Guideline for remote access between supplier and organization

This guideline is a support document to the Code of conduct for information security

Published with the support of:

Helsedirektoratet

Version 2.0

www.normen.no

CONTENTS

1 INTRODUCTION

1.1 Background

It is necessary for most *organizations* in the sector that *suppliers* assist with the aid of *remote access*. The background to a separate guideline for *remote access* between *supplier* and *organization* is to provide guidance for the establishment of technical and organizational solutions.

The *organization* (data controller) is responsible for ensuring that the remote access solution fulfils the requirements of the Code. The tasks relating to *remote access* can be divided between the *organization* and the *supplier* by written agreement.

The guideline also assists the sector in establishing solutions that ensure that applicable safety requirements are met.

1.2 About the guideline

The guideline has been prepared for the Steering group for the Code with the support of the Directorate of Health by the companies INCERTUS and INFOSEC Norge AS.

The aim of the guideline is to provide guidance concerning compliance with the requirements in the Code as regards the technical and administrative measures which must be implemented within the *organization* and the *supplier* in connection with *remote access*. The *organization* is bound by the Code in connection with entry into a customer agreement with *Norsk Helsenett* (cf. chapter 1.6 of the Code). From this, it follows that the solution for *remote access* must fulfil the requirements of the Code. The *supplier* and *organization* must fulfil the requirements of the Code.

The guideline has been prepared in collaboration with *suppliers* in the sector and the sector's own reference group. See chapter 5.6 for participants in the reference group.

The guideline applies to *remote access* for all types of information system within which *personal health data* is processed. Examples of information systems include medical image diagnostics, electronic patient records (EPR), operation and maintenance management, technical medical equipment, laboratory systems and ICT infrastructure.

The guideline must be read in its entirety because requirements are documented in several chapters.

1.3 Target group and the assistance provided by the guideline

The target group for the guideline consists of the *organization* and the *supplier*.

The guideline provides the *organization* with a basis for choosing a solution for *remote access* so that it is established in accordance with the requirements laid down in the Code. The *organization* may use the guideline as a specification of requirements in relation to *suppliers*.

The guideline provides *suppliers* of systems and technical solutions that are used for the *processing* of *personal health data* with a basis for establishing solutions for *remote access* in accordance with the Code.

Examples of systems and technical solutions are:
- *Specialized systems* (e.g. electronic patient records, patient administration systems, laboratory systems)
- Technical medical equipment (e.g. image diagnostics)
- ICT infrastructure (e.g. servers, networks, archiving equipment, communication equipment, security technology, etc.)

The guideline reproduces the requirements of the Code and gives recommendations as regards how the requirements can be fulfilled in connection with the establishment and use of *remote access*.

The guideline also gives guidance when the *supplier* provides *remote access* without the *organization* being operationally involved. Such actions must be agreed upon and no connections must be established without the knowledge of the *organization*.

1.4 Definitions

Definitions are taken from the Code. New terms are defined and summarized after the definitions from the Code. Defined terms are indicated by *italics* in the text.

Definitions from the Code (of 2 June 2010)

-A-

"***Access***" means, for the purposes of the *Code*, that *health and personal data* concerning one or more specific *patients/clients* is, or is made, available to *authorized* personnel. The decision to grant *access* to a *personal health data filing system for therapeutic purposes* shall be made after a concrete evaluation based on the provision of medical assistance to the *patient. Access* to *specialized systems* in connection with the provision of services to a *patient/client* shall only be granted based on an *official need*. *Access* in relation to quality assurance and administrative tasks shall also be decided upon on the basis of *official needs*.

"***Administrator right***" means, for the purposes of the *Code*, the highest level of access to a system, server, database and security barrier. This level of access usually has the right to perform any and all operations.

"***Authentication***" means, for the purposes of the *Code*, the process that is carried out in order to confirm a claimed identity.

"***Authorize/authorized/authorization***" means, for the purposes of the *Code*, that a person in a certain role may be granted or has been granted specific permissions to read, register, edit,

correct, delete and/or block *health and personal data. Authorization* may only be provided insofar that it is necessary for an individual to fulfil his or her *duties* and all provisions regarding the *duty of secrecy*.

