

Wessex Secure Data Environment (SDE)

Data Sharing Agreement / Heads of Terms Agreement

made on

02/06/2026

between

**University Hospitals Southampton NHS Foundation Trust (UHS)
(operating as Wessex SDE)**

and

Dorset and Hampshire & Isle of Wight General Practices

This is a high-level Data Sharing Agreement / Heads of Terms Agreement which is used to outline the key elements of personal data sharing between the relevant parties, for the operation of the Wessex SDE. This document refers to information relating to both living and deceased individuals. “Personal data” retains its meaning under UK GDPR (relating to living individuals only) but the scope of this policy also includes information relating to deceased individuals where relevant.

Document Management

Revision History

Version	Date	Author	Description
0.1 DRAFT	03/09/2025	Antje Carpenter, NHS SCW	First draft for consideration
0.2 DRAFT	10/10/2025	Adam Tuckett, NHS SCW	QA amendments
0.3 DRAFT	14/10/2025	Adam Tuckett, NHS SCW	Amendments following Primary Care Feedback.
0.4 DRAFT	04/11/2025	Antje Carpenter, NHS SCW	Amendments following further Primary Care Feedback and inclusion of data repository model. Updated controllership diagram.
1.0 DRAFT	06/11/2025		Restructured for flow and clarity
1.1 DRAFT		Antje Carpenter, NHS SCW	Alignment with DPIA
1.2 DRAFT	27/05/2026	Antje Carpenter, NHS SCW	Consideration of new processors
1.3 DRAFT	03/06/2026	Keith Gomes Pinto	Review and further edits – resolved some comments
1.4 DRAFT	04/06/2026	Antje Carpenter/Keith Gomes Pinto	Final edits
1.5 DRAFT	05/06/2026	Jo Stuart	Addition of Appendices

Reviewers

Version	Date	Reviewer	Description
1.3 DRAFT	xx/xx/2026		

Approved By

Version	Date	Approver (Name)	Title

Table of Contents

Purpose of this document	5
Introduction to SDE.....	5
Benefits:	7
Benefits for individuals (patients and service users)	7
Benefits for organisations (GP practices, NHS bodies and researchers)	8
Benefits for the wider public and health system	8
Parties involved	8
Data Controller:	10
Data Processor(s):	10
Data Contributors:	11
Approved Data Users:.....	12
Purpose of data sharing.....	12
Value and benefit of data sharing	13
Data	13
Data systems, modalities and fields	13
Source systems:	13
Identifiable personal data and deceased data	14
Health and care data (special category data)	14
Additional sensitive data (where required and proportionate)	15
Types of data:	15
Accuracy of data being shared	17
Data provenance	17
Data sharing process	18
1. Agreement and approval	18
2. Data extraction from GP systems	18
3. Secure transfer into the SDE.....	19
4. Data preparation and protection (within DPE)	19
5. Provision to researchers (TRE)	19
6. Output checking and release	19
7. Optional sharing between SDEs.....	20
8. Retention and disposal	20
Regional (Wessex) repository for GP data (still in development)	20
Collaboration with other SDEs.....	20
Notification and Default Inclusion for Approved Research Studies	21
How data is secured within the SDE	22
Retention and disposal requirements for the information to be shared	22
Breach Management	22
Controls.....	22
Legal Gateways	22

Lawful processing (UK GDPR) - Article 6 basis – all Personal Data.....	23
Most appropriate lawful basis for processing:	23
Lawful processing (UK GDPR) - Article 9 condition – Special Categories of Personal Data	23
Compliance with Confidentiality/ Right to Privacy.....	23
Management of Individual Rights	24
Transparency	24
<i>Contractual management of this agreement.....</i>	<i>25</i>
Specify any particular obligation on any party to this Agreement	26
Amendments and Variation	26
Routine Review	26
Right to Vary	26
Notice of Variation.....	26
Opt-Out on Variation	26
Ending the Agreement.....	27
Signatories	27
<i>Appendices</i>	<i>28</i>

1.	PURPOSE OF THIS DOCUMENT This Data Sharing Agreement sets out the purpose, process, responsibilities and controls for sharing data between participating Dorset and HIOW general practices and UHS operating as Wessex Secure Data Environment (SDE). This agreement ensures that any data shared is handled securely, lawfully, and transparently, in line with data protection legislation and NHS governance standards. The aim is to support approved research and analysis that benefits patient care, population health, and service improvement, while maintaining the highest standards of confidentiality and public trust.
2.	INTRODUCTION TO SDE Secure Data Environments are platforms that allow approved users to access and analyse sensitive data (such as health records) without the raw data ever leaving the secure environment. Currently, when approved researchers use NHS data for research, they are sent a copy of the data they need and must follow the terms set out in a data access agreement. A Secure Data Environment holds NHS data and allows approved researchers to safely access designated research workspaces within the SDE (per research study) to analyse patient-level de-identified data for research. Researchers cannot remove data from the SDE; any outputs are anonymised and undergo technical and clinical review before release. The Wessex SDE is funded through an NHS England programme based on the Data Saves Lives policy published by the Department of Health & Social Care, and is part of a network of regional secure data environments across England. The Wessex Secure Data Environment (SDE) will be used for data-driven translational research in any field of health or social care. The SDE provides a secure infrastructure for approved research programmes conducted by commercial and non-commercial researchers in the NHS, enabling them to access integrated multi-modal data from various sources, including electronic health records, imaging, pathology, genomics, and research cohorts. It will remove the need for sending large volumes of data between organisations and researchers. This will make data more accessible, less fragmented, and of higher quality while also gaining public and patient support for health data research. This allows us to unlock the potential of NHS data in supporting research, creating lifesaving new treatments and medicines, and bringing wider benefits to patients and the NHS. The SDE comprises two key environments which are physically separate from one: 1) Data Processing Environment (DPE) is where any identifiable data is processed within a restricted environment accessible exclusively by Wessex SDE technical personnel: • Identifiable personal data and deceased data (e.g. NHS number, name, date of birth) is used for:

