Code of conduct for information security in the health sector

Published with the support of: Helsedirektoratet

Remote access between supplier and organization

Support document
Fact sheet no 36
Version: 3.0
Date: 31 May 2012

Purpose	To prevent unauthorized use and maintain integrity and confidentiality for health and personal data in connection with remote access. To ensure that there is adequate security during the connection and transfer of health and personal data.		
Responsibility	The organization's management is responsible for ensuring that the use of remote access from suppliers fulfils the requirements concerning confidentiality, integrity, availability and quality.		
Execution	Shall be implemented before connection of remote access and as a continuous activity during use of remote access.		
Scope	When establishing and using remote access.		
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	• Personal Data Regulations, sections 2-10, 2-11, 2-12, and 2-13 • Personal Health Data Filing System Act, section 16 • Health Personnel Act, section 25		
References	• Code of conduct for information security in the health sector • Guideline for remote access between supplier and organization • Fact sheet 15 – Incident registration (logging) and follow-up • Fact sheet 7 – Risk assessments • Framework for authentication and non-repudiation in electronic communication with and in the public sector, April 2008 (cf. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf)		

No	Activity/Description
1.	**Principles of remote access** a) Principles of remote access must be based on the organization's Information security management system. b) The organization should establish a consistent solution for remote access in connection with health and personal data and not several fragmented solutions for individual suppliers. c) All access to the organization's systems through the use of remote access. d) Following a risk assessment, and if in accordance with the purpose of remote access, it may in exceptional cases be permitted to use solutions that do not require manual operations to open up access to remote access (see Guideline for remote access between supplier and health organization). e) All activities must be recorded in incident registers. The supplier must document what has been carried out in the organization. Incident registers may be both in electronic and manual form.
2.	**Before remote access is established** a) A requirement survey must be carried out for each new or changed supplier relation with the purpose of determining: - The professional purpose of the connection and the importance for the organization - The systems or records that will be accessed - The technical solution the connection is based on: terminal server, client, database tool, WEB, etc. - TCP/IP network addresses and port numbers to be used

No	Activity/Description
	- The need for access to read, write and upload/download personal health data, and how this shall be administered and documented - Access with administrator privileges to operating system, database or specialized system - Use of remote management (control of screen, keyboard and mouse) that is to be initiated by the organization b) A risk assessment must be carried out based on the organization's level of acceptable risk. c) Based on the risk assessment, the organization must determine the following: - Whether remote access is to be used and whether it shall be used for the solution in question - At which level the access shall take place with respect to operating system, database etc. - Use of predefined equipment for access to the remote access solution - Access to parts of records with personal health data and the type of access in relation to: reading, writing, uploading and downloading - Use of uploading and downloading of technical corrections in software and configuration parameters - Requirements concerning the supplier's network and equipment - Connection and use of tools for remote administration shall primarily be initiated from the organization as a conscious action - Requirement for coordination between several suppliers before the solution is established - The procedures and agreements that must be in place with regard to other requirements in the organization's Information security management system
3.	**Agreements** a) Written agreements shall be entered into, which must contain at least the following: - Who the agreement concerns - The purpose of the agreement or special agreement - Responsible individuals/roles - The organization must have access to the supplier's documentation of security objectives and strategy - The organization must have right of access to the supplier's solution for compliance with the Code - The organization must have right of access to the supplier's relevant incident registers - Duty of secrecy for the supplier's personnel - The procedures that apply for the remote access solution - Routine for handling nonconformities - Consequences in cases of agreement breaches - Summary of which systems remote access applies to - Description of equipment the supplier can use for remote access and ownership of the equipment - Impact assessment in the case of deliberately dropped connections while using the remote connection
4.	**Documentation** a) The following documentation must be present before remote access is granted: - Signed statement of secrecy with respect to access to personal health data. The supplier keeps these on behalf of his own personnel. See the Code with regard to duty of secrecy for employees - Security directive that has been read and accepted - Procedure for: ▪ Signing of statement of secrecy and confirmation that the security directive has been read and accepted

No	Activity/Description
	▪ Training of service associates ▪ Administration of authorization for equipment used for remote access ▪ Use of solution for strong authentication ▪ Handling nonconformities in connection with remote access ▪ Incident registration and follow-up of incident registers ▪ Erasing of data files retrieved from the organization ▪ Destruction of storage media upon disposal ▪ Tasks that may be associated with connection to/establishment of remote access. Granting of authorization for network, equipment and systems ▪ Authentication of service associates with supplier ▪ Control of authorizations granted ▪ Tasks that must be carried out associated with connection to/establishment of remote access ▪ Other technical and administrative procedures that the management system requires or that the risk assessment indicates
5.	**Selection and establishment of technical solution** a) The technical solution should include the following elements: - The external termination should take place through a firewall and in a separate DMZ for remote access - Only previously approved and explicitly defined traffic will be permitted - Authentication shall be at security level 4 - If there is a professional need for the supplier to move health and personal data to the supplier's secure network areas, this shall be carried out in accordance with a data processor agreement - All external communication involving personal health data shall be encrypted with a minimum encryption strength corresponding to the use of PKI or an organizational certificate in accordance with the applicable "Specification of requirements for PKI in the public sector" in order to be satisfactory [1] - There must be solutions in place to prevent malicious software with both the supplier and the organization - Technical measures must ensure that the supplier's workstation is not connected to other networks when connections to the organization's network take place Examples of technical solutions can be found in "Guideline for remote access between supplier and organization".
6.	**Incident registration** a) Incident registration shall be implemented so it is possible to detect and resolve security breaches. The following incident registration shall take place in the organization's systems and networks in connection with authorized use: - Unique identifier for the authorized user - The role of the authorized user in connection with access - Organization affiliation - Organizational affiliation of the authorized person - The type of information for which access has been granted - The basis for the access - The time and duration of *the access* b) In the case of remote access by *the supplier*, the following shall be recorded in addition to incident registration:

[1] http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki

No	Activity/Description
	- Initiated traffic with respect to IP addresses and port number - The data/files that were downloaded to the supplier (data files) or uploaded to the organization (application files and patches) - Unique identifier for the person with *the supplier* who has used the *remote access* in question c) The following incident registration shall be carried out concerning attempted unauthorized use: - The user identity that was used - Time (date and time) - IP address or other identification of PC/workstation that was used (for example MAC address or NAT address) d) Incident registers shall be retained for a minimum of two years.