

## General Principles

- **Don't** store NHS identifiable information on home computers, laptops, hand held devices, digital cameras or other imaging equipment.
- **Don't** store identifiable information on floppy disks or CDs.
- **Don't** send identifiable information via the internet to an email address that does not end in '.nhs.uk' unless encrypted.
- **Don't** send identifiable information to individuals, who you know forward their e-mails to other e-mail addresses (potentially outside the NHS).
- **Don't** forward your NHS e-mail to a non-NHS e-mail address
- **Don't** allow persons without legitimate reasons access to the data.

## Key References

- **Research Governance Framework**  
<http://www.doh.gov.uk/research/index.htm>
- **ICH—GCP**  
<http://www.ich.org/>
- **MRC Use of Personal Data. Patient Information Advisory Group**  
<http://www.doh.gov.uk/ipu/confiden/index1.htm>
- **Information Commissioner Data Protection Act**  
<http://www.dataprotection.gov.uk/>
- **MRC Ethics Series: Personal Information in Medical Research**  
<http://www.mrc.ac.uk/pdf-pimr.pdf>

## For further information

Contact **Christine McGrath**  
**R&D Manager (Governance and Quality)**  
[christine.mcgrath@ubht.swest.nhs.uk](mailto:christine.mcgrath@ubht.swest.nhs.uk)

Bristol Royal Infirmary  
Level 1, Old Building  
Marlborough Street  
Bristol BS2 8HW  
Tel: 0117 928 3565

or

**Data Protection Officer**  
United Bristol Healthcare  
Trust Headquarters  
Marlborough Street  
Bristol BS1 3NU  
Tel: 0117 928 3730

or

**Caldicott Guardian**  
United Bristol Healthcare  
Trust Headquarters (as above)

UBHT Intranet and Internet  
websites  
<http://intranet/r&d/>  
<http://www.ubht.nhs.uk/R&D/>

**The purpose of this leaflet is to draw your attention to the DoH Research Governance Framework for Health and Social Care (March 2001) and the key responsibilities of all staff involved in research.**

# Research Governance

Essential Information for Researchers  
Data Protection in Healthcare Research

United Bristol Healthcare   
NHS Trust

## Data Protection Act 1998

The **Data Protection Act 1998** came into force in 2000. It is a legal requirement to comply with the provisions of the Act.

The Act gives legal rights to individuals with regard to how their personal data is used.

**Personal data** is all information, including images, that can identify, in isolation or in combination with other data, a living individual.

## Data Protection Principles

Personal data must be:

- processed fairly and lawfully.
- obtained and processed for specified and lawful purposes only.
- adequate, relevant and not excessive.
- accurate.
- kept no longer than necessary.
- processed in accordance with individuals' rights.
- kept secure.
- only transferred to countries with adequate data protection systems.

## Data Protection in Research

The **Lead Researcher** (or delegated person) must inform the Data Protection Officer of the use of personal data for research.

All those involved in research must be aware of and comply with the Data Protection Act.

## Caldicott

In addition to Data Protection Act, the **Caldicott Principles** as laid down by the NHS Executive must be followed by the Trust and its employees.

All patient-identifiable information, relating to living or deceased patients, is confidential and must be treated in accordance with the Caldicott Principles.

## Caldicott Principles

- Justify the purpose for using confidential information.
- Only use when absolutely necessary.
- Use the minimum required.
- Access should be on a strict 'need to know' basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.

## Caldicott Guardian in Research

Research which makes use of existing patient-identifiable data (and stored samples) must have the permission of the **Caldicott Guardian**.

## Anonymised Data

Data is considered **anonymised** when individuals cannot be identified from the information

The Research Ethics Committee must approve **all** research including research using anonymised data.

For guidance on how to anonymise the data

## Do's and Don'ts

- **Do** gain ethical approval for all research using personal data.
- **Do** gain consent from individuals to use their data, unless otherwise approved by a Research Ethics Committee.
- **Do** inform the Data Protection Officer of all research (via the R&E office).
- **Do** inform the Caldicott Guardian if necessary (see opposite).
- **Do** treat data as confidential at all times.
- **Do** anonymise data wherever possible, as soon as possible.
- **Do** password protect and back-up electronic data.
- **Do** ensure all researchers have full or honorary contracts with the Trust before allowing access to data. [In certain circumstances a confidentiality agreement only may be sufficient - contact R&E office.]
- **Do** ensure data is stored securely for a minimum of 15 years.