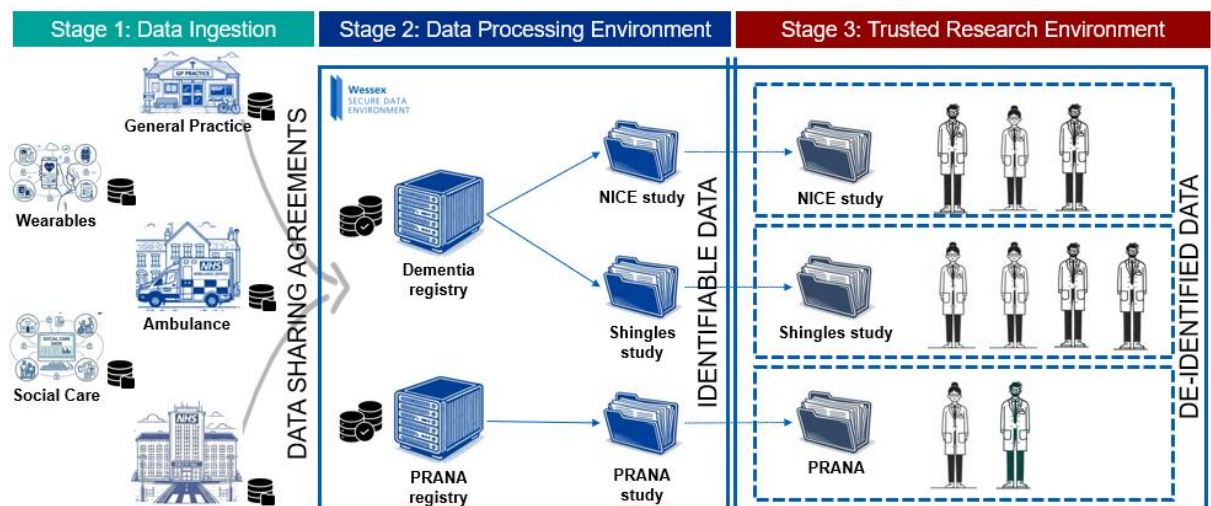
- Data ingestion and validation
 - Record linkage across datasets
 - Application of national and local opt-outs
- This data is NOT accessible to or shared with researchers within the Trusted Research Environment (TRE) – discussed below.
 - Personal identifiable data will be processed exclusively by the SDE's Technical Team in the DPE with the following steps undertaken:
 - Acquisition of the raw primary care data
 - Versioning and cleansing of the raw data
 - Merging the data, such that it is in a consistent format regardless of the system of origin.
 - Tracking and application of opt-outs, including:
 - ✓ National Data opt out
 - ✓ Type 1 opt-outs
 - ✓ A local Wessex SDE Opt-Out – by patient or practice

All data opt outs above will be implemented in line with guidance within 21 days of receipt of notification or sooner within the DPE. This will include removal of data held where a patient has previously provided data but has now decided to opt out.

Where data has already been pseudonymised and provided to researchers in the TRE (see below), the opt out will not be applied retrospectively, but no additional data pertaining to the opted-out patient will be provided for that (or any other) study.

2) **Trusted Research Environment (TRE)** is where research datasets are staged for approved researcher access. The datasets are:

- Pseudonymised (identifiers replaced with codes or hashes)
- Minimised to only what is necessary for the study
- Researchers only have access to the de-identified data applicable to the research study that has been approved by the Data Access Committee (DAC)



Activity within the researcher-accessible area is monitored, and data cannot be downloaded. The anonymised results of analysis may be exported, but these will be subject to individual, manual inspection and a range of automatic checks to ensure that the proposed export fits within the terms of the agreement - including any conditions placed upon dissemination and publication.

Data may also, where relevant, be linked from datasets already securely held within the DPE. Manual inspection and analysis will be required whenever a new data flow is introduced or an existing data flow changes. In the context of a specific, approved research project, additional manual annotation or elaboration of metadata may be required. Data from the DPE is only linked with data from other environments once an approved programme of research has been identified.

Using and sharing data through the Wessex Secure Data Environment (SDE) provides significant benefits for individuals, healthcare organisations, and the wider public by enabling safe, efficient, and evidence-driven use of health and care information.

Whilst data ingress flows may be pseudonymised where feasible, University Hospital Southampton NHS Foundation Trust will have access to the encryption keys for two reasons:

- to enable linkage of patient data from different sources within the DPE prior to combination for pseudonymised research datasets
- to enable reidentification for specific purposes. At present no such purposes have been identified and agreed via the National Confidentiality Advisory Group.

Benefits:

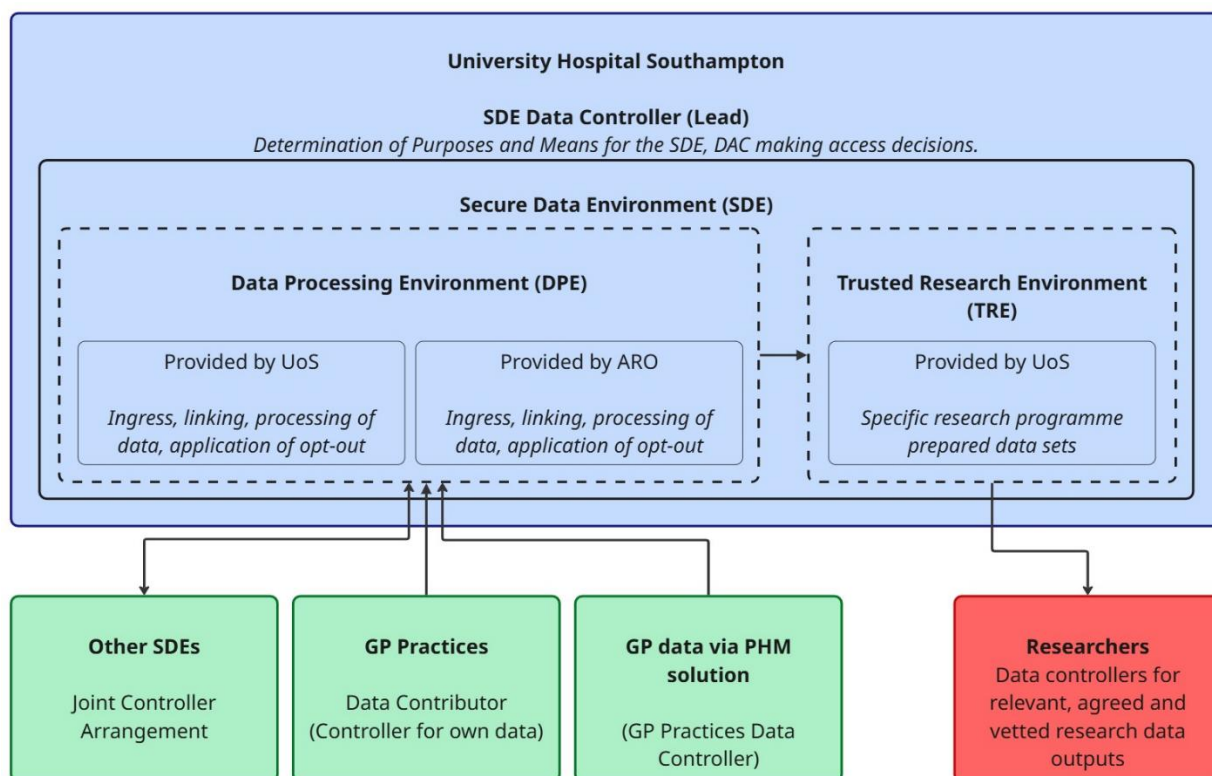
Benefits for individuals (patients and service users)

