Norm for informasjonssikkerhet
www.normen.no

Published with the support of:

Helsedirektoratet

Information security when performing testing

Supporting document
Fact sheet no 48
Version: 1.1
Date: 15 Dec 2010

Purpose	Ensuring that the person performing testing has sufficient knowledge to ensure confidentiality, integrity and availability.		
Responsibility	The organization's manager shall ensure that information security is maintained when testing is performed. The practical day-to-day responsibility may be delegated to e.g. the ICT manager and the head of the department in which testing is taking place.		
Execution	Regularly and at least annually.		
Scope	All testing of systems that are used for processing health and personal data.		
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 Health Data Filing System Act section 16.		
References	• The Code of conduct for information security • Guidelines for remote access for maintenance and updates between supplier and health organization • Fact sheet 43 – Use of test data in systems containing health and personal data • Framework for authentication and non-repudiation in electronic communication in and with the public sector, April 2008: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf (in Norwegian only).		

'***Test manager***' refers to the person responsible for the execution of the test.

'***Test user***' refers to the person carrying out the operational aspects of the test (either employee of the data controller, or of the supplier/data processor)

The preparation of test data is detailed in Fact sheet 43 – Use of test data in systems containing health and personal data.

No	Action
1.	**Test procedure** a) The test manager shall develop a procedure that must at minimum cover the below points
2.	**Duty of secrecy** a) The test manager shall keep a record of the test participants, and of compliance with the duty of secrecy b) The test user shall on his own initiative ensure that the duty of secrecy has been formalized either through the employment contract or through a special form that is signed prior to the commencement of the test
3.	**Separate testing role with its own user name and password** a) The individual test user shall not use his ordinary authorization, but shall instead be assigned a personal role with its own user name and password b) In incident registers the test user shall be registered as its own role for testing purposes, in order that analysis of the incident registers will not appear to show that the test user has performed illegal acts (cf. the Personal Health Data Filing System Act section 13a and the

No	Action
	Health Personnel Act section 21a).
4.	**Level 4 for remote access authentication** a) The test user shall use level 4 for authentication from a home office for access to health and personal data that are used for testing (cf. Fact sheet 29 – Home office (in Norwegian only) and Fact sheet 36 (in Norweigan only) – Remote access for maintenance and updates)
5.	**Securing portable equipment** a) Use of portable equipment shall be done in compliance with the security requirements of Fact sheet 18 (in Norwegian only)– Securing portable equipment, wherein two of the main requirements are encryption of storage media in accordance with current requirements and the use of security level 4 for access to health and personal data
6.	**Securing the wireless network** a) Use of wireless technology be done in compliance with the security requirements of Fact sheet 26 (in Norwegian only)– Securing wireless technology, wherein one of the main requirements is the encryption of data communications b) The requirement applies both to the use of a wireless network at the workplace and at a home office (cf. Fact sheet 29 – Home office) (in Norwegian only)
7.	**Storing printouts** a) The test user shall lock away printouts containing health and personal data b) This may be done by locking the office or by locking the printouts in a separate drawer or cabinet
8.	**Destroying printouts** a) The test manager shall provide information concerning the location and use of document destruction equipment b) The test user shall destroy printouts once they have served their purpose
9.	**Securing memory sticks, CDs, and other removal storage media (herein referred to as 'memory stick')** a) A memory stick used for storing test data, files containing health and personal data, etc., shall not be removed from the workplace b) Memory sticks shall be stored in the same manner as printouts c) Memory sticks encrypted in line with current requirements may be removed from the workplace d) Non-encrypted memory sticks must be deleted in accordance with an approved deletion solution (see Fact sheet 34 – Storage media management, in Norwegian only) **c)** Memory sticks containing health and persona data shall be so labelled
10.	**Physical security of testing area (office, home)** a) When performing testing outside the regular workplace the rules concerning the use of a home office shall be complied with (cf. Fact sheet 29 –Home office, in Norwegian only)
11.	**Use of e-mail** a) E-mail shall not be used for sending health and personal data
12.	**Describing errors and shortcomings** a) Errors and shortcomings shall in the main not be described using identifiable health and personal data b) If errors and shortcomings are described using identifiable health and personal data the data files shall be secured in the same manner as health and personal data and printouts as described above
13.	**Reporting nonconformities** a) Every nonconformity with established procedures shall be reported as a nonconformity in accordance with the established procedures for handling nonconformities (cf. Fact sheet 8 – Handling nonconformities)