

Safe Data: How the Wessex Secure Data Environment protects your privacy

The Five Safes Framework

The Wessex Secure Data Environment (SDE) works under an official government framework called the **Five Safes**. This is a set of rules used by the NHS and the Office for National Statistics to make sure health information is used responsibly.

This leaflet focuses on the **Safe Data** aspect of the Five Safes – the technical steps we take to protect your identity. Using these privacy-protecting methods is a **legal requirement** set by our regulator, the NHS Health Research Authority. You can find out more about the Five Safes framework at:

www.gov.uk/data-ethics-guidance/the-five-safes-framework

Respecting your choices (Opt-outs)

Before any information is used for research, we respect your right to choose how your data is handled:

- NHS Trusts check and apply the **National Data Opt-Out** before they send any information to us.
- When information arrives at the SDE, we check it again to make sure that your choice to opt out has been respected.
- At this stage, we also apply the **Local Data Opt-Out** for the Wessex SDE for anyone who has contacted us directly to say they do not want their data included.

To find out more about the opt-out options and your choices visit: wessexsde.nhs.uk/your-choices/

Replacing personal details (Pseudonymisation)

The main way that the SDE protects you is by removing identifiable patient information – like your name, address and NHS number – from any data before we make it accessible to researchers. The SDE's technical team replaces personal details through a process called pseudonymisation:

- We remove information that directly identifies you, such as your name and address.
- These details are replaced with a secure code.
- Because health information is stored in different places, you will have different secure codes for each NHS organisation the data comes from, such as GPs and hospitals.
- Researchers only ever see secure codes and never have access to the code keys or your real identity.
- To link these records together, each dataset has a "code key". We use this key to "unlock" the data. We then use personal identifiers – like your NHS number – to match your records accurately.
- This linking happens only in a restricted part of the SDE that is managed by the NHS and never accessible to researchers.

We use varying technical methods to code information depending on the specific needs of a study, always following official standards.

It is important to know that it is a criminal offence to deliberately try to identify someone from de-identified health data. Any person or organisation found attempting to do this would be reported to the Information Commissioner's Office for investigation and may face criminal prosecution.

Preventing re-identification

Even when direct details like names are removed, there is a small risk that someone could try to guess who a person is by looking at rare or unique health details. This is called re-identification risk.

To prevent this, the Wessex SDE uses several Privacy Enhancing Technologies:

- **Data Minimisation:** Researchers are never given your whole health record. They only see the limited pieces of information they absolutely need for their specific study.
- **Small Number Suppression:** If a piece of information applies to only a very small number of people, we hide that specific detail or round the numbers. This makes it much harder for anyone to "pick out" an individual from a group.
- **Generalisation:** We group specific details together into broader categories. For example, instead of using a specific date of birth, we might use an age range like "40 to 45 years old."

These are the main tools we use, but we constantly review our methods against the latest security standards to keep your information protected.

The final check (Safe Outputs)

Before any research results are allowed to leave the secure environment, they undergo a **human review**.

- NHS staff manually check every graph and table to make sure it is not possible to "reverse engineer" or guess an identity from the results.
- Researchers can only take out results that have been confirmed as **anonymous statistical patterns**.
- While no system can claim to be 100% anonymous, these manual and automatic checks ensure that the risk of identifying anyone is extremely low.

Find out more

You can read about our full security standards and see a list of our approved research projects at: **WessexSDE.nhs.uk**