- *Improved health outcomes and quality of care*

	• <i>Better understanding of individual health needs</i> • <i>Earlier identification of risks and preventative care</i> • <i>Improved patient experience</i> Benefits for organisations (GP practices, NHS bodies and researchers) • <i>Facilitates joined up working across systems</i> • <i>Improves accuracy, completeness, and reliability of data</i> • <i>Speeds up processes and access to data</i> • <i>Reduces administrative burden on staff</i> • <i>Supports more effective use of resources</i> Benefits for the wider public and health system • <i>Improves population health and reduces inequalities</i> • <i>Enables innovation and research at scale</i> • <i>Enhances system-wide planning and service design</i> • <i>Maintains public trust through secure data use</i>						
3.	PARTIES INVOLVED <table><tr><td>Data Sharing Agreement Owner</td><td>University Hospitals Southampton NHS Foundation Trust (UHS) – operating as Wessex SDE.</td></tr><tr><td>Data Controller</td><td> University Hospitals Southampton NHS Foundation Trust (UHS) is the lead data controller, operating as Wessex SDE. General Practice will continue to be the data controller for their own data and can opt-out of any approved studies. (Researchers access data within the SDE as authorised users and do not act as data controllers for the underlying datasets but are a separate controller for their outputs (see further details under approved data user(s)). </td></tr><tr><td>Data Processor(s)</td><td>University of Southampton (UoS) as the technical platform provider.</td></tr></table>	Data Sharing Agreement Owner	University Hospitals Southampton NHS Foundation Trust (UHS) – operating as Wessex SDE.	Data Controller	University Hospitals Southampton NHS Foundation Trust (UHS) is the lead data controller, operating as Wessex SDE. General Practice will continue to be the data controller for their own data and can opt-out of any approved studies. (Researchers access data within the SDE as authorised users and do not act as data controllers for the underlying datasets but are a separate controller for their outputs (see further details under approved data user(s)).	Data Processor(s)	University of Southampton (UoS) as the technical platform provider.
Data Sharing Agreement Owner	University Hospitals Southampton NHS Foundation Trust (UHS) – operating as Wessex SDE.						
Data Controller	University Hospitals Southampton NHS Foundation Trust (UHS) is the lead data controller, operating as Wessex SDE. General Practice will continue to be the data controller for their own data and can opt-out of any approved studies. (Researchers access data within the SDE as authorised users and do not act as data controllers for the underlying datasets but are a separate controller for their outputs (see further details under approved data user(s)).						
Data Processor(s)	University of Southampton (UoS) as the technical platform provider.						

		ARO as the platform provider for an additional Data Processing Environment for the SDE. The Data Processors will not be a signatory of this agreement but have signed a Data Processing Agreement to legally control the processing of data.
	Data Contributor(s)	General Practices in Dorset and Hampshire & Isle of Wight (HIOW).
	Approved data user(s)	Researchers approved by the NHS Research SDE Network validation process. Organisations that are users of data from the SDE will not be signatories to this agreement but will sign a separate Acceptable Use Agreement (Appendix C).
	Integrated Care Boards Hampshire & Isle of Wight Integrated Care Board	NHS Dorset Integrated Care Board (ICB) are Lead Controller for the Dorset Intelligence and Insight Service (DiiS). Hampshire & Isle of Wight Integrated Care Board are Lead Controller for the Cerner HealthIntent Platform. GP data may transfer directly from the relevant PHM system into the SDE (instead of direct transfer from GPs). Whilst this Data Sharing Agreement stands on its own, it is considered a ‘companion’ of the Population Health Management (PHM) Platform Data Sharing Agreement. It is used to agree the flow of primary care data to the Secure Data Environment through a PHM Platform. Only data originating from General Practices signed up to this agreement can be transferred to the Secure Data Environment.

Wessex SDE Data Controllershship diagram from a General Practice data perspective:



Data Controller:

The organisation(s) which determine(s) the purposes for which, and the means by which, personal data and deceased data is processed in accordance with Article 4(7) of the UK GDPR.

University Hospital Southampton (UHS) is the **data controller** of the data that is used within the Wessex SDE. As the host organisation they have determined the scope of research the SDE will support (the 'purposes' for processing) and decided on the detail of the system(s), technical controls and overall data management (the 'means' of processing).

General practices act as **data controllers** for their own data as they determine the purposes and means of processing patient data held in their clinical systems, are legally responsible for ensuring compliance with data protection requirements, and control how and when data is shared with the Wessex SDE. They transfer controllership to the SDE when releasing data to the programme.

Practices will be able to opt-out of their data being used in specific research datasets on a project-by-project basis.

Data Processor(s):

The organisation(s) which process(es) personal data on behalf of the controller(s) in accordance with Article 4(8) of the UK GDPR.

The '**Core**' **Data Processor** for the Wessex SDE is the **University of Southampton (UoS)**, through a contractual agreement and delegation of responsibilities. This contract ensures that the data is processed lawfully, securely, and only for the agreed purposes; in compliance with the Data Protection Act 2018, the UK GDPR, the Common Law Duty of Confidentiality, applicable NHS information governance and confidentiality guidance and in line with the SDE's ISO27001 accreditation.

ARO acts as the **Data Processor** for the provision of the Data Processing Environment, under a formal contractual agreement that defines roles and delegated responsibilities. This arrangement ensures that all data processing is conducted lawfully, securely, and strictly for agreed purposes, in compliance with the Data Protection Act 2018, the UK GDPR, the Common Law Duty of Confidentiality, applicable NHS information governance and confidentiality guidance, and aligned with the SDE's ISO 27001 accreditation.

Additionally, for GP data, the SDE may rely on data ingestion from the ICBs in relation to the processing of population health data as set out below:

- **Hampshire & Isle of Wight Integrated Care Board** for any provision of General Practice data from the ICB's Population Health Analytics Platform, where a Data Sharing Agreement is in place between the HIOW General Practice(s) and UHS as the SDE, and where the Practice has not objected to the use of Practice data in an SDE approved research programme.
- **Dorset Integrated Care Board** for any provision of General Practice data from the ICB's Population Health Analytics Platform – Dorset Intelligence and Insight Service (DiIS), where a Data Sharing Agreement is in place between the Dorset General Practice(s) and UHS as the SDE, and where the Practice has not objected to the use of Practice data in an SDE approved research programme.

