Code of conduct for information security
www.normen.no

Published with the support of:

Helsedirektoratet

Information security management system

Supporting document
Fact sheet no 2
Version: 3.0
Date: 12 Feb 2015

Purpose	• Documenting an overview of specific and practical activities the data controller shall execute in order to control the organization in terms of information security. • Form the basis for implementing necessary security measures in the individual organization in relation to relevant threats that may have an impact on the processing of health and personal data, ensuring that the processing of health and personal data is handled in accordance with Chapter 2 of the Personal Data Regulations.		
Responsibility	The management of the organization is responsible for creating and introducing an information security management system.		
Execution	An information security management system shall be established when processing health and personal data.		
Scope	All organizations in the healthcare sector shall establish an information security management system. The scope of the management system shall be proportionate to the organization's size and the volume of health and personal data processed.		
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 security regulations in the annotated Personal Data Regulations, December 2000, The Data Inspectorate, Part I, Introduction, section 3. • The Patient Records Act sections 22 and 23		

References	• Code of conduct for information security, chap. 4.1 Information security management system
	• Guidelines available at www.normen.no
	  ○ Data protection and information security for pharmacies
	  ○ Data protection and information security for GP practices
	  ○ Data protection and information security for dental care organizations
	  ○ Data protection and information security for psychologists, physiotherapists, manual therapists, and chiropractors
	• Fact sheet 3 – Documents in the information security management system
	• ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements		

The information security management system shall ensure that personal data protection and security becomes a continuous process and is taken care of in a systematic and documented manner. The scope of the management system shall be proportionate to the organization's size and the volume of health and personal data processed. Incorporating the management system into an existing quality assurance system is recommended.

The below example consists of management, execution, and review sections.

The management section includes the management's requirements concerning data protection and information security and describes the organization's overriding objectives. It further describes the organization of the security and the individual roles within the organization responsible for tasks at various levels. As a starting point for the organization's work with data protection and information security an overview of the organization's processing of health and personal data is developed.

The execution section contains all the organization's detailed rules and requirements for data protection and information security. These must satisfy the requirements of the management section. The rules and requirements apply to the management, individual employees, and the individual responsible for information technology.

The review section contains the review mechanisms that will be used to assess whether all the requirements have been satisfied and whether all procedures have been followed.

Example of the **contents** of an information security management system

1. Management section
    a) Overriding objectives for the use of information technology
    b) Security objectives and strategy (see the Code of Conduct chaps. 4.2 and 4.3)
    c) Description of the organization of information security (see Fact sheet 1)
    d) System overview and system classification
    e) Overview of the data processing, including the purposes of and authorities for such processing (see Fact sheet 13)
    f) Acceptable risk level (see Fact sheet 5)

2. Execution section
    a) Procedures describing all rules and requirements for data protection and information security (see Fact sheet 3)
    b) Documentation of security measures
    c) ICT security instructions
    d) Training

3. Review section
    a) Risk assessment (see Fact sheet 7)
        i. Risk assessment plan
        ii. Procedures for carrying out risk assessment
        iii. Handling the results of the risk assessment
        iv. Procedures for following up risk assessment results
    b) Security audits (see Fact sheets 6 and 6b)
        i. Plan for carrying out security audits (must be carried out at least annually)
        ii. Procedures for carrying out security audits
        iii. Processing audit reports

iv. Procedures for following up security audit results

c) Handling of nonconformities (see Fact sheet 8)
    i. Procedures for handling nonconformities
    ii. Results from nonconformity handling
d) Management review (see the Code of Conduct chap. 6.4)
    i. Procedures for management review (must be carried out at least annually)
    ii. Processing the management review minutes
    iii. Procedures for following up action plans decided by the management

In the above example the execution section appears very limited, but in reality the execution section constitutes the most extensive section, as it must contain all procedures for the processing of health and personal data.

Using Fact sheet 3 – Documents in the information security management system as a basis for determining the procedures that must, at a minimum, form part of the management system is recommended.