-C-

"***Configuration***" means, for the purposes of the *Code*, the information system's construction, including both technical equipment and software.

-D-

"***Data controller***" means the entity which determines the purpose of the *processing* and the means to be used, unless *responsibility for such data control* is specially prescribed in the Act or in Regulations laid down in accordance with the Act, ref. the Personal Health Data Filing System Act section 2 no. 8 and the Personal Data Act section 2 no. 4) (here, the term "controller" is used). To be clear, it is emphasized that it is the *organization* that functions as the *data controller* for the *processing* of *health and personal data.* The responsibility shall be taken care of by the day-to-day management of the *organization*, while the *organization* is the legal subject responsible for the fulfilment of the obligation.

"***Data processor***" means an individual who *processes health and personal data* on behalf of the *data controller*, cf. the Personal Health Data Filing System Act section 2 no. 9 and the Personal Data Act section 2 no. 5. It should be emphasized that a *data processor* is an individual or *organization* external to the *data controller's organization*. This entails that the *data controller's* own associates are not his or her *data processors*.

"***Duty of secrecy***" means, for the purposes of the *Code*, a legal or agreed obligation to prevent others from accessing or gaining knowledge of *health and personal data*, cf. the Health Personnel Act section 21, the Personal Health Data Filing System Act section 15, the Social Services Act section 12-1 and the Public Administration Act sections 13 to 13e, in addition to other information pertinent to information security, cf. the Personal Data Regulations section 2-9. The *duty of secrecy* involves both a passive obligation to remain silent and an obligation to actively prevent unauthorized persons gaining knowledge of confidential data.

-H-

*"**Health and personal data**"* is used in the *Code* as a generic term for *personal health data* and/or *personal data* within the scope of the *Code* as defined in the section 1.5 of the Code.

The "***health net***" means, for the purposes of the *Code*, the network provided by Norsk Helsenett SF [Norwegian Healthnet SF].

-I-

"***Incident filing system/register***" means, for the purposes of the *Code*, a logical *filing system* in which incidents in the information system are recorded; cf. incident registration.

"***Incident registration***" means, for the purposes of the *Code*, the registration of incidents in an information system, amongst other things for the purposes of preventing, uncovering and hindering the recurrence of breaches of security.

-N-

"***Nonconformity***" means, for the purposes of the *Code*, any processing of *health and personal data* not done in accordance with any and all applicable regulations, guidelines and/or procedures, as well as other security breaches.

"***Norsk Helsenett/Norwegian Healthnet***" means, for the purposes of the *Code*, Norsk Helsenett SF [Norwegian Healthnet SF].

-O-

"***Organization***" means, for the purposes of the *Code*, a legal unit such as a health trust, *municipality*, hospital, medical practice, dental clinic, pharmacy, pharmacy chain, X-ray institute, independent laboratory, university, university college, foundation, etc.

-P-

"***Processing***" means, for the purposes of the *Code*, any purposeful use of *health and personal data*, be it, e.g. collection, recording, collocation, storage and disclosure, or a combination of such uses, cf. the Personal Health Data Filing System Act section 2 no. 5 and the Personal Data Act section 2 no. 2.

-R-

"***Register of authorizations***" means, for the purposes of the *Code*, a *register* of *authorizations* issued, which shall be kept by the *data controller*.

-S-

"***Security level 4***" means, for the purposes of the *Code*, two-factor *authentication* where one factor is dynamic, based on qualified certificates, and which in all other respects satisfies the requirements for *security level 4* in the "Framework for Authentication and Non-repudiation in Electronic Communication in and with the Public Sector".

"***Specialized system***" means, for the purposes of the *Code*, a computer application or an IT system that *processes health and personal data*. The term 'system solution' is also used to refer to a *specialized system*. Examples of *specialized systems* are: nursing services systems, doctor's surgery systems, and child protective services systems. The information in individual *specialized systems* may constitute *electronic patient records (EPR)* and other *service documentation*.

"***Supplier***" means, for the purposes of the *Code*, a legal entity providing technical and/or administrative services to the *organization*. Examples are *EPR suppliers*, X-ray suppliers, *suppliers* of solutions for text messaging systems, ICT suppliers, etc.