The Parties may engage **third-party organisations** to support data processing and analysis activities. Where a third party is required to act as a data processor and access personal data and deceased data, the Data Sharing Agreement will be formally updated (or supplemented) to reflect the new arrangement, and an appropriate Data Processing Agreement will be put in place, clearly defining roles, responsibilities, and governance controls.

Data Contributors:

A Data Contributor is an organisation or body, such as a general practice, NHS Trust, or other approved data-holding organisation, that supplies data to the Wessex Secure Data Environment (SDE) for the purposes of approved research, analysis, or service improvement.

	In contributing data, they transfer the Data Controller responsibility to UHS for ensuring that any data shared for research is accurate, up-to-date, minimised, and lawfully disclosed under the UK GDPR, Data Protection Act 2018, and the Common Law Duty of Confidentiality. Practices will be able to opt-out of their data being used in specific research datasets on a project-by-project basis. Approved Data Users: Researchers are approved to access and use SDE held data by being validated against the NHS Research SDE Network validation process. This process has been set out by NHS England and is applied consistently across all SDEs in the Network. The process is currently completed by UHS as the Wessex SDE Host organisation, however in time this function will become a central function which supports all SDEs in the Network. A copy of the User and Organisational validation form is provided in Annex A.
4.	PURPOSE OF DATA SHARING The SDE has approval for the use of data for the purposes outlined below, as set out in our Health Research Authority (HRA) approval from the Confidentiality Advisory Group (CAG) and the Research Ethics Committee (REC). WSDE-HRA-approvals-and-amendments.pdf Purposes: • New approaches to diagnosis, making better use of blood tests, medical images, and other information already in patient records. • New approaches to treatment, including changes to clinical pathways, better support for clinical decisions, and the introduction of new therapies. • New approaches to patient records, improving the accuracy and relevance of the data recorded and the management of patients across services. • Clinical trial feasibility using previously collected clinical and operational data (but NOT including re-identification of data subjects or any form of direct approach for recruitment to clinical trials without amendment to this agreement). • Population health research to identify factors to aid understanding of health outcomes of a group of individuals including the distribution of such outcomes within groups including study of health determinants, health behaviours and the impact of health policies and interventions. • Operational healthcare research using health and social care data to improve decision making, efficiency, and effectiveness in health services and systems.

	From time to time, updates to our Health Research Authority (HRA) approvals may be required to support new areas of research, clinical trials, or data testing. Any such amendments will be made in full compliance with HRA requirements and oversight processes. Details of any approved changes will be published on the Wessex SDE website to maintain transparency. <i>In addition, all practices that have signed a Data Sharing Agreement will receive a notification update outlining the nature of the change and its relevance to data sharing activities.</i> Value and benefit of data sharing Sharing data securely through the SDE enables research that directly benefits patients, the NHS, and wider society. By contributing data, practices help ensure that research reflects real-world patient experiences, supports earlier diagnosis and better treatments, reduces health inequalities, and informs the design of more effective and efficient healthcare services, these include: • To improve patient care and outcomes • To understand population health and ensure appropriate service provision • To support health and care research and innovation • To improve the accuracy and completeness of data • To ensure data is available securely when needed • To reduce burden and support efficient use of NHS resources
5.	DATA
5a.	Data systems, modalities and fields Each Data Contributor will decide the data modalities [and data fields] from their source systems that they are willing to share. Source systems: ○ GP clinical systems – Optum (EMIS), TPP (SystemOne) ➤ Pseudonymised ➤ Identifiable ○ ICB PHM Platform ➤ Pseudonymised data ➤ Anonymised aggregated data ○ Regional GP data repository ○ Other SDEs within England ➤ Pseudonymised ➤ Identifiable

The Wessex Secure Data Environment (SDE) requires the use of both **personal (identifiable)** and **special category (health) data** to support data linkage, research, and service improvement. The types of data used and the reasons for their inclusion are outlined below.

Identifiable personal data and deceased data

The following identifiers are required:

- Name (forename and surname)
- Address and postcode (full or partial)
- Date of birth / age
- Date of Death
- Gender
- NHS number
- GP/practice details

Why this is needed:

- To accurately link records across multiple datasets (e.g. GP, hospital, and national datasets) to create a complete patient pathway
- To ensure data quality and accuracy, including deduplication and validation of records
- To enable application of national, local, and GP opt-outs and meet legal and confidentiality requirements
- To support safe and reliable dataset preparation prior to pseudonymisation

These identifiers are only used within the secure Data Processing Environment (DPE) and are not accessible to researchers.

Health and care data (special category data)

This includes:

- Clinical information (diagnoses, conditions, procedures)
- Medications and treatment details
- Laboratory and test results
- Vital signs and clinical measurements
- Patient records (including coded data and, where necessary, free text)

Why this is needed:

- To identify disease patterns, risk factors, and outcomes
- To support research into diagnosis, treatment, and prevention of disease
- To evaluate clinical pathways and service effectiveness
- To enable population health analysis and service planning

Additional sensitive data (where required and proportionate)

In some cases, limited use of additional information may be required, such as:

- Ethnicity and demographic characteristics
- Genetic/genomic data (where relevant to a study)
- Other factors influencing health outcomes (e.g. religion where clinically relevant)

Why this is needed:

- To identify and address health inequalities and disparities
- To improve understanding of risk factors and treatment effectiveness across populations
- To support targeted interventions and personalised approaches

Types of data:

- **Patient Identifiable Data (personal data and deceased data):** Patient identifiable data is any information that can be used to identify an individual directly or indirectly, and it is protected under the UK General Data Protection Regulation (UK [GDPR](#)). The UK GDPR requires that this data, especially sensitive health information, be processed lawfully, fairly, and transparently, in compliance with Individual's Rights and used only for specified and legitimate purposes, limited to what is necessary, kept secure and confidential, and subject to additional safeguards due to its sensitive nature.

For any study the default is always to process pseudonymised data only. However, based on a study's requirements, the SDE may need to process identifiable patient-level data for the purposes of linkage, avoidance of deduplication and application of opt outs.

Researchers will NEVER have access to identifiable data. The data is always pseudonymised before it is made available in a defined secure workspace within the SDE.

- **Pseudonymised Data:** Pseudonymised data is personal data and deceased data that has been processed so that direct identifiers are replaced with artificial identifiers, such as codes or numbers, thereby reducing the ability to attribute the data to a specific individual; however, it remains identifiable where additional information exists, which is kept separately and subject to appropriate technical and organisational security measures.
- The following techniques help reduce the risk of identification of individuals:
 - **Data minimisation and reduction techniques** – the principle of collecting, processing, and storing only the personal data and deceased data that is **adequate, relevant, and strictly necessary** for a specific purpose.

Article 5(1)(c) of the UK GDPR says that personal data shall be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).’

