Code of conduct for information security
www.normen.no

Published with the support of:
Helsedirektoratet

Risk assessment

Supporting document
Fact sheet no 7
Version: 3.0
Dato: 12 Feb 2015

Purpose	Document that the data controller has implemented adequate measures and that the processing is conducted within the level of acceptable risk. The organizations are obliged to evaluate the probability and consequence of security breaches, and to base the security work on the results of such evaluations measured against the acceptable risk level.
Responsibility	The organization’s management is responsible for a risk assessment being carried out in relation to the processing of health and personal data.
Execution	The risk assessment shall be carried out prior to the commencement of the processing of health and personal data, and in connection with changes to the processing that may have an impact on security.
Scope	All organizations within the health care sector must conduct risk assessments. Risk assessments shall be adapted to the organization’s size and the scope of the processing of 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 Data Regulations section 2-4. • The Regulations relating to interorganizational access to personal health data section 5
References	• Risk assessment of information systems. The Data Inspectorate, Updated: 15 Feb 02, Reissued: 6 March 09 • The Code of conduct for information security, Chapter 6.2 Risk assessment • Fact sheet 5 – Level of acceptable risk • www.difi.no with risk assessment model

No	Activity/Description
1	**Planning** a) The management shall develop and adopt a plan for risk assessment in in relation to the processing of health and personal data b) Carrying out several smaller risk assessments, rather than a large and extensive one is recommended where possible. This provides a better overview, and the individual risk assessment may be concluded and appropriate measures planned and implemented.
2	**Preparing for a risk assessment** a) Obtain an overview of the processing of health and personal data b) Choose the area that is to be assessed (processing, interorganizational access to personal health data, IT system, technical solution, etc) c) Prepare, and, if necessary, update the basis for risk assessment, in order that all participants have the same understanding of the area to be assessed - Information flow to render visible how health and personal data are being processed - Configuration diagram of the technical solution d) Preparing proposals concerning threats and unwanted incidents that the working group should consider with regard to processing, process flow, and configuration map e) Establish a working group for carrying out the risk assessment. The composition of the group depends on what is to be assessed. It is especially important that daily users of the IT system are involved when the use of IT systems is to be assessed

No	Activity/Description
	f) Adapt the scale of probability and consequences with regard to the level of acceptable risk
3	**Carrying out the risk assessment** a) Inviting participants to bring forward unwanted incidents they desire assessed b) The group should go through, and, if necessary, adapt the process flow or configuration diagram c) Adapt the scale of probability and consequence in line with the group's assessment. The use of a unified internal scale system is recommended. In that way the information security management system becomes an integrated part of the organization's management systems. d) Document the risk assessment of each individual unwanted incident in line with the scale, consequences, and the magnitude of the consequences, calculate risk (probability multiplied with consequence), existing and proposed measures (NB! Evaluate one unwanted incident at a time) (see the form for risk assessment below). The use of a projector is recommended, in order that all participants may observe what is being documented e) Indicate if the incident will have an impact on confidentiality, integrity, and availability, in order that a comparison with the predetermined level of acceptable risk is made easier.
4	**Evaluating and recommending new measures** a) Evaluate risk with regard to the determined level of acceptable risk (see Matrix – evaluating risks below) b) Prioritize measures where the risk is greater than the level of acceptable risk c) Develop a plan of action setting out which measures should be implemented when, and who is responsible for doing so. It is important to distinguish between emergency and long-term measures.

Example

The example on the next page shows a suggested form for risk assessment, not the process described above.

In the first example on the next page the risk has been determined as being 8 (probability multiplied by consequence). The matrix below has been taken from *Fact sheet 5 – Level of acceptable risk*, and shows the connection between the level of acceptable risk and the determined risk. The level of acceptable risk in processing health and personal data has been set to 6. The calculated risk of 8 thus exceeds the acceptable risk level, with the consequence that measures must be implemented in order to bring the risk down to an acceptable level (suggested measures are shown in the table on the next page).

