Code of conduct for information security
www.normen.no

Published with the support of:

Helsedirektoratet

Security audits

Supporting document
Fact sheet no 6
Version: 4.0
Date: 12 Feb 2015

Purpose	The purpose of conducting security audits is: • To confirm that necessary security measures have been taken in relation to the results of the risk assessments that have been carried out • Evaluating whether the security measures are sufficient • Confirming compliance with laws and regulations concerning information security • Ensuring that established procedures for security are being followed and are fit for purpose		
Responsibility	The organization's management is responsible for security audits being carried out. The data processor has an independent responsibility for its own security audits.		
Execution	To be conducted regularly, at minimum annually		
Scope	All organizations that process health and personal data are obliged to conduct security audits. Security audits must be adapted to the 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 section 2-5 • The Patient Rcords Act section 23		
References	• The Code of Conduct for information security, chap. 6.1 Security audits • Fact sheet 6b – Security audits – checklist		

The management of the organization is responsible for ensuring that security audits are carried out. In smaller organizations the general manager should carry out the security audits in collaboration with other persons filling roles related to security and computer system operations. In larger organizations the practical aspects of the audit may be conducted by e.g. the head of security/security coordinator or the privacy protection ombudsman. It is emphasized that the use of an external auditor is not a requirement.

The results of the security audit must be documented and shall be reviewed during management review. Additionally the implementation of corrective measures in relation to any nonconformities that have been discovered must be considered subsequent to every audit. Any identified nonconformities must be dealt with as specified in the procedures for handling nonconformities. That all nonconformities have been dealt with must be confirmed at the annual security audit.

The scope of the security audits must be adapted to the size and needs of the organization, and must cover all areas that are relevant and of significance in ensuring satisfactory information security. Carrying out a periodic series of smaller audits covering individual areas that together cover all relevant areas is recommended. One security audit may for example cover:

- The physical security of areas used for the processing of health and personal data
- Procedures for the review of incident registers
- Procedures to be followed following the resignation or termination of an employee
- Interorganizational access to personal health data
- Review of entries in the register of authorizations

The data processor must carry out a security audit of its own processing of health and personal data. In order that the data controller may be in compliance with the duty to ensure that the information security is satisfactory the data processor should provide the data controller with the results from its security audits. Arrangements are made for this in the data processing agreement.

In order to carry out a security audit satisfying all the requirements of the Code of Conduct Fact sheet 6b – Security audits – checklist may be used. The fact sheet may be used to develop audit lists, for example by following the fact sheet's division into four separate areas.