Guidelines for management of audio recordings in research at USN.

(These guidelines have been developed by the Department for Research and Internationalization)

It can be very easy to identify individual persons in audio recordings, and the more sensitive the information contained in the recording, the more important it is to take appropriate security measures.

Reduction of the number of personally identifiable factors in audio recordings

The Norwegian Centre for Research Data (NSD) usually recommends that the interview subjects are briefed ahead of time to avoid providing information that can lead to identification of themselves or others. Examples include information about geographic locations or workplaces that the interview subject can be associated with should not be mentioned unless they are absolutely necessary for the data assembly. In some situations you can consider pseudonymizering of the recording through the use of voice changing technology (additional software/hardware required).

Recording equipment and the use thereof

NSB recommends against the use of private equipment (such as smartphones or other recording devices) for recording, storing, or archiving, and any such use must be cleared with the managing institution (in this case, USN). USN does not currently have a shared lending system for recording equipment, and have therefore developed these guidelines which can be referred to if privately owned equipment is used.

In most cases the data contained in the recordings is such that there is very little risk of personal identification of the subjects, in which case the recordings can be stored on privately owned equipment on the condition that these are treated in a responsible manner. This includes the equipment being protected with a pin code or password; the recording should not be shared to anyone not involved in the project, and the recordings should be deleted from the equipment as soon as they are no longer needed, for instance once they have been transferred or encrypted (see below).

You must be aware of your actions when working with recordings; for instance do not leave the equipment unattended in places where you do not have complete control of it, lock the office in which the equipment is stored, and do not loan the equipment to others.

Items with internet or mobile network access (such as mobile telephones, smartphones or tablets) should not be used for audio recordings if very sensitive information is to be collected. We recommend the use of a Dictaphone with an external memory card, for example Olympus DM-70 or Sony PX4700, where a memory card of 4 GB should be sufficient.

Encryption

The recorder can be used for several projects at the same time if they are used by the same person. However it is recommended that the recording is transferred to an encrypted unit (USB drive or external hard drive) or that the interview is transcribed as soon as possible so that the original recording can be deleted from the dictaphone or mobile telephone.

Please see the attached document regarding encryption of data.

The memory cards or disks in recording equipment usually cannot be encrypted directly.

If a recorder is shared by several researchers at the same time, it shall only be used for one project at a time. The recordings will be transferred to encrypted storage and deleted from the recording device as soon as possible after recording. If the recorder is to be used in a new project then a new memory card must be utilized. Used memory cards or disks must be destroyed upon completion of the project; they cannot be reused.

Recording devices shall be stored in locked cabinets or drawers when they are not in use; see information below regarding the storage of audio recordings. Other encrypted recording equipment shall also be stored in a locked cabinet.

Editing and transferring audio recordings from one storage device to another

Audio recordings with medium to high levels of sensitivity, and which have not been anonymized, shall not be edited or saved on a PC connected to the internet.

Audio recordings can be edited on stationary or portable PCs that are either permanently or temporarily disconnected from the internet. Temporary disconnection includes unplugging of internet cables and/or turning off wireless access (Wi-Fi). If the recordings are temporarily stored on a PC you must be certain that the files have been completely deleted before the machine is re-connected to the internet.

Permanent disconnection means in this case that it is not possible to connect the PC to the internet.

The degree of sensitivity of the material determines whether or not the computer should be temporarily or permanently disconnected from the internet. The sensitivity of the data increases with increasing data volume (number of observations, amount of data collected), but is also dependant upon the contents of the data:

- The expectation of confidentiality can be high in cases where there is information about health, wellbeing, or working conditions.
- Confidentiality is also expected when the data includes information about the private life of the subject (home, recreation, etc.).
- “Special categories of personal data” have a higher degree of sensitivity. These include but are not limited to health status, race, religion, union membership, political affiliation, genetic or biometric data, or information about sexual relationships or orientation.
- Be aware that the sensitivity level of “innocent” data CAN increase if the material is combined with other sources. Therefore all personal information should be treated as confidential.

You must ensure that unauthorized persons are not in the room when editing of sensitive information is taking place.

Deletion of audio recordings after completion of the project

Data must be anonymized or deleted after the project has ended, which means that the audio recordings must be deleted.

Data which has been transferred to a memory card or USB drive cannot be completely deleted in an unrecoverable fashion. After the project has been completed these must be destroyed if they will not be reused by the same person or people. When these are reused by the same person or people the program CCleaner can be used to remove the data from the card or drive.

