Code of conduct for information security
www.normen.no

Published with the support of:
Helsedirektoratet

Creating a message communication solution

Supporting document
Fact sheet no 16
Version: 3.0
Date: 1 Dec 2011

Target group This fact sheet is particularly relevant for:	☒ Supplier ☒ ICT manager ☐ Researcher ☐ Project manager	☐ Head of security/Security coordinator ☒ Organization manager/management ☐ Person or body responsible for research	☐ Staff/employee ☒ Data processor ☐ Privacy protection ombudsman
Responsibility	The organization's management is responsible for ensuring that message communication takes place in accordance with the Code.		
Execution	When implementing solutions for message communication.		
Purpose	That health and personal data are transmitted in accordance with the requirements concerning confidentiality, integrity, availability, and quality.		
Scope	All organizations that are to exchange health and personal data.		
Authority	The Personal Data Regulations, sections 2-11, 2-12, and 2-13.		
References	• Information concerning national message standards at www.kith.no and PKI at www.difi.no (in Norwegian only) • The Address register at www.nhn.no • Fact sheet 37 – Security requirements and security documentation in ICT projects		

No	Action/Execution
1	**Consider the consequences of implementation** - Decide whether the new communications solution should be connected to other ICT systems and the possible effects of any such connections - Evaluate whether other critical systems will be dependent upon the new system/whether the new system will be dependent on any other systems (e.g. catalogue services, security services, etc.) - Evaluate whether an existing communications channel can be used for the implementation or whether the implementation leads to the opening of a new communications channel
2	**Evaluate the information security of the communication party** Health and personal data may only be transferred to parties satisfying the statutory requirements concerning information security. If the organization complies with the requirements of the Code this will be satisfactory – if not, this will need to be clarified in other ways.

No	Action/Execution
3	**Risk assessment** When implementing a new message communication solution a risk assessment must be performed. The risk assessment shall determine whether the implementation will entail a need for security measures, cf. Fact sheet 7 – Risk assessment. The risk assessment should, amongst other things, consider risks related to: - The opening of security barriers for communication in and out of the organization - Securing information while it is being transmitted - The risk of unintended disclosure of health and personal data - The risk that application receipts are not received - Non-repudiation - The risk that the sender’s duty of secrecy is breached when the message is received because internal personnel with no role related to patient follow-up gain access to the message - The risk of messages being sent to the wrong recipient or not reaching the intended recipient, e.g. because of insufficient support for correct addressing - Risks associated with a lack of message monitoring - Risks associated with a lack of available competencies for user support and troubleshooting
4	**Preparation of documentation and securing of adequate competencies** Satisfactory documentation must exist before the solution is put into operation and transferred from project to the line. This entails, amongst other things: - Ascertaining whether users of the ICT system and operating personnel have received training to ensure that information security will be addressed - Ascertain whether the ICT system has been documented in such a manner that the system/operations manager can maintain information security (discover weaknesses, install the correct security updates, etc.) - Establishing procedures for the monitoring of message traffic and the handling of nonconformities - Ensuring adequate competencies are available for troubleshooting and user support
5	**Enable the electronic addressing of messages** - Establishing procedures for the recording and updating of addresses in the NHN Address register for own services or persons. The addresses must conform to the standardization developed within the organization’s area of operation (municipality/health trust), provide the sender with a robust solution that to the least possible degree depends on individuals and internal organization, and contribute to messages being delivered as directly as possible to the relevant recipient. - Ensure that the electronic addresses of relevant communication partners are easily available to employees when they are going to send a message, and that these are not easily confused with other addresses.
6	**Managing PKI certificates** - Acquire and install organizational certificates for the organizations - Acquire and install any personal certificates - Registering any external partners the organization will collaborate with, and installing their certificates - Implementing procedures for updating the certificates of the organization and any partners when these expire

The table below provides an overview of some current electronic interaction standards and requirements.

Area	Information
National message standards	The national standardization body for messages develops national standards for messages in the health, care and social sector. Existing standards shall be complied with. For several messages an arrangement has been made for acceptance testing of the messages whereby a supplier will receive approval of its implementation.
Electronic signature	An electronic signature ensures the authentication of the sender, integrity, and traceability. The format for electronic signatures may be described in the documentation for the message. For messages needing a strong connection to an individual, a qualified signature as provided for by the Act relating to electronic signatures may be required. For other messages an organizational signature combined with textual information identifying the responsible sender will be sufficient.
Encryption	Messages containing sensitive personal data must be encrypted.
Message service specification (ebXML)	The transmission of messages should take place by means of the message service specification (ebXML), which is an international standard for the exchange of messages. The specification consists of a message envelope and procedures for reliable message exchange. The envelope ensures the unique identification of the communicating parties (sender and recipient), and identifies the business transaction (medical certificate, prescription, etc.). The specification further describes how security is maintained when transmitting messages.
NHN Address register / **HER-id**	The NHN Address register contains information to identify and address each of the organization's various recipients and senders. Upon registration in the NHN Address register, the individual organization and its own communication partners (senders/recipients) will be associated with a unique identifier referred to as the HER-id. HER-id identifies healthcare personnel, organizations, and departments, and will, amongst other things, contribute to a more secure addressing of information.