-T-

"***Technical measures***" means, for the purposes of the *Code*, measures of a technical character that may not be influenced or circumvented by employees, and that are not restricted by actions that individuals are assumed to perform. Examples of such measures may be *authentication* at *security level 4*, or *configuration* of a firewall such that it only allows specific data traffic, or a message service that is designed in such a way that all messages are automatically encrypted.

Definitions in this guideline

-P-

"***Physical access***" means physical access to equipment and areas that are used for the *processing* of *health and personal data*.

-R-

"***Remote access***" means, for the purposes of this document, external *access* from *supplier* to *organization* via a communication line. Examples of areas of use are: error correction, troubleshooting, updating, *remote administration*, testing and development, transfer of data files, operational monitoring (databases, servers, archiving solutions), processing of error messages and data files held by *suppliers* and the sending of error diagnoses, etc. of *specialized systems* and ICT infrastructure.

"***Remote administration***" means, for the purposes of this document, that a user in one location may operate a workstation at a physically different location by remotely controlling the screen, keyboard and mouse.

-S-

"***Service associate***" means, for the purposes of this document, an associate of the *supplier*.

2 REQUIREMENTS AND RECOMMENDATIONS CONCERNING REMOTE ACCESS

This chapter describes requirements taken from the Code which shall and should be met in connection with *remote access*. Compliance with the individual requirements is generally the responsibility of the *data controller*, but this responsibility may also be assigned to the *supplier* by agreement. The tables below propose a delegation of tasks, but it is up to the *data controller* and *supplier* to determine the actual delegation of tasks. The division of tasks between the *organization* and the *supplier* shall collectively ensure that the requirements in the *Code* are met.

The individual requirements are inserted in quotation marks.

2.1 Responsibility and agreements

This section presents a description of the requirements concerning agreements and the clarification of responsibility, including fulfilment of the *duty of secrecy* through a statement of secrecy. This section describes typical control obligations such as security auditing and non-conformity management.

The *organization* and the *supplier* may enter into an agreement where a security provider is used for the remote access solution. 'Security provider' means a subcontractor who performs security tasks in accordance with the Code (cf. chapter 5.8.4 of the Code).

2.1.1 Written agreement with supplier (chapter 5.8 of the Code)
"Written agreements shall be entered into with the supplier. The agreements shall include obligations which require the parties to fulfil the requirements and measures that follow from the Code for information security applicable at any one time, as well as the regulation of penalties in the event of a breach of the Code and the agreement in general."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
It is recommended that the agreement that regulates the obligation relating to the Code is incorporated as part of the agreement with the *supplier* concerning *remote access*. Use the draft contractual text in chapter 5.4 as a basis for the actual agreement. The agreement should be revised and updated as and when necessary. For example, following *non-conformities*, risk assessments and security audits. It is recommended that a general security directive is prepared for *suppliers*.	The *supplier* must ensure that *service associates* are familiar with the content of the agreement and, where applicable, the security directive (ref. chapter 5.5). The *supplier* may use subcontractors. If this is the case, this must be stated in the agreement between *supplier* and *organization*. The subcontractor should have *access* to the *organization* through the *supplier's* network unless otherwise agreed, and must comply with the security requirements that apply to the *supplier*. The same requirements that apply to *suppliers* apply to subcontractors.	Fact sheet 1 – Responsibility and organization Fact sheet 9 – Training of managers and associates

2.1.2 Statement of secrecy (chapter 5.8.3 of the Code)

"The *supplier's* staff has signed a statement of secrecy that implies an absolute *duty of secrecy* with regard to all *health and personal data*."

It is the supplier's responsibility to safeguard the duty of secrecy for his or her service associates and to ensure that a statement of secrecy is signed by his employees.

