Research & Innovation
Research Governance Framework Factsheet

Data Protection

Data Protection Act 1998
The Data Protection Act 1998 came into force in 2000. It legislates for the control and protection of personal data generally. The more stringent requirements of the Act do not apply to some kinds of healthcare research (e.g. research using anonymised unlinked data and some epidemiological research) because of an 'exemption' clause. Adherence to this law and advice on compliance in the UK is monitored by the Information Commissioner.

Main Provisions of the Data Protection Act
Personal data, in written or electronic form, must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive for the purpose
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to countries with adequate data protection systems

Data Protection in Research
The Research Governance Framework for Health and Social Care incorporate the stipulations of the Data Protection Act and requires that in the research setting, the appropriate use and protection of patient data is paramount. All those involved in research must be aware of their legal and ethical duties in this respect. Particular attention must be given to systems for ensuring confidentiality of personal information and to the security of these systems.

What is personal information?
Personal information is all information about individuals, living or dead. For example medical records which are written or held on a computer system, images, recordings, information obtained from samples and opinions expressed about the individual.

What is Personal Data?
Personal data has a narrower definition and is more closely concerned with avoiding the possibility of identification. It is information about living people which in isolation or in combination with other data which may be available, may lead to the identification of the patient.

Confidential information in the context of healthcare is information about oneself given on the explicit or implicit understanding that it will not be disclosed to others outside the patient's care, without the patient's consent. Both the law and patients assume that this is the case when personal information is disclosed as part of clinical care.

Sensitive information refers to information about individuals which may have particularly deleterious effects if it is disclosed inappropriately. The Data Protection Act 1998 refers to "sensitive personal data" as including all information about physical or mental health or condition, or sexual life (Annex3B).

Coded data is not anonymous data. Identities are disguised by the code but the code can be easily decoded by those in control of the data. For example, an 'alphanumeric code' made up of a patient's postcode/initials and date of birth is not anonymous. Informed consent from the participants is required for this situation (except in exceptional situations where the need is waived by applying to the Department of Health).

Anonymised data is data which has been coded by others outside the research team, for example from a national database such as the Cancer Registry or a large pharmaceutical company. Permission for this data to be used in future research should be requested at the time of initial consent to registration or research.

Linked anonymised data can be decoded by the organisation supplying it to the researchers but not by the researchers themselves. For example a Care Organisation may need to link perhaps unexpected research data to a particular patient in the interests of their care. Informed consent from the patient is sometimes necessary when using linked anonymous data. The Research Ethics Committee should be consulted.

Unlinked anonymised data describes the situation where the link between the data and the person to whom it refers has been irreversibly broken. No one could use this data to identify a specific individual. Informed consent is not necessary for research which makes use of unlinked anonymised data.

Caldicott Principles
The Caldicott Principles were the result of the 'Report on the Review of Patient Identifiable Information' by the Caldicott Committee, Department of Health 1997. A recent review of the principles was carried out in September 2013. The Caldicott Guardian in each Trust is charged with ensuring that these principles are respected and acted upon. The Caldicott Principles apply in addition to the requirements of the Data Protection Act.

Principle 1 – Justify the Purpose
Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 – Don't use patient identifiable information unless it is absolutely necessary
Patient-identifiable information items should not be used unless there is no alternative.

Principle 3 – use the minimum necessary patient-identifiable information
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Principle 4 – Access to patient-identifiable information should be on a strict need to know basis
Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

Informed Consent
Informed consent for the use of personal data should be sought wherever this is practically possible and will not cause more harm in terms of distress to the patient or their family. This should be balanced against the possibility of contributing to the advancement of medical knowledge. People are usually happy to allow access to their data; it is often the omission to ask which causes offence. There is a need for more research and public debate about the levels of access to personal data the public will allow without consent. Where consent is not sought this should be justified to the Research Ethics Committee.

Practical Tips

- Where informed consent is not possible, justify this in detail to the Research Ethics Committee
- Identify the local Data Protection Officer for the Directorate in which you work
- Store all non-electronic research data in locked filing cabinets
- Make sure that the sponsors (who have access to the data) do not remove it to a country outside the EU without adequate data protection systems

- Remember that the Funders have no right to check patient records on which research is based unless they have taken on formal responsibility as 'sponsors' of research
- Any researcher from outside the NHS must have an honorary contract with the Trust before they are allowed access to data, samples or patients
- The Principal or Lead Investigator is responsible for ensuring the appropriate archiving of data when the research has finished.
- Data may need to be stored for up to 15 years or longer for research involving children. Liaise with the Sponsor or R&I department for guidance.