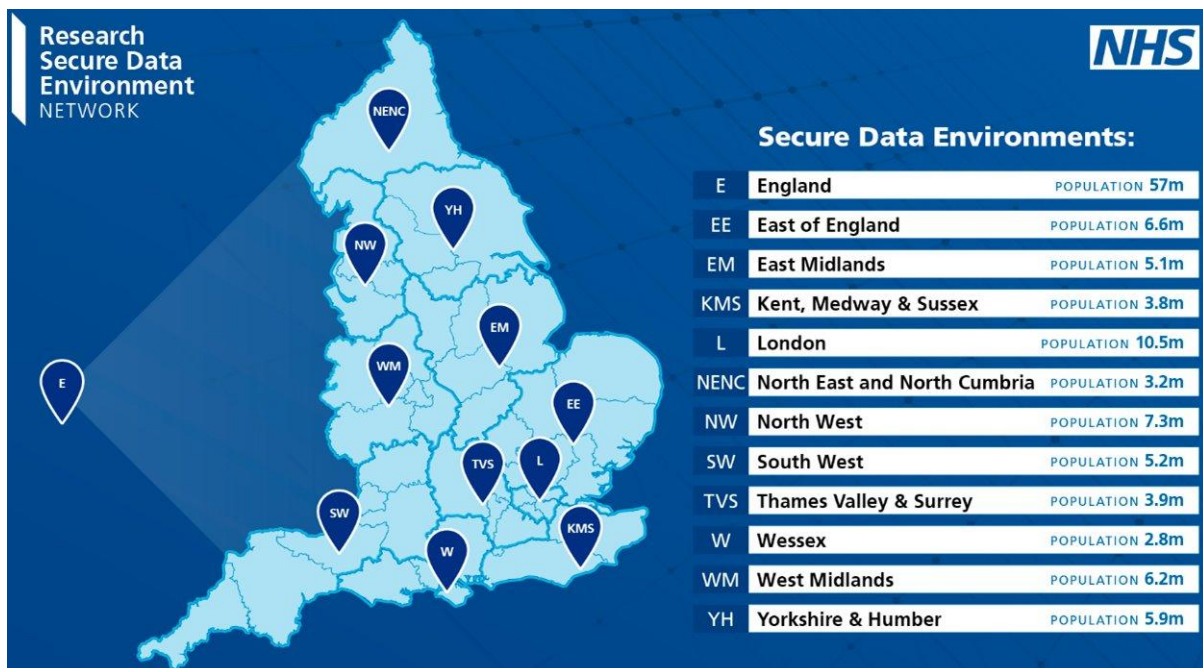East of England
SECURE DATA
ENVIRONMENT

From Privacy to Progress: The Power of Secure Data in Health Research

In the age of digital health, data can save lives, but only when it's handled with care. That's where Secure Data Environments (SDEs) come in.

An SDE is a secure, carefully controlled digital space where approved researchers can access data to carry out approved research. The NHS has created a national network of Secure Data Environments for Research and Development (R&D) to facilitate access to de-identified NHS data for research, making data as useful as possible while protecting the privacy of individuals and retaining NHS control of the data.

Research Secure Data Environment NETWORK

NHS

Secure Data Environments:

E	**England**	POPULATION **57m**
EE	**East of England**	POPULATION **6.6m**
EM	**East Midlands**	POPULATION **5.1m**
KMS	**Kent, Medway & Sussex**	POPULATION **3.8m**
L	**London**	POPULATION **10.5m**
NENC	**North East and North Cumbria**	POPULATION **3.2m**
NW	**North West**	POPULATION **7.3m**
SW	**South West**	POPULATION **5.2m**
TVS	**Thames Valley & Surrey**	POPULATION **3.9m**
W	**Wessex**	POPULATION **2.8m**
WM	**West Midlands**	POPULATION **6.2m**
YH	**Yorkshire & Humber**	POPULATION **5.9m**

The East of England (EoE) SDE was developed in partnership with the NHS and research organisations and shaped through engagement with patients and the public in the region. Its purpose is to support health research that benefits public health and patient care while keeping personal data safe. For example, understanding the trends in diseases such as heart disease or diabetes so that treatments and services can be improved for everyone.

Who oversees the EoE SDE?

Responsibility for the East of England SDE sits with Cambridge University Hospitals NHS Foundation Trust as the 'lead accountable organisation' working with Cambridge University Health Partners (CUHP) and Health Innovation East as the delivery partner.

All research projects using NHS data in the EoE SDE must be approved by a Data Access Committee. This committee includes public representatives, data, legal and

clinical experts. They make sure data is only used for research that is ethical, safe, and in the public interest. For studies that are approved, the researcher is granted access to just the data they need to answer their research questions.

How does the SDE keep data safe while supporting beneficial research?

The SDE follows strict legal and security standards, including:

- The UK General Data Protection Regulation, (UK GDPR) as part of the Data Protection Act, 2018

- ISO/IEC 27001, an international standard for information security and

- The Five Safes framework which encourages safe and responsible use of data by ensuring that measures are in place to ensure the **people** using the data, the **projects**, **setting**, **data**, and research **outputs** are all safe.

Figure 1: Five Safes Model

FIVE SAFES

SAFE PEOPLE	SAFE PROJECTS	SAFE SETTINGS	SAFE DATA	SAFE OUTPUTS
Ensures people using the data are trustworthy and trained i.e., they are approved researchers	Only approved projects which have clear benefit to public health	Data is stored in a secure and controlled environment so that it can't be misused	Data processed to protect confidentiality & minimise the risk of identifying individuals, i.e. personal/identifiable information has been removed	The results generated by the researcher must be checked before they are shared in a process called disclosure or output checking

Adapted from: The "Five Safes": A framework for planning, designing and evaluating data access solutions, Ritchie (2017)

The EoE SDE makes it possible to securely bring together information from different parts of the NHS in a way that ensures individuals cannot be identified. Strict security and privacy measures are built in, including:

Safe People

Approval: Only approved researchers from approved organisations can access the Secure Data Environment (SDE).
Verification: Two-factor authentication is used to verify user identity.

1. Safe Projects

Just the data needed to support research in the public interest: Researchers can only access the de-identified data that is necessary to answer their approved research question. They must explain each piece of data they need and justify its necessity.

Transparency: All uses of the SDE are published on the SDE website via the [online SDE Data Use Register](#).

2. Safe Settings

Security: Access is through secure virtual desktops only with no direct download, cut and paste capability, or external internet access – which prevents data being copied or moved. These systems are independently accredited to the internationally recognised ISO27001 security standard.

3. Safe Data

Anonymisation and minimisation: In the EoE SDE, researchers can only access de-identified data that has been approved for their specific use. i.e., information that has had all personal identifiers such as name and address removed. Other 'privacy enhancing technologies' (PET) may be used – for example to covert dates of birth to age-range bands etc.

4. Safe Outputs

Strict Disclosure: Only anonymised, pre-checked outputs like summaries or statistics can be shared. These are reviewed (by airlock managers) to ensure no identifiable data is released to researchers.

The EoE SDE is like a high-security lab, not for chemicals, but for data. Everything that happens inside is tracked and governed by clear rules.

Why does this matter for patients?

The EoE SDE helps improve health by:

1. Preventing illness before it starts
2. Identifying who's at risk and which treatments are likely to work best
3. Involving people in making decisions about how their data is used
4. Making care more personal and effective for everyone

It's a safe, secure way to use NHS data to support better care and help people live healthier lives, while maintaining patient privacy. By protecting privacy and supporting vital research, SDEs help turn information into better care for everyone.