Further reduction of re-identification risk within a pseudonymised dataset can be achieved by removing or modifying indirect identifiers that, either alone or in combination, could enable the identification of an individual.

The SDE will apply the required data minimisation techniques in line with our HRA approvals to limit the extent of data transfer.

➤ Other techniques such as generalisation, small number suppression and noise addition may also be utilised.

- **Anonymised aggregated data:** Data that has been processed so that individuals are no longer identifiable and then combined into summary-level information to show general trends or patterns without revealing details about any individual.

It is used to protect individual privacy while still enabling analysis of patterns in large datasets. Where anonymisation is carried out effectively, such that individuals are no longer identifiable by any reasonably likely means in line with ICO guidance, the data will fall outside the scope of UK GDPR, will no longer constitute confidential patient information, and the National Data Opt-Out will not apply.

The data that is shared outside of the SDE consists only of fully anonymised, aggregated outputs. Recipients cannot identify individuals, either directly or indirectly, and do not receive any pseudonymised or identifiable data.

- **Disclosure control (“airlock”) process**

All outputs are subject to a formal review process before release:

- Automated and manual checks are applied
- Outputs are assessed for re-identification risk
- Only safe, non-disclosive outputs are approved

Example data modalities:

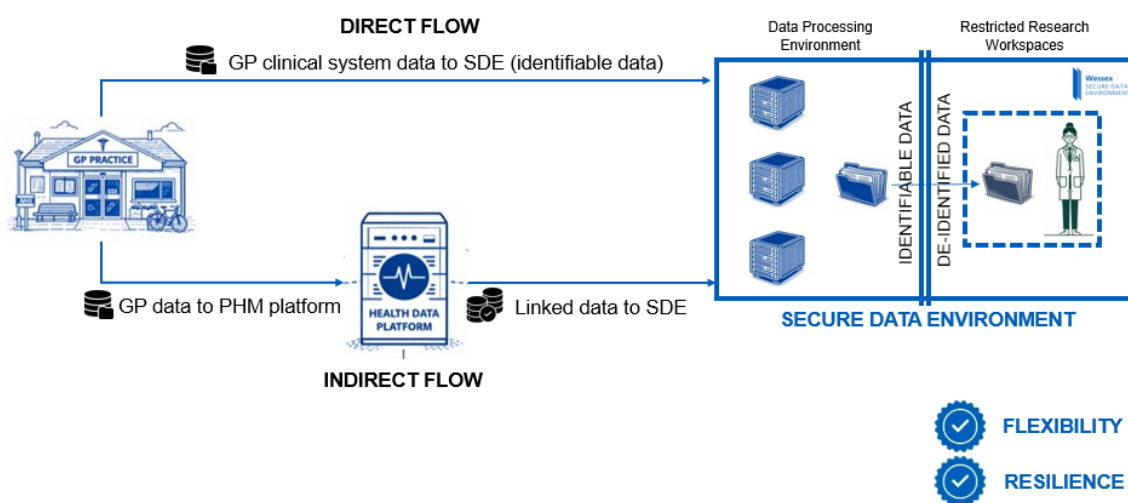
- Nationally reported commissioning datasets (CDS)
- Structured, coded data from EPR/primary care systems
- Free text, notes and reports from EPR/primary care systems
- Patient-reported outcomes, patient-provided data against forms and questionnaires
- Detailed laboratory test results from pathology systems/services
- Detailed medications data
- Detailed notes, reports, and structured data from specialist Cancer systems
- Detailed radiology reports
- Medical Imaging
- Digital Pathology Imaging, with relevant metadata, linked to reports

	• Detailed genetic/genomic/panel test results • Genomic source data • Sensor data • Medical photography • Video content • Researcher-collected/specified data Example data fields: • Patient Demographics • Biochemistry Results • Virology Results • Haematology Results • Microbiology Results • Histology Requests • Radiology Requests • Cancer Referrals • Cancer Progression • Vital Signs • Maternity Services Data Set • Surgeries & Procedures • Endoscopies • Discharges to GP • Radiotherapy • Chemotherapy • Physiology
5b.	Accuracy of data being shared Wessex SDE supports data quality through robust validation, standardisation, governance, and monitoring processes, enabling the identification, management, and continuous improvement of data quality. Data provenance GP practices are asked to provide clear information on the provenance of their data, including how it was collected, its source systems, and any relevant coding or recording processes. This information is essential to ensure that research using GP data is accurate, transparent, and ethically robust. Understanding the provenance helps researchers to interpret results correctly, assess data quality and completeness, and confirm that findings genuinely reflect patient care and outcomes. It also strengthens accountability and public trust, demonstrating that all data used for research has been lawfully and responsibly sourced. As the lead Data Controller, providing data for studies, the SDE will ensure that data is shared in alignment with the study protocol and data minimisation protocols.

5c. Data sharing process

Flowing primary care data into the Wessex SDE will follow defined pathways which will mature over time. These processes have already been tried and tested across the SDE Network and provide robust, secure processes that are approved by the HRA.

The data sharing process for the Wessex Secure Data Environment (SDE) is a **controlled, secure, and governance-led process** that ensures data is only shared where appropriate, necessary, and lawful.



A more detailed version is available in [Appendix E](#).

1. Agreement and approval

- GP practices (as **data controllers**) must first **agree to participate** by signing a:
 - Data Sharing Agreement (DSA)**
 - Data Protection Impact Assessment (DPIA)**
- These agreements set out:
 - The **purpose of data use**
 - The **legal basis for sharing**
 - The **roles and responsibilities** of each organisation

2. Data extraction from GP systems

- For participating practices, data is extracted:
 - Directly from GP clinical systems (e.g. EMIS, TPP SystemOne), or
 - Via approved intermediaries (e.g. Diis platform in Dorset, GP clinical system suppliers)
- Data flow only starts:
 - With appropriate **technical authorisation (e.g. system notification/approval)**

- After **formal approval by the practice**

3. Secure transfer into the SDE

- Data is transferred using **secure, encrypted methods** into the:
 - **Data Processing Environment (DPE)** hosted by Wessex SDE

4. Data preparation and protection (within DPE)

Within the secure DPE, data undergoes a series of controlled steps:

- **Cleansing and standardisation** (consistent format across systems)
- **Application of opt-outs:**
 - National Data Opt-Out
 - Type 1 GP opt-out
 - Local opt-outs (where applicable)
- **Pseudonymisation** (e.g. SHA256 hashing)
- **Data minimisation** (only necessary fields retained)
- **Data linkage** (where required for approved research)

At this stage:

- Identifiable data is **only accessible to authorised technical processes/users**
- Researchers do **not** have access to identifiable data