Implications for		References to fact sheets and guidelines
Organization	Supplier	
As part of the agreement with the *supplier*, the *supplier* should be required to organize statements of secrecy for *service associates*. Use the template under references which are adapted to.	The *supplier* organizes the signing of statements of secrecy for all *service associates*. Statements of secrecy are individual and cannot be signed collectively. The *supplier* archives the statements of secrecy, which must be made available to the *organization* upon request. Even if a statement of secrecy has not been signed, anyone who performs a service or work for an administrative body shall be subject to a *duty of secrecy*, cf. Section 13 of the Public Administration Act. The same shall apply to the *duty of secrecy* in accordance with the Personal Health Data Filing System Act, cf. Sections 13 and 15.	Template for statement of secrecy

2.1.3 Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)

"The *supplier* complies with the Code with respect to the *data controller's* obligations regarding security audits and non-conformity management."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall regularly conduct security audits of the solution for remote access. The *organization* shall ensure that the *supplier* conducts security audits and has procedures for non-conformity management. The *suppliers'* security audits and non-conformity management may form the basis for measures which the *organization* must implement.	The *supplier* shall regularly and at least once a year conduct a security audit of the solution that is used for *remote access*. All non-conformity reports pertinent to the agreement concerning *remote access* must be reported to the *organization* without undue delay.	Fact sheet 6 – Security audits Fact sheet 8 – Non-conformity management

2.1.4 Raising awareness of the duty of secrecy (chapter 5.1 of the Code)

"To safeguard the confidentiality of *health and personal data*, the *organization's* manager shall ensure that all personnel who are granted *access* are subject to a *duty of secrecy*, and that they are aware of the content and scope of the *duty of secrecy*, for all *health and personal data* as well as for other information pertinent to information security."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
In the agreement with the *supplier*, the *organization* should: • Describe the consequences for *service associates* of a breach of the *duty of secrecy*. • Describe the consequences for *service associates* of obtaining or attempting to obtain information for which they have no official need (unlawful acquisition). • Describe the consequences for *service associates* of changing/attempting to change information that they are not *authorized* to change.	The *supplier* shall train *service associates* with regard to the content and consequences of the *duty of secrecy* in the event of a breach of the *duty of secrecy*, of obtaining information for which they have no official need and of changing/attempting to change information that they are not *authorized* to change.	

2.2 Risk assessment

This section presents a description of the requirements for carrying out the risk assessments based on the requirements concerning acceptable risk regarding confidentiality, integrity, availability and quality.

2.2.1 Risk assessment before access is granted (chapter 4.6 of the Code)

"Risk assessments shall be carried out at least prior to:

- the commencement of *processing* of *health and personal data*
- establishment of new information processing systems or data filing systems which contain *health and personal data*
- the implementation of organizational changes which could impact on information processing
- the implementation of technical changes to equipment and/or software which could impact on information processing
- the implementation of other changes of significance to information security

The risk assessment must be documented. If technological measures for achieving an acceptable risk are not implemented immediately, administrative measures may be used for a transitional period, e.g. in the form of procedures."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* must perform a risk assessment of the complete solution that is used before the *supplier* is granted *access*. As a basis for the risk assessment, the *organizations'* requirements for acceptable risk regarding confidentiality, integrity, availability and quality shall be used. The risk assessment must be documented. A simplified risk assessment may be carried out using the form in appendix (chapter 5.2). It is not necessary to carry out a new risk assessment of the remote access solution for each new *supplier* that is affiliated.	The risk assessment that has been carried out of the *supplier* may constitute sufficient documentation that a risk assessment has been carried out. As a basis for the risk assessment, the *organizations'* requirements for acceptable risk regarding confidentiality, integrity, availability and quality shall be used. The risk assessment from the *supplier* may form the basis for the risk assessment which the *organization* is required to carry out.	Fact sheet 7 – Risk assessments Fact sheet 5 – Determination of acceptance criteria for availability, confidentiality and integrity

2.2.2 Risk assessment in operations (chapter 6.2 of the Code)

"The *organization's* management shall also regularly carry out risk assessments in order to map risk areas and clarify the probability and consequences of accidents and incidents."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* should establish a plan for carrying out risk assessments. The plan should cover *remote access* such that applicable solutions are evaluated in relation to the level of acceptable risk.	The *supplier* shall carry out risk assessments by agreement with the *organization*.	Fact sheet 7 – Risk assessments

2.3 Training

This section presents a description of the requirements for training of the *organization's* associates and the *supplier's service associates*. Aspects for a training plan are also presented.

