Code of conduct for information security
www.normen.no

Published with the support of:

Helsedirektoratet

Security requirements and security documentation in ICT projects

Supporting document
Fact sheet no 37
Version: 2.1
Date: 15 Dec 2010

Target group This fact sheet is particularly relevant for:	☒ Supplier ☒ ICT manager ☐ Researcher ☒ Project manager	☒ Head of security/Secuirty coordinator ☒ Organization manager/management ☐ Person or body responsible for research	☐ Staff/employee ☒ Data processor ☐ Privacy protection ombudsman
Responsibility	The data controller will normally delegate responsibility for ensuring that projects are carried out with satisfactory information security to the project manager.		
Execution	Carried out from the planning stage/commencement of the project and until it is integrated into ordinary operation.		
Purpose	Ensure satisfactory information security and good security documentation in projects intended to change or implement new ICT solutions. Ensure that security solutions and documentation are transferred to the operating environment at the close of the project.		
Scope	All projects intended to implement/change/extend an ICT solution which includes the processing of health and personal data.		
Authority	• The Personal Health Data Filing System Act section 16 • The Personal Data Regulations chapter 2		
References	• Fact sheets nos 6, 9, 10, 14, 15, 16, 20, 24, 25, 26, 34, 38, and 43 • Code of conduct for information security Chapter 3.3, 5.3.3, and 5.8		

In this fact sheet 'project' refers to projects such as the introduction of a new patient records system or new functionality in such a system and not research projects.

No	Action/Execution
1.	**Security requirements and security documentation at the commencement of the project** a) Requirements concerning confidentiality, integrity, availability, and quality are basic requirements that must be complied with at all times (cf. the Code): - The project must document the overriding requirements concerning confidentiality, integrity, availability, and quality in the solution - The project must in cooperation with the system owner ensure that acceptance criteria are set (in regard to uptime, response time, capacity, etc.) which shall apply to the solution the project is to introduce/change/extend - The requirements concerning information security must be seen in conjunction with the solution's criticality and acceptance criteria - Risk assessment must be carried out prior to the introduction of the solution. This must be performed as early as possible in order that it is possible to change the solution's specification based on the results from the risk assessment - The project must clarify the consequences of the introduction of the system, e.g. dependence upon other systems, the need to change the infrastructure and the consequences of this b) The project manager must contact the head of security/security coordinator in the organization to inform and discuss with him the planned solution in order that it may be included in the security management's 'portfolio'. Larger projects should consider having a separate security coordinator reporting to the project manager c) If the organization has a privacy protection ombudsman he shall be informed/involved when the planned solution includes the processing of health and personal data

No	Action/Execution
	d) The project manager should review already existing similar solutions and former projects in order to take advantage of existing knowledge and lessons from experience e) The project manager should ascertain whether the project and/or the planned solution requires a licence from the Data Inspectorate (should be done prior to the commencement of the project/introduction of the solution. The privacy protection ombudsman (in organizations that have one) shall assist in this. f) The project manager must ascertain whether the planned solution gives rise to a duty to inform patients concerning the processing of health and personal data, and, if necessary, obtain consent, cf. paragraph 5.3.3 of the Code
2.	**Security requirements of the technical and functional solution** a) The requirements concerning functional and technical security must ensure the overriding requirements developed in accordance with paragraph 1 (cf. Fact sheet 3) b) The security requirements must take any performed risk assessments into account, in order that the solution complies with the given acceptance criteria that apply to the solution c) The requirements concerning the functional and technical solution must be adapted to the kind of solution in question. Relevant areas where requirements should exist are (for several of these areas separate fact sheets have been developed): - External communication (cf. Fact sheets 16 and 24) - Architecture (cf. Fact sheet 20) - Access control (cf. Fact sheet 14) - Incident registration (cf. Fact sheet 15) - Storage and deletion (cf. Fact sheet 25) - Wireless technology (cf. Fact sheet 26) - Passwords and password management (cf. Fact sheet 31)
3.	**Security documentation for technical and functional solution** (cf. paragraph 3.3 of the Code) a) The security documentation must be stored for a minimum of 5 years b) Incident registers for the use of the solution (authorized use, attempts at unauthorized access, etc.) shall be stored for a minimum of 2 years
4.	**Security requirements and security documentation in relation to the preparation for inviting tenders** a) The security requirements that have been developed (cf. sections 1 and 2) regarding the confidentiality, integrity, availability, and quality of the solution must be included in the request for tender b) That the tenderer must specify how it is to comply with the requirement must be made explicit in the invitation to tender c) Requiring the supplier to conduct a risk assessment in relation to the solution in question, or to disclose the results of previous risk assessments, should be considered d) Requirements concerning the testing and auditing of the solution must also be included, in order that the organization can be certain that the solution fulfils the set requirements. For systems that include information exchange (messages) approval through the Test and approval scheme of KITH must be required, where relevant e) The supplier's ability to comply with the security requirements shall be one of the criteria on which special emphasis is placed when choosing a supplier
5.	**Security requirements and security documentation in the agreement with the supplier** a) The agreement must ensure that the supplier complies with the requirements of the Code, cf. paragraph 5.8 of the Code. b) The agreement with the supplier shall encompass and regulate the relevant security requirements (cf. Fact sheet 38) c) Requirements concerning the testing of the delivery shall be part of the agreement d) The right to audit the supplier's ICT solution shall be part of the agreement e) The agreement shall ensure that the supplier supplies security documentation and

No	Action/Execution
	provides fast and necessary support during the start-up phase f) When testing using real data the Code shall be complied with as if the system were in ordinary operation. This entails, amongst other things: - An agreement must be made with the data processor (cf. Fact sheet 10) - Agreements with other external parties must regulate the security of the project - The duty of secrecy must be complied with by all parties - Use of test data (cf. (Fact sheet 43)
6.	**Security requirements and security documentation when transferring the system into production and administration** a) Describing responsibilities b) Training operational personnel and users that will make use of the solution (cf. Fact sheet 9) - Competence requirements for adopting the solution - Any need for superusers or equivalent - Training user support - Satisfactory training of users and operational personnel - Training shall be performed using training data unless patient consent has been obtained for the use of real data (cf. paragraph 5.3.3 of the Code) c) When terminating the project the following minimum documentation must exist: - Operating procedures - Security documentation for the solution (overview of configuration, etc.) - Reports from security audits - Relevant agreements with suppliers, data processor, etc. - Overview of the data processed during the project period (incident registers, accesses, etc.) - Authorizations assigned in the system during the project period - Report to/licence from the Data Inspectorate, if needed d) When transferring from project to ordinary operation copies of health and personal data which no longer will be used for their intended purpose (e.g. testing and training) must be deleted in a satisfactory manner (cf. Fact sheets 25 and 34) e) When transferring from project to ordinary operation one must ensure that the implemented solution and relevant security documentation become part of the 'portfolio' of the security management

Sketch of project security and documentation requirements