Note: In some approved research programmes, where a contributing NHS organisation cannot independently identify the shared cohort, the Wessex SDE may securely provide that organisation with a list of patient identifiers for the sole purpose of identifying matching patients and returning relevant data only

5. Provision to researchers (TRE)

- Pseudonymised, minimised datasets are transferred to the:
 - **Trusted Research Environment (TRE)**
- Researchers can only access data if they:
 - Are **approved and accredited**
 - Have a **clearly defined project** approved through governance (DARF, DAC)
- Controls include:
 - Role-based access
 - No ability to download or remove raw data
 - Full audit and monitoring

6. Output checking and release

- Results generated by researchers are:

- **Aggregated and anonymised**
- Subject to **disclosure control (including small number suppression)**
- Outputs pass through a **strict “airlock” process** before release
- Only **non-identifiable outputs** are shared externally

7. Optional sharing between SDEs

- Where approved, pseudonymised datasets may be:
 - Shared with other SDEs, or
 - Received from other SDEs
- This supports **multi-region or national research**, with the same safeguards applied

8. Retention and disposal

- Data is retained in line with:
 - **NHS Records Management Code of Practice**
- Project datasets are:
 - **Archived or securely destroyed** after use

Regional (Wessex) repository for GP data (still in development)

The aim is that all GP data will be held securely within a repository within the SDE. When a project is approved by the DAC, GPs are notified and have a 10- working day opt-out window if they do not wish their data to be used for this specific research project.

This model removes the need for GPs to share data individually for each project (reduction of repeat data transfer), reducing administrative burden, enables faster access and improves efficiency whilst still making decisions on providing data on a per project basis.

The regional repository model is the preferred approach because it provides a more efficient and secure way to manage GP data for research. By holding all GP data securely within the SDE, this model eliminates the need for repeated data transfers for each approved project, reducing administrative burden and technical complexity. It also ensures consistency in data quality and governance, while still respecting GP autonomy through the opt-out window for each DAC-approved project. Over time, the SDE will continue to develop and refine this solution for the use by GPs across Wessex.

No GP data will be shared outside the UK.

The SDE operates a “data stays within the environment” model, so raw data is not exported or shared externally. Fully anonymised aggregated outputs from the research studies that have been approved may be shared outside of the UK.

Collaboration with other SDEs

	Wessex SDE will at times work in collaboration with other SDEs within England on research programmes where data from more than one SDE is required. This will mean data shared under this agreement can be transferred to another SDE for a specific approved research programme. Wessex SDE currently has a data sharing agreement with the southern SDEs (Kent and Medway System (KMS) SDE & Southwest (SW) SDE) covering collaborative programmes and each SDE applies a consistent baseline of governance and security. The SDE Collaboration Data Sharing Agreement, which is modelled on this agreement, committing the SDEs to very similar arrangements, only permits data to be shared between SDEs on the following basis: • The data shared can only be used for the approved collaborative programmes. • The default sharing of data between SDEs will be pseudonymised data. This will be linkable via a shared pseudo approach if required by the programme. • The default controllership model for collaborative programmes will be joint control between the relevant SDEs. • SDEs will collaborate on Data Access Committee reviews and approvals for collaborative programmes to the extent that each SDE is able to approve the programme in accordance with its own governance, legal, and risk-acceptance requirements. • Data providers will be informed about collaborative programmes in the same way as they are for standard SDE programmes. • Collaborative programmes will be subject to any limitations on the use of data in any SDE set in respect of any National Confidentiality Advisory Group (CAG) support. Any programme that cannot be managed within these will need to seek either specific support or appropriate amendment to the SDE CAG support prior to approval. • Researchers will access the data via the SDE leading on the programme.
5d.	Notification and Default Inclusion for Approved Research Studies 1. When a research study has been approved by the Wessex SDE Data Access Committee (DAC) UHS will issue a notification email to all signatory GP practices through their DPOs and deputies informing them of the study giving them the opportunity to review the study and opt-out. 2. The notification will summarise: ○ the study title, sponsor, and DAC reference number; ○ the purpose and type of data requested; ○ confirmation that all required HRA/CAG approvals are in place; and ○ the link to the study's entry on the Wessex SDE Data Use Register (DUR). 3. From the date of issue, GP practices will have ten working days to provide written notice if they do not wish their data to be used in that study.

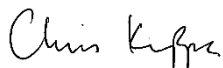
	Unless such notice is received within this period, the practice's data will be included by default in the approved research study. 4. The opt-out described in this clause applies on a per-study basis and does not affect the practice's participation in other approved research or its wider participation in the SDE.
5e.	How data is secured within the SDE All data within the SDE is managed in line with our HRA approval: WSDE-HRA-approvals-and-amendments.pdf
5f.	Retention and disposal requirements for the information to be shared Once the research has finished, the dataset (and any copies) will be archived and destroyed according to UHS policy/ Wessex SDE policy. The data will be retained for as long as the purpose(s) described above remains valid or a new legal purpose agreed. This will be in line with the: NHS Records Management Code of Practice 2021 and updates 2023 A guide to the management of health and care records Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk). No physical or electronic copies will be made of the identifiable data except to the extent reasonably necessary for the purposes described in this agreement.
5g.	Breach Management Parties to this agreement must be committed to raise relevant incidents to the lead controller for coordination and notify all affected partners. Where an incident involves personal data and deceased data, it must be assessed against the UK GDPR threshold. If it is likely to result in a high risk to individuals' rights and freedoms, it must be reported to the ICO within 72 hours with notification made via the DSPT Incident Reporting Tool.
6.	CONTROLS
6a.	Legal Gateways There are multiple controllers involved but all have a statutory basis to either lead, commission, support or participate in research activities. Some of those legal gateways are explicit which are as follows:

	General Practice contract: This recognises and supports the NHS commitment to conducting research, in particular through (non-mandatory) contractual incentives in the Quality & Outcomes Framework. NHS Trust – NHS Act 2006: Schedule 4, Paragraph 16 – may undertake and commission research and make available staff and provide facilities for research by other persons. NHSE (indirect support for GP practices participating in research, especially when coordinated through NHSE or ICBs) - NHS Act 2006, Section 13E – places a duty on NHSE to secure continuous improvement in the quality of service, which includes research. Section 13L – requires NHSE to promote research on matters relevant to the health service and use of evidence obtained from research. - Health and Social Care Act 2012 – Section 6 – imposes a duty on the Secretary of State to promote research in the health service. Section 254 – allows the Secretary of State to direct NHSE to establish and operate information systems for the collection and analysis of health and care data, including for research, Section 255 – enables other bodies to request NHSE to operate information systems for research purposes.
6b.	Lawful processing (UK GDPR) - Article 6 basis – all Personal Data Most appropriate lawful basis for processing: Processing Personal Data - Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; This article supports the legal powers of all public authorities. UHS as an NHS Trust has a legal power to conduct research as set out in section 5a. Art. 6 GDPR – Lawfulness of processing - General Data Protection Regulation (GDPR) A guide to lawful basis ICO
6c.	Lawful processing (UK GDPR) - Article 9 condition – Special Categories of Personal Data Most appropriate condition for processing: Article 9(2)(j) - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation (GDPR)
6d.	Compliance with Confidentiality/ Right to Privacy <i>[Please state here how you will be satisfying Confidentiality]</i>

