Code of conduct for information security
www.normen.no

Published with the support of:
Helsedirektoratet

Documents in the information security management system

Supporting document
Fact sheet no 3
Version: 4.0
Date: 12 Feb 2015

Purpose	To give the data controller and the person or body responsible for research an overview of the most important procedures in the information security management system.		
Responsibility	The organization’s management and the person or body responsible for research are responsible for the organization having the necessary procedures in the information security management system.		
Execution	Information security management system procedures must be developed prior to the processing of health and personal data.		
Scope	The scope of the procedures shall be adapted to the nature, activities, and size of the organization.		
Target group This fact sheet is particularly relevant for:	☒ Organization manager/management ☒ Person or body responsible for research ☒ Project manager – research ☒ Head of security/Security coordinator	☐ Staff/employee ☐ Researcher ☒ Privacy protection ombudsman	☐ ICT manager ☒ Data processor ☐ Supplier
Authority	• The Personal Data Regulations chap. 2. • The Health Research Act section 6. • The Patients’ and Users’ Rights Act chap. 5 • The Patient Records Act sections 22 and 23		
References	• The Code of conduct for information security, chap. 3.2. • Fact sheet 2 – Information security management system		

The below overviews cover elements which may form part of an information security management system. For recommendations concerning the structure of an information security management system see Fact sheet 2 – Information security management system.

The overview is divided into three parts: management, execution, and review documents.

It is recommended that the information security management system is integrated into the organization’s existing management system. Areas in which procedures might already exist that can be expanded with a view to information security could include:

- Nonconformity handling
- Confidentiality declarations
- Audits
- Management review

By *procedure* is meant a description of a predetermined sequence of specific actions to be taken in particular circumstances. In the management system such procedures must be documented in writing.

1. Management documents
- Overriding objectives for the use of information technology - Description of the organization of security - Overview of the processing of health and personal data, including the purposes behind such processing and the legal authority for the processing - Security objectives and strategy - System overview and classification of systems

1. Management documents

- ICT security directive

2. Execution documents:

<u>The organization shall develop:</u>

- An overview of the organization’s partners, data processors, and suppliers
- Configuration diagram of the information systems and technical descriptions of the configurations
- Procedures for configuration control
- Description of the solution for protection against destructive computer applications
- Procedures for the creation and maintenance of a register of authorizations
- Procedures for incident registration
- Rules for password management
- Backup procedures
- Use of Norsk Helsenett (the health net)
- Rules regarding the physical security of rooms and areas

- Procedures for obtaining informed consent
- Procedures for providing the data subject with access to his or her own health and personal data
- Procedures for taking care of the right to opt out
- Procedures for providing information to the data subject concerning personal data privacy rights
- Procedures for the correction of health and personal data
- Procedures for the deletion of health and personal data

- Procedures for ordering, changing, and deleting user accounts
- Procedures for handling printouts containing health and personal data
- Procedures for the storage of documents containing health and personal data
- Procedures for the destruction of documents containing health and personal data
- Procedures for information security training
- Procedures for the use of the information systems
- Duty of secrecy declarations from new employees
- Procedures for duty of secrecy and user declarations from others who will have access to health and personal data
- Procedures for the release of health and personal data to third parties
- Procedures related to the duty of reporting or applying for a licence (to/from the Data Inspectorate)

<u>The organization should develop (as needed):</u>

- Procedures for the use of a data processor
- Procedures for research on health and personal data
- Procedures for access control
- Agreements for interorganizational access to personal health data
- Agreements concerning collaboration on personal health data filing systems for therapeutic

2. Execution documents:

purposes

- Procedures for the disclosure of personal health data for the purposes of quality assurance and training
- Emergency procedures for manual operation
- Procedures for the handling of removable data storage media
- Procedures for the use of computer networks
- Procedures for the use of wireless technology
- Procedures for the use of portable computing equipment
- Authentication requirements when accessing health and personal data using portable equipment
- Procedures for the use of standard messages to communicate health and personal data
- Procedures for connecting to suppliers for remote access
- ICT supplier requirements concerning servicing and maintenance
- Messaging communication containing health and personal data
- Duty of secrecy statements and authorization for remote access for internal ICT consultants
- Duty of secrecy statements and form for authorizing remote access for service employees

3. Review documents

- Risk assessment plan
- Procedures for carrying out risk assessments
- Risk assessment results
- Procedures for following up risk assessment results
- Procedures for handling nonconformities
- Results from nonconformity handling
- Procedures for management review (at minimum conducted annually)
- Minutes of the management review
- Plan for carrying out security audits (at minimum conducted annually)
- Security audit procedures
- Audit reports
- Procedures for following up security audit results