Should long-time storage of audio recordings be necessary (for follow-up in long-term studies) approval from NSD and REK must be attained.

Storage of audio recordings

Audio recordings can be stored on encrypted USB drives or encrypted external hard drives. Employees at USN have access to an encrypted hard drive on their employer-issued PC, and non-sensitive audio recordings can generally be stored there.

USB drives or external hard drives should be stored in a locked cabinet or filing cabinet in a room with limited access. If the cabinet stands in a room that the public has access to, they should be stored in a safe or cabinet with two doors that are difficult to break into. However if the cabinet is in a room with limited access a regular lock should suffice.

If the raw data needs to be kept for a long time then the storage cabinet should be fireproof and stand in a room with smoke detectors and either fire extinguishers or sprinkler systems in the same room.

If the recordings are to be stored in your office it must be locked when you are not present.

The recordings can also be stored at the Service for Sensitive Data (TSD). Contact forskningsdata@usn.no for more information about this service.

Archiving and long-term storage of recordings

If there is a need to store the data for future use, the audio recordings can be archived by NSD; please see their websites regarding archiving. They provide a description of how the data can be prepared for archiving and include an overview of preferred file formats and the relevant documentation that should be included, and specifies which forms should be filled out and signed by the sender.

Instructions especially for the health and care sectors: (Videos in Norwegian)

Veileder video-, lyd og bildeopptak i helse- og omsorgssektoren
(https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-video-lyd-og-bildeopptak-i-helse-og-omsorgssektoren ehelse.no).

Attachment: Encryption of data

This memorandum is a short description of methods of encrypting data to secure it against being lost during transport, and for securing data saved on external drives during fieldwork.

Any data that includes personal information or sensitive personal information must be secured against loss in transport or when being stored outside of the IT-service providers that would normally manage such data. Transport of data includes sending of data via email or temporary storage in cloud-based services. Transport of data can also include temporary storage on USB drives with the intention of transferral to secure storage for analysis.

The methods described in this memorandum are NOT replacements for the laws and regulations governing the collection and use of personal or sensitive personal information. Any project which collects and analyses sensitive personal must be approved.

The methods described in this memorandum are meant to secure data assembled by students during transport. The data shall be given to the students' advisor(s) for secure storage on USNs IT-infrastructure.

Encryption of files

Encryption shall be used to secure data against loss. There are several methods of encryption available; USN uses the AES 256 method. AES stands for **Advanced Encryption Standard** and **256** is the length of the encryption algorithm key. The key length indicates the amount of resources needed to use the encryption. This site provides more information about AES.

The contents of a file encrypted with AES is opened with the same password that is used to encrypt them.

The password should be sent by a different means than the data in order to avoid it being intercepted. The password can be shared by SMS or orally, but should **by no means** be sent in the same email as the encrypted data.

There are several free tools that support AES 256 encryption. Two of the most stable for Windows or Mac OS are:

- for MS Windows - 7-zip
- for MacOS - Keka

It is important that you read the user instructions for the tool you use so that you are certain that you are using AES 256.

Encryption of USB drives

USB drives are not secure. It is therefore recommended that two separate drives are used to protect against losing the data should one fail.

If the data to be transported on the USB drive is encrypted before they are stored on the drive then the drive itself does not need to be encrypted. However if the data itself has not been encrypted then the drive must be. Encryption of the drive must be performed using MS Windows Bitlocker.

Hvis data som skal transporteres på minnepenner er kryptert før de lagres på minnepennen er det ikke nødvendig med kryptering av selve minnepennen. Minnepennen skal krypteres dersom data som skal lagres på minnepennen er ukryptert. Kryptering av minnepenner skal gjøres med MS Windows Bitlocker.

Files on a Bitlocker-encrypted drive can be read on MacOS using this app. The free version of the app provides only the possibility to read the files, not to edit them; however the paid version allows both reading and editing Bitlocker-encrypted USB drives.

USN-administered PC clients

Data traffic between USN-administered PCs and USNs data centre are end-to-end encrypted. The hard drive on all USN-administered PCs are automatically encrypted during the initial setup process. Employees engaged in short-term field work kan therefore safely store data on the PC itself; however this does not secure against loss should the machine malfunction. Data should be copied to the P: (M:) drive during the field work. If a network is not available the data can also be backed up on an encrypted USB drive.