Security Protocol for the use of digital recorders in connection with The University of Sheffield Doctorate in Clinical Psychology Training Programme

This document presents the security protocol to be applied to the collection, handling and storage of qualitative data obtained and processed in relation to conducting research within the Doctorate of Clinical Psychology Training Programme (DClinPsy), University of Sheffield. It also includes some additional notes for trainees planning to use encrypted digital recorders in a placement setting.

These should be read in conjunction with the 'instructions for using digital voice recorders' which are available on BlackBoard.

Using encrypted digital recorder for research

Overarching principles

Trainees should be familiar with the University of Sheffield's Research Ethics Policy**,** and Note no. 4: Principles of Anonymity, Confidentiality, and Data Protection are particularly relevant here (https://www.sheffield.ac.uk/research-services/ethics-integrity/policy)

Clearly, details of data collection tools/equipment, storage arrangements, and destruction time points should be specified in the research protocol and these aspect of the protocol must have been subject to ethical and governance scrutiny prior to the collection of data. As such the proposed plans for data collection must concur with local requirements of the site where data is being collected. Therefore, trainees are required to liaise with local NHS research governance offices in the preparation of their research protocol, in planning this and other aspects of their proposed research.

In any event, Trainees should ensure that all aspects of data collection and management are in line with The Data Protection Act (see http:/ico.org.uk)

Trainees who record interviews with participants are required at all times to apply due diligence to the security of the digital recorder that they use and any field/process notes which they make to accompany an interview. *Such items should be treated as one would treat case notes and only transported between sites with appropriate permissions and should not be left unaccompanied where they might be vulnerable to being lost or stolen*.

Minimum requirements

Equipment and data capture

1. All equipment must be approved by the research site and relevant research governance office. The department has some equipment that may be loaned but you might need to budget for equipment from the funds available to support your research (if you need to purchase equipment – details must be provided on the costing form within the proposal and you must demonstrate that it is suitable for use at the proposed research site).
2. Encrypted digital recorders are required for use as they provide enhanced security and have a record of being used in the NHS. The department has some DS5000. *These recorders are also likely to be acceptable to NHS sites but it is the trainee's responsibility to check that this is the case*.

3. In the interview itself it is always preferable to ask participants not to name specific people or sites so that the data file will already be anonymous to some degree.
4. Trainees using digital recorders will have the option (and are encouraged to use this) to delete any remaining identifying information present prior to sending recordings for transcription.

Transportation

1. This must be done by a secure mechanism as detailed below.

Storage and destruction

1. It is strongly recommended that anonymous audio files are stored on the trainee's personal space on the University server and labelled with an appropriate code to link them to the original participant and consent form.
2. If they are to be stored on a personal computer or laptop then they should be stored in an encrypted folder and each file password protected.
3. Unless agreement has been explicitly obtained to keep original audio files these should be destroyed following successful completion of the course.
4. Transcripts should be stored following completion of the course as per the site file guidelines.

Transcription

1. If an individual professional transcriber is to be used then they must have signed a confidentially form (available on BlackBoard) and be on our approved list. If a company is being used you must provide details in your research proposal of the confidentiality agreement that they have with their transcribers (this information is usually available on company's websites or via email). This information must be retained on the site file.
2. If proposing to use a transcriber you must consult the costing guidelines regarding how to manage payment.
3. Files should always be encrypted and password protected before transportation and on the computer of the transcriber. Pre encrypted audio files should be transported to the transcriber's computer via an encrypted memory stick. These can be borrowed for brief periods from the Unit.
4. Audio files may be uploaded directly to a transcribing company that provides a secure facility/portal (details of this should be contained in the research proposal and is usually clear from providers websites).
5. Once the recordings have been transcribed they are to be saved by the transcriber as password protected word documents and transferred to either a secure memory stick or emailed to your University address. The password should be sent separately or provided by telephone. Internet companies will either send you transcriptions as password protected documents or may require you to log into a secure site (please provide details of this in the protocol).
6. Contracts with transcribers are to stipulate that the transcriber is required to securely erase all data from their computer. Again details on internet companies' procedures in relation to disposal of files must be provided in the proposal.

Supervision

1. Typically supervisors and others (as specified in the protocol) will require access to the transcripts. Supervisors may listen to interviews where the audio files have been secured for transportation i.e. are on an encrypted piece of hardware. Only email anonymised password protected transcripts to your supervisor(s)/collaborators.

Adherence to this protocol

1. Any actual or suspected security incidents or breaches of this Protocol are to be reported to the supervisor and to the Director of Research Training at the earliest opportunity.
2. The research tutors and research support officer will periodically audit adherence to this policy.

Additional notes for trainees in a placement setting

Trainees wishing to use digital recording equipment on placement must ensure that their proposed plan concurs with local requirements of the site where recordings are being made, prior to any recording taking place.

Individual trusts have their own policies on the use of digital recording equipment and any such local policy must be followed. It is unlikely that any trust would allow the use on unencrypted digital recorders, however policies around the use of encrypted recorders vary between trusts.

In any event, as with research, trainees should ensure that all aspects of data collection and management are in line with The Data Protection Act (see http:/ico.org.uk).

The unit has a small stock of encrypted digital recorders and memory sticks which may be lent to trainees on a 4 week loan (which can be renewed if there is no waiting list). As the stock is small trainees working at the same placement location may need to share a digital recorder and memory stick. ***However, trainees should first check with their placement supervisor whether recording devices are available for use within the service.*** When completing the case study, it may be useful to record all sessions with the client if possible, but this not necessary for the purposes of the assignment as long as sufficient material is available to illustrate the key points being made.