Procedure for processing personal data in student and quality assurance projects in health research at VID Specialized University

Approved by the Research Committee on 27 August 2019.

Information: *As, there exist no official translations of Norwegian laws into English, all hyperlinks to Norwegian laws in this document are to the Norwegian language website www.lovdata.no.*

1. Scope and definitions

1.1 Scope

This procedure concerns the processing of personal data in medical and health research as described in the Norwegian Health Research Act. The purpose of the procedure is to ensure that all research ethics and data protection considerations are met. Note that not all health-related projects fall under this definition. If you are unsure whether your project is subject to the Health Research Act, you can consult the Regional Committees for Medical and Health Research Ethics' website.

1.2 Definitions

Personal data:

The EU's General Data Protection Regulation (GDPR) defines personal data as 'any information relating to an identified or identifiable natural person, ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Processing of personal data in health research

'Processing' is defined as any purposive use of data concerning a natural person's health, such as collection, recording, compilation, storage or distribution or a combination of these, see the Personal Health Data Filing System Act, section 2 b.

Anonymized data

This is data that cannot be linked to individuals by either the data controller or other parties.

De-identified data

'De-identified' data is data from which personal identifiers such as names, national identity numbers and other unique identifiers have been removed, such that the data can no longer be linked to an individual. An individual's identity can only be revealed if the data that was removed is re-introduced. The data must be processed in such a manner that once the serial number has been removed, it is anonymous. De-identified data can be categorized as anonymous if the scrambling key file is removed.

2. Apportionment of responsibility

The apportionment of responsibility in VID is stipulated in VID's Procedure for processing personal data in research and student projects.

3. Responsibility of the project manager

Note that for master students, the supervisor is the project manager. PhD students are project managers for their own project.

3.1 At project start-up:

- Define the intended use of the research data.

- Prepare a consent form and information letter in accordance with the relevant requirements in the Health Research Act, section 13. A template is available on the Regional Committees for Medical and Health Research Ethics' website.

- Apply to the Regional Committees for Medical and Health Research Ethics (REC) for approval of the research project and notify the Norwegian Centre for Research Data (NSD) of the project. Click on this link to access NSD's online notification form. Quality assurance projects do not need REC's approval.

- In collaborations with researchers from other institutions, the partners must decide who has the formal processing responsibility. The collaboration must be formalized in an agreement that covers, among other things, the apportionment of responsibilities and funding, the hierarchy of responsibility, who is the initiator of the project, use of data, the principles of ownership and an explanation of why the research data is not openly accessible where this is the case. VID has devised its own agreement template. The project manager must familiarize him/herself with applicable procedures for the processing of personal data at partner institutions.

- Assess whether there is a need for a *data protection impact assessment* (DPIA). VID has drawn up a checklist for this assessment. Contact VID's data protection officer: personvernombud@vid.no. Note that it is NSD that performs the data protection impact assessment in collaboration with the individual researcher.

- If the project involves the transfer of personal data to countries outside the EEA, the project manager must contact the data protection officer at VID: personvernombud@vid.no.

- Safeguard confidentiality. The project manager must ensure that all project members who are subject to the duty of confidentiality sign a non-disclosure agreement and that this is securely stored. Note that the duty of confidentiality may be revoked if consent is obtained from the data subject, ref. the Health Research Act, sections 13-17 and 17-19; or if a dispensation from the duty of confidentiality is granted, ref. the Health Research Act, sections 28 and 35.

- Conduct a risk assessment. The project manager must ensure that the project undergoes a risk assessment. Relevant aspects of the risk assessment are:
    - method for controlling access to research data,
    - whether research data has been satisfactorily de-identified, and
    - whether the scrambling key, where one exists, has been satisfactorily secured.

3.2 During execution of the project:
During the execution of the project, the project manager is responsible for the following:

- Ensuring that research data is collected as provided for in the consent form and in the information submitted to NSD and REC. Personal data must *always* be processed in accordance with VID's Procedure for processing personal data in research and student projects.

- Ensuring that research data is kept secure at all times and that only project members have access to it. The project manager must maintain an overview of who has access to the research data at any given time. The project manager is responsible for terminating access rights when necessary. This applies to data stored electronically and in hard copy. The project manager must, upon request, know who has access to the data.

- Ensuring that active research data is stored and handled in accordance with VID's procedures for this.

- Ensuring that project members receive the necessary training in data security.

- Ensuring that instances of non-conformance are dealt with as they arise, in accordance with VID's non-conformance management procedure.

- Ensuring that the research project undergoes regular security audits. This is particularly important in long-term research projects. The frequency of security audits is determined according to the size, scope and duration of the research project, the number of research participants and the complexity of the data protection challenges in the project.

- Safeguarding the right of access. Requests for access must be answered without undue delay, and within 30 days.

- Ensuring that health and personal data are not disclosed to unauthorized parties. Health research data is disclosed in accordance with the consent form from the register or the approval from REC.