	- Consent - Statutory Override X - Substantial Public Interest CAG Approval has been granted to the SDE for the option to receive identifiable data into the SDE. This support extends to the data contributing site, where required. It also extends to re-identification for specific purposes (access to pseudo key), sharing of confidential patient information to contributing sites for cohort finding, and linkage of core data set prior to any data requests (repository). CAG (IRAS ID: 334643) & REC (IRAS ID: 339034) support provides a lawful basis to allow confidential patient information to be processed by the relevant parties for the specified purposes without incurring a breach of the common law duty of confidence. CAG: Confidentiality Advisory Group - Health Research Authority REC: Research Ethics Service and Research Ethics Committees - Health Research Authority Is there any interference with Human Rights Article 8? No If yes, document why it is necessary and proportionate to do so: N/A
6e.	Management of Individual Rights Identifiable GP data will be ingested to be linked with other data sets within the SDE but only pseudonymised data is made accessible to researchers inside the SDE. Outputs will always be fully anonymised. Identifiable data will potentially be kept for longer amounts of time to assure accuracy and data quality, repeatable, auditable linkage and for error correction and validation which makes the application of individual Rights applicable. Once data is pseudonymised for research, re-identification is neither needed nor permitted, so data subject rights such as access, rectification, restriction, and objection are limited in accordance with DPA 2018 Schedule 2, Part 6, Section 27. National and Local Data Opt Out: The Wessex SDE is responsible for applying the Type-1 opt-out and National Data Opt-Out (NDOO) within the DPE following receipt of data, as well as other opt-outs including the Wessex-specific local opt-out, prior to release of the data to any research project. The Wessex SDE is responsible for keeping opt-out status up to date through periodic refreshes including refresh of data ingestion into the DPE. Any individual rights requests received by the controller of the SDE will be considered on a case-by-case basis. Partner organisations in receipt of any individual request related to the SDE will redirect the request to UHS.
6f.	Transparency

	Informing individuals about the use of data for Wessex SDE is informed by the MoU with NHSE, detailed in the business case and the NHS HRA guidelines for sub-national SDEs. Wessex SDE's HRA approval (Annex B) requires all Data Contributors to the Wessex SDE to provide transparency about sharing their data for research use. To meet this requirement, once the Data Sharing Agreement is signed, the organisation must: • Update its existing fair processing and/or privacy notice to explicitly reflect the sharing of data into the Wessex Secure Data Environment ("SDE"). See Appendix B for template wording. • Provide a concise and accessible explanation of the SDE, detailing how patient data may be used or linked. This explanation should include links to relevant resources, including the Wessex SDE website (wessexsde.nhs.uk). • Conduct patient notification activities in a timely manner following coming into force of this agreement by prominently displaying posters, leaflets, and digital signage provided by Wessex SDE in patient-facing areas of their operational sites where data subjects are likely to encounter them. • Provide photographic evidence of these notification activities and confirm compliance with the obligations of this clause in writing to University Hospital Southampton NHS Foundation Trust (UHS). The Contributing Organisation acknowledges that individual patients or service users will not receive direct notification of the specific use of their data. However, the Wessex SDE will maintain a publicly accessible data-use register detailing approved research projects conducted within the environment, published on the Wessex SDE website In addition to the requirements of the HRA, the SDE is also required to provide further transparency about how the data is used and for what purposes. Our commitments to transparency are captured in the Wessex SDE's Transparency Policy which includes our publication and disclosure commitments. Key commitments in relation to this Data Sharing Agreement are our: • Data Capabilities Register, which is used to capture information about what data is, or could be, made available across Wessex. • Data Use Register, which provides details about all studies approved by the SDE to access data within the SDE. These registers are publicly available on our website and completed in line with NHS England transparency requirements. A copy of our transparency policy is available here: Privacy policy – WSDE. The programme supports transparency through the provision of a dedicated communication pack and a publicly accessible website that provide clear information about its purpose, data use, and governance arrangements.
7.	CONTRACTUAL MANAGEMENT OF THIS AGREEMENT

7a.	Specify any particular obligation on <u>any</u> party to this Agreement Roles and responsibilities are described in this agreement. General details concerning the roles and responsibilities are recorded in Appendix A.
7b.	Amendments and Variation Routine Review This Agreement will be reviewed annually by University Hospital Southampton NHS Foundation Trust (UHS) as Data Controller and the Wessex SDE Governance Team to ensure continued compliance with all relevant legislation, HRA and CAG approvals, and NHS data governance requirements. Right to Vary UHS, as Data Controller for the Wessex SDE, may from time to time amend or vary this Agreement to ensure alignment with: ○ any updated or amended approvals issued by the Health Research Authority (HRA) and/or the Confidentiality Advisory Group (CAG) under the Health Service (Control of Patient Information) Regulations 2002; ○ any new or amended use cases or data processing activities falling within the scope of those HRA/CAG approvals; and ○ changes to the SDE's data systems, modalities, or fields necessary to maintain consistency with relevant legislation, NHS data governance requirements, national standards, or other data protection obligations. Any such variation will take effect twenty-eight (28) calendar days after written notice is issued to all signatory Data Contributors unless the Contributor provides written notice to terminate its participation in the Agreement within that period. Notice of Variation Each notice of variation will: ○ specify the nature and purpose of the amendment; ○ reference the applicable HRA/CAG approval or regulatory change; and ○ direct recipients to the current Data Capabilities Register and Data Use Register maintained on the Wessex SDE website. A standard template notice of variation is provided at Appendix D for reference. Opt-Out on Variation

	During the 28-day notice period, a Data Contributor may opt out in full by written notice to UHS. An opt-out under this clause shall terminate the Contributor's participation in this Agreement and prevent any further use of its data within the SDE.
7c.	Ending the Agreement Any party wishing to end this agreement will be required to give 28 calendar days' notice in writing to University Hospital Southampton as the data controller. During this time a meeting of the Data Controller signatory and the SDE Governance team will be convened to review the implications of the termination.
8.	Signatories By signing this DSA, all signatories acknowledge and accept the requirements placed upon them and others within their organisations and their responsibilities under data protection legislation. Organisation: XX Signature: XXX Name: XXX Role: XXX Date: XX/XX/26 IG Contact (person responsible for compliance with this DSA): XX Organisation: University Hospital Southampton NHS Foundation Trust (Lead Controller) Signature:  Name: Christopher Kipps Role: Senior Responsible Officer, Wessex Secure Data Environment Date: 22/06/2026 IG Contact (person responsible for compliance with the DSA): XX

