Guidance 2 of NHS Lothian eHealth and IM&T Security Policy

Guidance to Research Staff on Data Management Best Practice

Introduction

All staff employed within NHS Lothian processing personal data whilst carrying out clinical research are required to comply with the Common Law on Confidentiality, Data Protection Legislation (the Caldicott Principles and any other legislation, current guidance or good practice protocols supported by NHS Lothian. It should be noted that this guidance applies to all data that can identify a 'living individual', including 'anonymised' data where individuals can be identified by cross-referring to a separately held database.

Personal (patient) data

1. All personal data must be processed in accordance with the NHS Lothian Data Protection and IT Security policies.

2. All data processed during the course of a researcher's duties remains under the 'ownership' of the Data Controller. In the vast majority of cases, this will be NHS Lothian, however there are limited circumstances where the Data controller will be University of Edinburgh or there may be Joint Data Controllers. Please refer to the appended 'Data Controller' flowchart for further guidance.

3. Databases containing personal data must be registered with the Data Protection Officer.

4. Regardless of who is identified as Data Controller, all personal data must be processed in accordance with this guidance and the eight principles of the Data Protection Legislation.

5. To ensure 'fair and lawful' processing, research subjects must be provided with a 'fair processing notice' (FPN) and given the opportunity to raise any queries as part of the consent process. The FPN must include the name of the Data Controller(s), the purpose(s) for which the personal data is going to be processed and any other information required to ensure fair processing from the research subject's perspective. This may include how long the data will be held, whether...
the data is being shared with other researchers (and if so, to whom) and whether the data is being transferred overseas for collaborative purposes.

6. In the instance of overseas transfer of data, the researcher must contact the NHS Lothian Data Protection Officer for further guidance, as the receiving country must meet certain levels of ‘adequacy’. This is particularly important when transferring to non-EU countries.

7. Researchers should carefully consider the data that they hold. Identifiable data should be adequate, relevant and not excessive (DPA Principle 3). Particular care must be taken when analysing data to ensure that the underlying data cannot identify individuals. Best practice is to separate the identifiable data items from the other data, and link tables (look up table) only when absolutely necessary.

8. Where a look up table is used to identify research subjects from the remainder of the data set, it should be held securely and separately, and destroyed at the end of the project. The end of the project is defined as the length of time the data will be held in the Fair Processing Notice.

9. NHS Scotland is committed to using the CHI (Community Health Index) number on all clinical systems as a means to link across all local and national systems. This number can only be used as a patient identifier within the NHS and may only be shared with other agencies under strict protocols that must be agreed in advance of any information sharing.

10. The R&D department and/or NHS Lothian Data Protection Officer will provide best practice advice to researchers wishing to securely store paper or computerised data on completion of a research project.

11. In the event a researcher leaves their post, they must not take any personal data collected during their employment with NHS Lothian or University of Edinburgh to their new post.

**IT Security**

1. Research data must be held in a secure environment. Where practical, it should be stored on the research server provided by NHS Lothian R&D department. Alternatively, it should be stored on a secure network drive requiring password access and is regularly backed up.
2. Research data must never be exclusively stored on a laptop or PC hard drive. When it is not possible for data to be saved to a secure network environment, the following procedures must be taken:

   a. The local hard disk must be suitably encrypted. Standard password protection of software packages, i.e., Microsoft Office, does not meet the required standard.

   b. Research data must be backed-up on suitable media upon completion of the data processing.

3. Only NHS equipment, including PCs, laptops, tablets and memory sticks may be connected to the NHS network. Researchers should be aware that the NHS networks can readily identify non-NHS hardware and will take any breaches very seriously.

4. Emailing of personal information via the Internet is not permitted. This includes email sent from an NHS email account to a University email account. If a researcher wishes to send information electronically, they should seek further guidance from the NHS Lothian IT Security team for advice on suitable encryption methods and secure methods of transferring data.