PROTECTING INFORMATION POLICY

Data protection, security and confidentiality should be maintained according to the relevant Acts and legislation including University requirements, the Research Governance Framework, the Data Protection Act 1998, requirements of the Research Ethics Committees, Research and Development and Good Clinical Practice.

Please note that the statements below apply to all staff and students working in HSRU as well as away from the office (e.g. working at home). Confidential data should not be taken away from the office or accessed from home unless it is strictly necessary. Please note that data is confidential as long as it remains personally identifiable. If you DO require access to confidential data out-with the office, please discuss with your line manager or the QA Manager.

All staff must adhere to the following statements**:**

1. Access to personal data

When you are responsible for personal information about an individual (e.g. participants in a research study, an interview study, a clinical trial or your work colleagues) you must make every effort to ensure that it is effectively protected against improper disclosure at all times. Except for all essential personal identifiable information/data (e.g. consent forms; participant entry forms; digital, audio and video recordings etc.) all other data should be anonymised.

Many improper disclosures are unintentional. You should not discuss patients/study participants where you can be overheard or leave patients' records/questionnaires/letters or any other identifiable information, either on paper or on screen, where they can be seen by other unauthorised staff or the public. Earphones should be used when transcribing personal interview tapes.

2. Storage of data

For paper-based and audio/visual data, all personal information which is only collected with the permission of the study participant should be stored securely in locked filing cabinets/tambours and retained for only as long as is necessary. Identifiable and non-identifiable data should be stored separately, where possible. Access to research data should be restricted to members of the research team, unless authorised by the Principal Investigator.

Do not leave any personal information lying on your desk overnight. Even if you intend working on a document again the following morning, lock the personal information away in your desk drawer or filing cabinet/tambour. Do not leave notes about/letters from/any personal information about a person on another person's desk (e.g. if a member of the Unit is away, do not leave a letter from an individual lying on their desk waiting to be dealt with on their return). It is good practice to develop a system within a team where identifiable data, awaiting attention, will be stored appropriately.

For electronic data, all personal information should be password protected and saved in the appropriate project folder on the HSRU drive, normally S: (**not** the C:\drive). Using the project folders on the S:\ drive ensures that the data is stored on a secure server with access restricted to authorised staff working on that project. If you use a USB drive and/or other portable device that contains sensitive data, it is mandatory that it is encrypted.

When away from your desk, your computer must be locked by pressing Ctrl/Alt/Delete and select 'lock computer'. It can only be unlocked when the current user enters their password again.

3. Transmission of data

Personal information being sent or received by post should be in a sealed envelope; it must be clearly addressed to indicate who the recipient is (could be a team of people). Audio or video recordings of consultations or interviews should be labelled with unique study identifiers and sent by registered mail or courier, requiring a signature on delivery. It is good practice for the transfer and receipt of paper-based data to be documented to ensure that a clear audit trail is maintained.

Do not e-mail identifiable data unless the e-mail has been encrypted. University e-mail is not encrypted by default. It is, however, possible to send queries/information to sites provided that no identifiable data is included and patients can only be identified by a unique study number.

To transfer data securely between colleagues both inside and outside the University, researchers can use the University File Transfer Service, ZendTo which is available at https://zendto.abdn.ac.uk/. If it is necessary to send data on disc or USB stick, it should be password protected and encrypted (e.g.: 256 bit encryption with WinZip 12.0), and sent by registered post. (Please speak to the CHaRT Senior IT Manager if you need advice or need to encrypt any data. In addition, please refer to www.abdn.ac.uk/staffnet/working-here/it-security.php#panel2599 for more information on IT security).

4. Archiving

The College of Life Sciences & Medicine standard operating procedure (UoA-NHSG-SOP-021) and approval form for archiving data are available at www.abdn.ac.uk/medical/mhra/sops.php. Except for all essential personal identifiable information/data, all other data should be anonymised before archiving. Identifiable and non-identifiable physical data should ideally be archived in separate storage boxes, if appropriate. Length of retention of data will be governed by the rules and requirements of the appropriate regulatory bodies (e.g. funder, sponsor ethics committee) as well as legislation such as the EU Directive and Data Protection Acts. See also University Records Management at www.abdn.ac.uk/central/records-management/ for more information.

Any data archived in the University of Aberdeen, will go through a formal process for review and/or disposal. If you have archived data you will be contacted at the appropriate time to discuss the retention or destruction of these documents.

5. Destroying data

Confidential data must be disposed of appropriately. Audio and video tapes should be erased and physically destroyed. For paper-based information, small volumes should be shredded, larger volumes placed in confidential waste bins or bags. This includes any identifiable information such as address labels and letters. Under the EU Directive, the reasons for destruction of essential documents should be documented and signed confirmation of disposal should be obtained.

Confidential data must **never** be disposed of in a waste paper bin. Any data stored in University archives will be destroyed as per University policy (see the link above in 'Archiving' for further details).

DEFINITIONS & FURTHER INFORMATION

Several types of information are generated, obtained, stored and destroyed within the Health Services Research Unit. This includes clinical information, financial information, sensitive information and personal information.

Personal information: Information about people from which individuals can be identified.

Anonymised data: Data that is derived from/about particular individuals, from which the particular individual cannot be identified (by the recipient of the information). The name, address, and full postcode must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the patient.

Confidential information: Information obtained by a person on the understanding that they will not disclose it to others, or obtained in circumstances where it is expected that they will not disclose it. The law assumes that whenever people give ***personal information*** to health professionals/members of a clinical research team caring for them, it is confidential as long as it remains personally identifiable.

Sensitive information: The term "sensitive" is used to highlight the need for extra care in using information about mental health, sexuality, racial or ethnic origin, political opinions, religious or other beliefs, trade union membership and criminal proceedings or convictions. Note that "sensitive personal data" is defined in the 1998 Data Protection Act as including all information about physical or mental health or condition, sexual life, or racial or ethnic origin. Sensitive data can only be processed with explicit consent of the individual, being required by law for employment purposes, in order to protect the vital interests of subject or another dealing with administration of justice or legal proceedings.

All staff are under an obligation to familiarise themselves with all aspects of data protection: To meet the University Policy on Data Protection (www.abdn.ac.uk/staffnet/governance/data-protection-255.php), all staff should comply with the MRC's code on *Personal Information in Medical Research* (www.mrc.ac.uk/Utilities/Documentrecord/index.htm?d=MRC002452), and the Data Protection Act (1998; www.legislation.gov.uk/ukpga/1998/29/contents).

All staff are required to have read this document and agree to do everything in their power to uphold its principles by signing and dating the page overleaf. Please retain this copy for your records.

I have read and understood the Health Services Research Unit Protecting Information Policy (Version 5) and agree to comply with it.

Signed……... Date……..

Name …….. (IN CAPITALS)