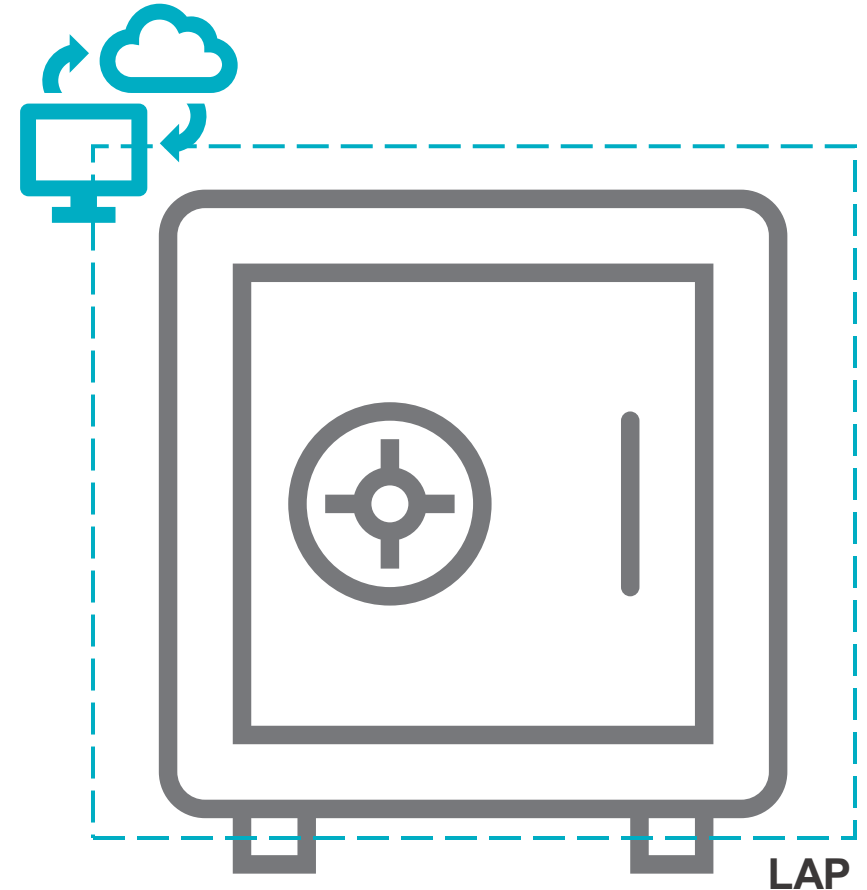


- The **Data Access Committee** will have the power to review applications and decide whether access is granted.
- The joint data controllers will have the right to participate, either directly or indirectly via nominated representatives, in the Committee.





- Users will be able to access the data via a Virtual Desktop Infrastructure (VDI) solution, ensuring that additional data cannot be ingested into the secure environment and that the existing data cannot be voluntarily extracted from the environment without authorisation from the joint controllers.



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



Confidentiality

It has been accepted by the Department of Health and Social Care (DHSC), the General Medical Council (GMC), and the British Medical Association (BMA) that when sharing information for the direct care of an individual patient, healthcare professionals that have a legitimate relationship with that patient can rely on that patient's implied consent to modify the original scope of the duty of confidence.

To rely on implied consent, however, it is necessary that certain conditions are strictly met:

- that the sharing of data is for **direct care**;
- that the sharing is undertaken amongst healthcare professionals that have a **legitimate relationship** for the patients' care;
- that there are '**no surprises**' to patients;
- that patients have a **right to object**.

All the above conditions will be robustly satisfied in the context of the Programme. Therefore, it is believed that the processing of data undertaken under it will not breach the principles of confidence.

For secondary use purposes, such as research, the data will be **pseudonymised** and, under appropriate technical and organisational measures, made available in de-identified form to Users. Sufficient **controls over the data** and **controls over the environment** are applied so that the dataset is de-identified from the perspective of the Users viewing the data.

Whilst reasonable precautions have been taken, both in terms of technical and organisational measures, the richness of the data has led to concerns about the potential remaining risk of re-identification. **CAG support** is sought to provide cover for this possibility, amongst other reasons, whilst the OneLondon SDE Programme continues to **further enhance** the LAP environment's privacy-enhancing technological capabilities.

After consulting with local data controllers and national bodies such as the National Data Guardian, it has been recommended that the OneLondon SDE seek a s251 exemption. CAG support is being sought for:

- **Linkage of national datasets** received via DARS with local datasets. They will then be available within the OneLondon Secure Data Environment for research and non-research purposes;
- The use of Community Service Data Set (CSDS) received via DARS for research purposes which is not covered by the Secretary of State Directions; and
- The **richness** of the dataset whilst the Programme continues to consider further privacy-enhancing technologies

Can a Patient Opt Out?

The OneLondon SDE Programme will provide patients with the choice to **dissent** and/or **object** to sharing information to the London Analytics Platform. The **National Data Opt-Out** will also apply in line with national policy. The Programme is currently considering how to operationalise these mechanisms at a regional level.



For any questions that could not be covered today, please contact us:
londonsde@informationgovernanceservices.com