Code of conduct for information security
www.normen.no

Published with the support of:
Helsedirektoratet

Information security in research projects

Supporting document
Fact sheet no 40
Version: 1.1
Date: 15 Dec 2010

Target group This fact sheet is particularly relevant for:	☐ Supplier ☐ ICT manager ☒ Researcher ☒ Project manager	☒ Head of security/Security coordinator ☐ Organization manager/management ☒ Person or body responsible for research	☐ Staff/employee ☐ Data processor ☒ Privacy protection ombudsman
Responsibility	The researcher must contribute to ensuring information security in research projects.		
Execution	Requirements and regulations concerning information security apply to all research projects.		
Purpose	Provide an overview of information security requirements applicable to research projects and in particular of requirements the researcher is responsible for following up.		
Scope	Used for all research projects authorized by the Health Research Act.		
Authority	• The Health Research Act • The Personal Data Act • The Personal Data Regulations		
References	• Code of conduct for information security • Guidelines: Data protection and information security in research projects in the healthcare and care sector • The Regional Committees for Medical and Health Research Ethics (REK): www.etikkom.no		

No	Activity/Description
1.	**Information security in research projects – background** Research will in the main take place in organizations that are required to comply with the Code a) To the extent the Health Research Act does not provide otherwise, the supplementary provisions of the Personal Data Act and regulations issued in pursuance the latter Act apply b) Research projects in the healthcare and care sector often entail the use of health and personal data in a manner that requires that personal data protection and information security is maintained in a satisfactory manner. The measures implemented to ensure information security must be documented in the application to REK c) Health and personal data may only be processed and used if a so-called authority to process data is present, i.e. a statutory authority for collecting and using information and biological material for a specific purpose. d) Research projects must have prior approval from REK. Prior approval is sufficient authority for processing health and personal data. e) All research projects must have a person or body responsible for the research and a project manager. The project manager is a physical person having day-to-day responsibility for the research project.
2.	Paragraph 2 provides information for the individual researcher (insofar the researcher and the project manager are separate persons). a) Guidelines for ‘Data protection and information security in research projects in the healthcare and care sector’ have been developed. The guidelines describe the requirements concerning information security prior to the commencement of the project, while the project is on-going, and at the close of the research project

No	Activity/Description
	b) Some of the measures described below may have been implemented centrally, in the organization's management system and thus be the responsibility of the organization c) Prior to the commencement of the research project the project manager must, amongst other things: – apply to REK for prior approval for the research project – establish procedures for information security – enter into necessary agreements – develop consent forms and informational material for research subjects – ensure the duty of secrecy – establish rules for the use of data
3.	**When carrying out the research project the individual researcher must:** a) familiarize himself with the procedures of the control system for information security b) comply with the duty of secrecy in order that personal data protection is ensured c) ensure that the purpose of collecting health and personal data is in accordance with the declaration of consent d) comply with the rules for the use of the re-identification key, conforming with the prior approval from REK e) follow the procedures for securing the research file f) participate in information security training (e.g. familiarizing himself with the security directive) g) follow the procedures for the use of equipment, in particular portable computing equipment h) follow the procedures for the use of removable storage media (e.g. memory sticks) i) follow the procedures for the transfer for research data abroad, when necessary j) follow the procedures if the research subject demands access to research data k) follow procedures if the research subject withdraws his consent l) not use traditional e-mail solutions for transmitting identifiable and de-identified research data, see Fact sheet 33
4.	**Requirements concerning information security at the close of the research project** a) The prior approval from REK will indicate that research data may be stored in connection with the research being carried out b) If research data are to be stored beyond the period for which approval was originally given, consent must be obtained from the research subject. The project manager may apply to REK for a dispensation from this requirement. c) The deletion of research data must be done in an appropriate, complete, and secure manner. Deletion is carried out by: – destroying or overwriting storage media, the destruction of re-identification keys, etc. Storage media include handwritten notes, CD-ROMs, ZIP disks, magnetic tape, memory sticks, etc. Please note that backup, the research file, and re-identification keys also have to be destroyed – anonymization through the deletion of the re-identification key