- Ensuring that personal data is not transferred to countries outside the EEA. If the project involves the transfer of personal data to countries outside the EEA, the project manager must notify VID's data protection officer: personvernombud@vid.no.

- Processing the withdrawal of consent: if a research participant withdraws his/her consent to participate in a research project, the project manager must ensure that research on the data subject's biological material or research data ceases. Data subjects who withdraw consent have the right to request that the material is destroyed and that any mention of them in the research data and research file is erased within 30 days. This right does not extend to cases where:

    - the material or processing of the material forms part of another biological product, or
    - the research data has already been included in completed analyses.

Data erasure decisions must be made by the project manager, but the decision can be appealed to REC. All erasures of data must be documented and traceable. However, if there are grounds to assume that using the material/data would be of major benefit to society and the field of research, application may be made to REC to continue this work.

Research file

- The project manager is responsible for creating a scrambling key and generating a research file where necessary, including ensuring that the degree of personal identification in the research file corresponds to that reported to REC. The project manager must ensure that both the research file and the scrambling key file are secure. The project manager must ensure that incorrect information is corrected, outdated information is updated and incomplete information is completed. The project manager must ensure that all data that is recorded, modified or erased in the research file is logged and checked.
- In multicentre studies, parties must sign a reciprocal agreement to safeguard the quality and integrity of the research file. These agreements must be in writing.

Storing the data

- Identifiable and de-identified personal data must be stored and processed in VID's systems or in systems that are covered by a data processing agreement with VID. Directly identifiable personal health data must be stored in encrypted form or in areas with a high level of security, such as VID's research server. In addition, VID has also entered into an agreement with the Services for sensitive data (TSD). If you want to use TSD, contact the pro-rector for research.
- Permission must be obtained for the use of privately-owned equipment (home computer). Data stored on such equipment is subject to the rule that personal data must always be encrypted.
- The main rule is that data containing health and personal data must be de-identified. Research data and identifiable components (the scrambling key) must be stored separately and in such a way that only project members have access.
- Paper-based research data that is not anonymized must be stored in a locked cabinet at all times. If paper-based research data is stored in a cabinet in an office, the office must be locked when no one is there.
- Paper-based scrambling keys must be stored in a locked cabinet separately from personal and health data. If the personal data and scrambling key are both stored electronically, they must be stored separately.
- Project members should not normally have access to any scrambling keys. In cases where they do have access, the data will be classed as directly identifiable personal data as opposed to de-identified data. This entails stricter requirements for processing and storage.

Transfer of data

- All data transfers must be encrypted. Contact the IT service on your campus for assistance with encryption.

3.3 Upon conclusion of the project:

- At the end of the project, the project manager must ensure that the research data is anonymized or deleted, unless REC and NSD have approved or required continued

storage. The project manager must ensure that copies of the data are handled in the same way. Full anonymization is equivalent to deletion. Data is usually anonymized by deleting the scrambling key. If this is not done, all directly and indirectly identifiable personal data must be removed from the research data.

- If the data is to be deleted, ensure that this is carried out in an appropriate, complete and secure manner in accordance with the requirements imposed by, for example, REC, NSD or the data supplier, or that information has been provided about this when obtaining consent. When data is deleted, it must not be possible to reverse the process. This means that all information on storage media must be deleted so that it is not possible to recreate research data or any research file. Full anonymization is equivalent to deletion.

- Source data or other research data and documents must not be deleted if the regulatory bodies have open cases relating to the research project, or if the project manager or project members are the subject of an inquiry being conducted by the National Commission for the Investigation of Research Misconduct or a local body concerned with research misconduct.

Retention of research data after completion of project

- If research data is to be retained for longer than provided for in the original consent, the research participant's consent must be obtained again. The project manager can apply to REC for dispensation in connection with prolonged storage without consent.

- If personal data is to be retained after the project is completed, the project manager must inform NSD of this in the initial notification of the project to NSD. The project manager is responsible for explaining why retaining the data is in the interests of society, the purpose of retaining the data and any negative consequences this could entail for the relevant data subjects. The data must be stored in accordance with VID's guidelines and assessments.

Duty to retain data

- In some contexts, a requirement to retain research data may be imposed for the purposes of retrospective controls and inspection.
- REC may require the research data to be retained for up to 5 years after completion of the project.
- Contractual provisions may also require a longer storage period. A requirement may be imposed for certain health data to be retained under the Regulations on Patient Records or the Archives Act.
- When students or project members leave the project, the project manager must ensure that research material obtained or accessed by them is securely stored.
- Source data or other research data and documents must not be deleted if the regulatory bodies have open cases relating to the research project, or if the project manager or project members are part of an inquiry being conducted by the Committee on Scientific Misconduct.

Comment:
This procedure does not include provisions on drug testing and clinical trials of medical devices because, at the time of approval, VID was not involved in this type of research. Researchers who conduct such research must first contact the data protection officer: personvernombud@vid.no.