Probability	4 Probable	🟨	🟨	🟥	🟥
	3 Possible	🟨	🟨	🟥	🟥
	2 Less probable	🟩	🟩	🟨 6[1]	🟨 **8**
	1 Improbable	🟩	🟩	🟨	🟨
		1 Insignificant	2 Moderate	3 Serious	4 Critical
		Consequence			

Table 1 – Evaluating risks

[1] Level of acceptable risk

Examples of risk assessment forms

Example 1

RISK ASSESSMENT

Organization: Dentist Gliset	
Assessed by: Peder Aas	**Date: 12 Feb 2015**
The purpose of the risk assessment:	Availability and confidentiality

Situations considered (unwanted incident/scenario)		**Probability**				**Consequence**				**Risk level** Probability × consequence
		1 = Unlikely	2 = Less likely	3 = Possible	4 = Likely	1 = Insignificant	2 = Moderate	3 = Serious	4 = Critical	Low risk, e.g. risk < 5 Corrective measures not needed. Medium risk, e.g. between 6 and 8 Corrective measures must be considered. High risk, e.g. risk > =9 Corrective measures must be taken.
1.	Server containing both current patient records and the backup is stolen from the dental office	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☐ 2	☐ 3	☒ 4	☐Low risk ☒Medium risk ☐High risk
2.	All data are not backed up prior to the installation of a new version of the electronic patient record	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☐ 3	☒ 4	☐ Low risk ☐ Medium risk ☒ High risk
3.	Patient identity numbers and personal health data are sent via email	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐ Low risk ☐ Medium risk ☒ High risk

Description of corrective measures *(In order of priority)*		**Significance/ Comment**	**Item no above**
1.	Develop procedures for the use of email and provide training in the relevant rules for all employees: sending full personal identity numbers and personal health data via an ordinary email system, either internally or externally, is prohibited	This is a high-frequency risk and the measures will have a significant impact	3
2.	Developing procedures ensuring that a full backup of all data in the electronic patient record is taken prior to the installation of a new version of the system		2
3.	Place the server in a locked room.		1

Example 2

Violation of level of acceptable risk: C=Confidentiality **I**=Integrity **A**=Availability

No	Violation of	Cause / Threat	Unwanted incident	P	Co	R (P×Co)	Possible consequences	Existing measures / Suggested measures	Person responsible / Deadline
1	C, A	Portable computer being stored insecurely in a car or during travelling. Portable computer holds health and personal data.	Theft of portable computer holding health and personal data.	2	4	8	a) Unauthorised access to the complete set of health and personal data b) Interruption to the processing of health and personal data on portable equipment	**Existing measures** a) None **Suggested measures** a) Encryption of portable equipment storage media b) Backup of data stored on portable equipment c) Possible ban on the processing of health and personal data on portable equipment	
2	C	User lacks training	User sends an SMS informing a patient that a specific medicine has arrived at the pharmacy. The medicine indicates the patient’s diagnosis.	2	3	6	a) Violation of the duty of secrecy	**Existing measures** a) Procedures for training new employees **Suggested measures** a) Tighten procedures ensuring that new employees receive training b) Require individuals to sign a document confirming that they have received training	

No	Violation of	Cause / Threat	Unwanted incident	P	Co	R (P×Co)	Possible consequences	Existing measures / Suggested measures	Person responsible / Deadline
3	I	GP practice burgled Server not secured	Server containing the electronic patient record (including backup) is stolen	1	4	4	a) Unauthorised access to the complete set of health and personal data b) Provision of patient care interrupted	**Existing measures** a) None **Suggested measures** a) Secure server in locked room b) Establish backup procedures requiring that the backup is stored separately in a locked and fireproof location	
4	I, A	Backup contents not tested	Backup is discovered to contain no data when an attempt is made to restore the electronic patient record from the backup to the server	1	4	4	a) Provision of patient care interrupted b) Patient records contain errors	**Existing measures** a) None **Suggested measures** a) Establish procedures for reviewing backup contents b) Establish procedures for periodically testing that restoring from backup is possible	
5	C	Printer is placed in public area	Visitor (patient or other individual) takes a printout directly from the printer	2	3	6	a) Unauthorized access to health and personal data	**Existing measures** a) None **Suggested measures** a) Place the printer in a secure area b) Acquire technical solution requiring users to authenticate before printouts may be collected	

No	Violation of	Cause / Threat	Unwanted incident	P	Co	R (P×Co)	Possible consequences	Existing measures / Suggested measures	Person responsible / Deadline
6	A	System configuration is changed without configuration control Inexperienced individuals carry out software updates	A new version of the electronic patient record is installed, but the system does not work	1	4	4	a) Provision of patient care interrupted	**Existing measures** a) None **Suggested measures** a) Establishing procedures for configuration changes, including a requirement that restoring the previous version of the software must be possible	
7	C	Decommissioned equipment is not securely stored Unauthorized individuals have access to computing equipment containing health and personal data	Computing equipment containing health and personal data ends up in a landfill	1	4	4	b) Unauthorised access to the complete set of health and personal data	**Existing measures** a) None **Suggested measures** a) Establishing procedures for decommissioning computing equipment b) Ensuring that equipment that is to be decommissioned is stored securely	