

Data Privacy & Security Process

10+ forms, 3+ legal contracts

Ethical approval

Assess the ethics of the research project

- What is the purpose of the research?
- Is it ethical and fair to participants?



Linkage Organisation approval

Co-ordinate the logistics of the data linkage

- What data is needed & how will the researchers ensure it stays safe & secure?
- Draft legal agreements between data owners and researchers



Public Benefit Approval

The Public Benefit & Privacy Panel controls access to NHS Scotland data

Weigh the potential benefits to the public against the potential privacy risks
[Our mission is...] to facilitate and promote ethical research that is of potential benefit to participants, science and society.” NHS Health Research Authority



Data Access Approval

Data owners set their own permission & access procedures

- National Records of Scotland control access to census, births, deaths & marriage data.
- National Research projects such as UK Biobank control access to their own databases.



Data Indexing

The data is made anonymous

- Researchers receive information in the most anonymous way possible.
- In most cases, this means that personal information, such as date of birth, are removed.
- To distinguish one person from another, the researchers uses a non-identifiable reference number



Data Linkage

Linking together anonymous data (e.g. health & census records)

An external Trusted Third Party coordinates the linkage process to ensure:

- Data owners only ever see their own data (not that of other data controllers)
- Researchers only ever see the requested data and not identifying information



Laws

Several Laws govern the work our researchers do, including:

- UK Data Protection Act 2018
- GDPR (European Union General Data Protection Regulation)



Data Protection Act 2018



Researcher Training



Researchers are trained to spot and report any risks to privacy.

e.g. when a health condition is very rare, it may be possible for an anonymous individual to be identified.



Secure Data analysis

Data is stored & analysed in a secure environment that is only accessible to the specified researchers.

For the most sensitive data this means:

- Restricted entry & CCTV-monitoring
- Nothing taken in or out
- All analyses externally checked for privacy risk