Institute of Health and Wellbeing:

Information Governance Policy

The Institute works to the highest standards of research governance, reflecting the needs of each of our partners. Our policy has been developed in line with strict Health Research Authority best practice for data management, security and storage. The following information describes our approach to these issues; where changes to these protocols are required they should be discussed with the University project team as described in the designated project proposal.

General Principles

The following general principles of information governance are applied to IoHW research and evaluation projects:

- All IoHW projects are subject to ethical review by a University approved committee. In the case of projects falling with the remit of the Research Governance Framework, this will be an NHS Research Ethics Committee. These committees consider and advise on issues relating to the collection, transmission, storage and processing of information on a project by project basis as part of their remit.
- All approved ethical protocols must be abided by. This policy should be used to inform the applications for ethics approval.
- Where possible, IoHW projects will be planned in ways which minimise the need for University research and evaluation teams to receive Personally-Identifiable Data (PID). This includes, for example, the use of participant postcode sector (first four digits) rather than whole postcodes and age rather than date of birth.
- Where data is collected by another agency on behalf of a University project team (e.g. by an NHS Trust, GP practice or Local Authority) Personal Identifiable Data will be stripped by them at source and before transfer except where specific alternative arrangements have been agreed in writing.
- This policy complies with the Data Protection Act (1998). All IoHW staff will be trained in the Data Protection Act, and must comply with this.

Information Governance Management

The following IG management issues are applied to IoHW projects:

- All research/project active staff have clearance from the Disclosure and Barring Service and are trained to follow strict ethical practice.
- Data will be stored securely for a period of three years with a local professional archival company following the completion of a project, except where otherwise agreed with particular project commissioners. After this time it will be destroyed.

- Projects commissioned by NHS Northamptonshire are subject to NHS governance review. Responsibility for obtaining this for *evaluation* rests with project commissioners and for *research* with the research team conducting the study.

Confidentiality and Data Protection

The following principles of Confidentiality and Data Protection will be applied by IoHW staff:

- IoHW will not disclose identifiable data, or seek to obtain permission for this.
- We seek informed consent from those participating directly in our projects, except in the case of questionnaires or surveys, for which implied consent may be applied.
- Where data is collected by another agency on behalf of a University project team (e.g. by an NHS Trust, GP practice or Local Authority) participant consent should be obtained at source.
- Transcription is completed either within the University or outsourced to a professional transcription company. All work undertaken by this company remains strictly confidential and they are registered under the Data Protection Registration Act.
- Data disseminated in project reports or via academic conference presentations or journals is at all times anonymised to ensure that no individual participant is identifiable from their content.
- Client information will only be used in accordance with professional practice, the Data Protection Act, and other relevant legislation.
- All transfers of personal and sensitive information are conducted in a secure and confidential manner. Databases are password protected and staff will not use fax/email or post for the transferral of PID data.
- All new members of IoHW staff will be trained on information governance during induction.
- IoHW project staff are responsible for the following:
    - personal information is not disclosed by them either orally or in writing, to any unauthorised third party;
    - they do not access any data which is not necessary for carrying out their work;
    - personal data in paper format is kept in a secure place when not being processed;
    - personal data on computer should not be accessed or viewed by unauthorised staff or students and as such workstations should be locked or password protected when not in use;
    - Staff processing personal data for research purposes (for example, use of questionnaires) should inform the participant why the data is being collected and how long it will be retained for.

Information Security

IOHW follows the principles of information security as defined by the National Health Service. Three key issues form the basis of our practice in this area:

- Information must be secured against unauthorised access – **confidentiality**;

- Information must be safeguarded against unauthorised modification – **integrity**;
- Information must be accessible to authorised users at times when they require it – **availability.**

These principles are put into practice using the following key standards:

- All hardcopy project data is stored on University premises in locked cupboards or cabinets;
- Unauthorised access to University equipment and records is prevented; staff offices are locked when not in use and computers are only accessible with a personalised password;
- All information assets that hold, or are, personal data are protected by secure password;
- Electronic data files will be stored on a secure University server in a project specific file;
- Hard copy raw data must be transferred to University premises securely within 24 hours, unless by prior arrangement with the Institute Manager;
- Electronic raw data must be transferred to the University server within 24 hours, unless by prior arrangement with the Institute Manager;
- Equipment used to store raw data in the process of collection off site, e.g. audio recorders and laptops, must be stored securely, accessible only to the designated researcher;
- Original data will be deleted from recording hardware immediately after download. Audio recordings must be deleted no later than 6 months after the completion of each project;
- Raw data must only be accessed for analysis on University premises or from University secure servers;
- The University will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident to it as an organisation or to any of its locations or services;
- All University employees (substantive and temporary) are expected to be familiar with, and to comply with, the Information Protection (Security) Policy at all times;

Associated University Policies[1]

- University of Northampton Data Protection Policy;
- University of Northampton Records Management Policy;
- University of Northampton Research Data Policy.

Contacts

- Institute of Health and Wellbeing Manager (katie.jones@northampton.ac.uk)
- University Records Manager (phil.oakman@northampton.ac.uk)
- Research Support Librarian (miggie.pickton@northampton.ac.uk)

[1] For copies of these policies, see the Records Management and Information Compliance collection in TUNDRA