APPENDICES

Appendix A – Roles and Responsibilities



Appendix B – Template Privacy Notice Content

Privacy notice(s) and/or other relevant communication materials must explain what Personal Data is processed through the SDE, when and who it may be shared with and why, and how Data Subjects can exercise their Individual Rights (including objections) concerning their information being shared through the SDE. Each organisation shall be responsible for its own compliance with Articles 12, 13 and 14 (“Transparency”) of the UK GDPR. Independent and voluntary providers who share and receive Personal Data subject to an appropriate lawful basis having been established must document this within their privacy notice(s) (along all the legally required details (e.g. lawful basis, retention etc.)). Transparency obligations will be formally agreed by signing the relevant Data Sharing Agreement.

Partners can use the following template which can be added to the relevant Privacy Information around sharing data into the Wessex SSDE:

‘We are part of the Wessex Subnational Secure Data Environment (SSDE). Data sharing into the SSDE will unlock the potential of NHS data to support research, create life-saving new treatments and medicines, and bring wider benefits to patients and our NHS. NHSE have published a [simple explainer](#) on Secure Data Environments in general. Please also access the [Wessex SDE website](#) for more detailed information.’

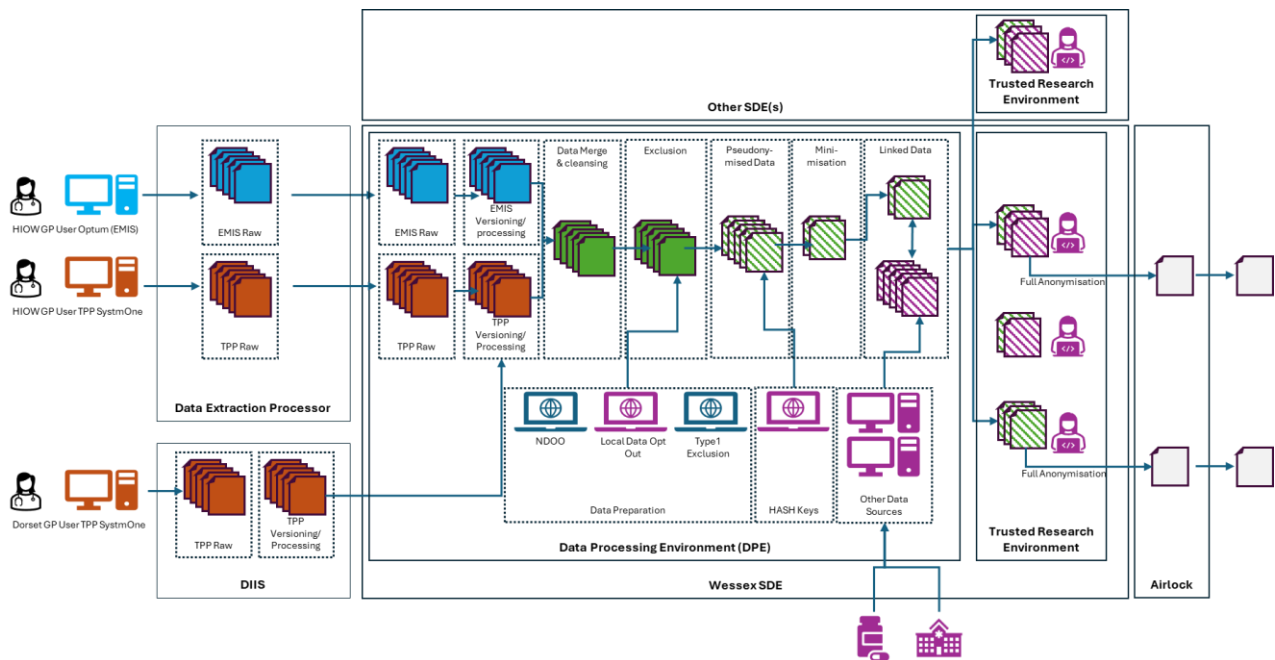


Appendix C – Acceptable Use Agreement (Academia & Commercial)



Appendix D - Template notice of variation

Appendix E



Appendix F – Accountability Matrix

	Stage 1 & 2 Capture & Extraction	Stage 3 Transfer to SDE	Stage 4 Data Processing	Stage 5 Transfer to TRE	Stage 6 Analysis	Stage 7 Output Checking	Stage 8 Release
Accountable (Controller)	GP Practices (Primary controller)	Transition point → UHS (Wessex SDE host becomes controller for processing)	UHS (Wessex SDE)	UHS (Wessex SDE)	- UHS (as SDE controller) - Research Sponsor (for study-level governance)	UHS (Wessex SDE)	- UHS (initial release decision) - Receiving organisation becomes controller for outputs
Processor	- GP system providers (EMIS, TPP) - Extraction Partners	ARO / BCP / Azure / CIRU (hosting and transfer infrastructure)	Platform providers	TRE Platform provider (CIRU)	TRE infrastructure provider	CIRU	CIRU
Risk Owner	- GP Practice Caldicott Guardian (primary) - Supported by GP Practice Data Controller / Practice Lead - Extraction Partners	- UHS Wessex SDE Technical Lead - Supported by Extraction Partner	- Information Asset Owner (IAO) – Wessex SDE GP Data Asset - Supported by SDE IG Lead / UHS Wessex SDE Technical Lead	UHS Wessex SDE Data Lead	- Data Access Committee (DAC) Chair (governance accountability) - Research Sponsor / Chief Investigator (use accountability)	CIRU	- SDE Governance Lead (pre-release) - Receiving Organisation Data Controller (post-release)
Key Risks	- Data accuracy - Lawful basis and transparency - Opt-out capture	- Secure transmission (encryption, integrity) - Unauthorised access during transfer - Data integrity in transit	- Incorrect linkage - Failure to apply opt-outs	- Dataset minimisation failure - Inappropriate data exposure	- Misuse of data - Attempted re-identification risk - Scope creep	- Residual disclosure risk - Small number identification	- Misinterpretation or misuse of outputs - Secondary disclosure risk

Annex A

User and organisational validation form

[NHS Research SDE Network Registration Service - NHS England Digital](#)

Annex B

HRA approval



24CAG0013
Supported
Outcome

CAG (IRAS ID: 334643) & REC (IRAS ID: 339034)