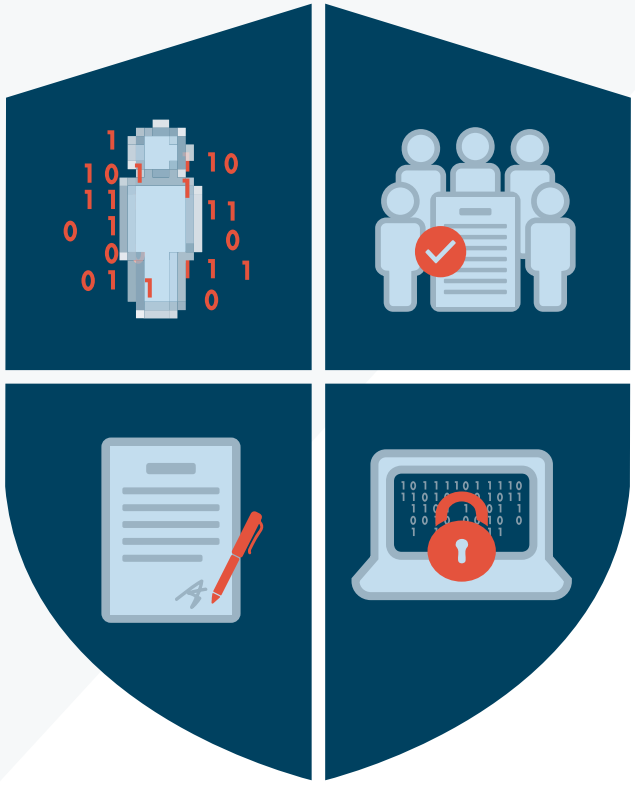
# How is data kept safe?

It is essential that patient data is kept safe and secure, to protect your confidential information.

There are four ways that your privacy is shielded:

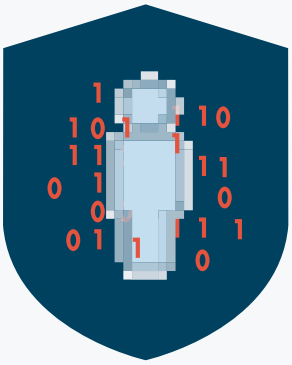
**Remove identifying information**
The best way to protect someone's information is to anonymise it, by removing details that identify a person. Anyone wanting to use patient data will only be given the minimum amount necessary to answer a question.

**Strict legal contracts**
A legal contract must be signed before data can be transferred. This sets out strict rules about what an organisation can do with the data, and has clear restrictions on what is not allowed.



**Independent review process**
Any request to use patient data must be assessed by an independent review committee, who check that the reason for using the data is appropriate.

**Robust data security standards**
Data must be stored in securely, with controlled access and robust IT systems to keep data safe.



# Remove identifying information

**How is information anonymised?**
Wherever possible, the data will be anonymised in line with guidance given by the Information Commissioner's Office (ICO Code of anonymisation). This code sets out what identifying details must be removed or masked, and the safeguards that must be followed to protect data.

**What if it isn't possible to anonymise the data?**
If it is not possible to anonymise the data, there are strict controls on how personally identifiable data can be used and stored. It can only be used if you give your permission or where required by law, and then only with robust safeguards.

# An independent review process

**What does a review committee check?**
All organisations that look after patient data will have a clear review process to ensure data is only used appropriately. There are three things that will be checked:

| WHY | WHO | HOW |
|---|---|---|
| is the data needed | is accessing the data | will the data be protected |

**What other checks are there?**

- All research applications will also be reviewed by an expert independent scientific committee.
- There are extra controls if a researcher wants to access personally identifiable information and it is not possible to ask consent. These requests are reviewed by the Confidentiality Advisory Group.

# Strict legal contracts

**What does a data sharing contract include?**

- What data will be provided, and how
- The purpose for which the data can be used
- When and how data must be destroyed after use
- The data security requirements that must be followed
- What an organisation must not do with the data:
  - data cannot be used in any way to re-identify an individual
  - data cannot be linked with any other data, unless explicitly approved in the application
  - data cannot be passed to any third parties, unless explicitly approved in the application
- The organisation can be audited to check data is being used appropriately

# Robust data security standards

**How is data protected?**

- Technology can be used to protect data, for example by restricting access (using passwords or swipe cards to control access to data), or using encryption so the data can only be read with a code.
- IT systems must be kept up-to-date to protect against viruses and hacking.
- Anyone accessing data must have appropriate training and be approved by the organisation.
- There must be an audit trail that records every time that data is viewed or used.