2.3.1 Training measures (section 5.6 of the Code)

"The *organization* shall implement measures which ensure that:

- everyone who is granted *access* to and/or operates the information systems and associated information shall have sufficient knowledge to use the systems for their role and to safeguard information security.

Competence development must take place continually and be appropriate for the various roles and user groups. Special training measures must be considered for new employees and in the event of changes to the information systems or to the *processing* of *health and personal data."*

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall train its own associates in the technical solution and the procedures that are to be used in connection with *remote access*. The training must also safeguard competence in monitoring use of the solution and the follow-up of incident registers. All *organizations* shall possess a minimum level of knowledge concerning their own remote access solution. This particularly applies to what *service associates* can carry out on technical equipment that is used for the *processing* of *health and personal data*. The training should include but not be limited to: a) Control on use of the remote access solution b) Follow-up of incident registers c) Granting and revoking of *authorization* d) Non-conformity reporting and processing	The *supplier* shall train *service associates* in the use of the remote access solution and the content and scope of the *duty of secrecy*, preferably through an established training plan. The training should include but not be limited to: a) Technical solution b) Use of the remote access solution c) Authentication solution d) e) Archiving of files from different *organizations* f) Follow-up of incident registers g) Non-conformity reporting h) Traceability of changes made by the *suppliers*	Fact sheet 9 – Training of managers and associates Fact sheet 3 – Overview of recommended procedures in the governance system

2.4 Connection and limitation of traffic

This section largely presents a description of the requirements for the technical solution relating to the connection of *remote access*, through or outside the *health net*. For troubleshooting, special rules apply which are referred to in chapter 2.4.2.

2.4.1 Internet service provider (chapter 5.7 of the Code)

"When data communication is used, each individual *organization* shall either fulfil the following requirements itself, or ensure that those who perform the task/supply the service fulfil the requirements.

All communication with *organizations*/services outside the *organization* should preferably take place via one channel, i.e. one internet service provider. If several internet service providers are used with respect to systems within which *health and personal data* is processed, all providers must satisfy the requirements."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Remote access for maintenance and updates should be routed through the	The *supplier* must establish a remote access solution which fulfils the requirements of the	Fact sheet 28 – Alternative technical

Implications for		References to fact sheets and guidelines
Organization	Supplier	
health net. Even if the connection takes place through the *health net*, the *organization* has an independent responsibility for ensuring that secure remote access is established within its own *organization*. *Norsk Helsenett (Norwegian Health Network)* may impose requirements through the contractual agreements which require all *access* to networks other than the *health net* to be approved by *Norsk Helsenett*. The *organization* is responsible for ensuring that this approval is obtained. The purpose of "one channel" is to ensure a better overview and control of communication solutions where there is only one net service provider.	Code. The *supplier* shall be free to choose communication through the *health net*, but must relate to the solution and requirements within the *organization*.	solutions for the primary health service Fact sheet 36 – *Remote access* for maintenance and updates Guideline for information security relating to a connection between municipalities, county councils and the *health net*

2.4.2 Limitation of traffic (chapter 5.7.1 of the Code)

"In the case of connections to networks outside the *organization*, *technical measures* shall be established which ensure that:

- Only explicitly defined traffic may pass; other traffic is blocked.
- Traffic from external sources cannot pass directly into the system; all such external traffic must be initiated from the *organization's* systems.

Incident registration is implemented in order to check that rules are not being breached; in the event of a breach, the communication channel will be closed until a new, secure solution is in place."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall ensure that the *technical measures* are taken care of in the solution. Under special circumstances, a firewall may temporarily be configured for more access than the agreement covers, e.g. in situations for testing solutions through connection or for troubleshooting and error correction. In such cases, the expanded *access* (opening) should be limited in terms of time. When a temporary connection is activated, it should be actively monitored by the *organization* and all traffic must be logged. When the issue has been resolved, one must make sure that the temporary opening for traffic is	The *supplier* shall ensure that the *technical measures* are taken care of in the solution.	Fact sheet 15 – *Incident registration* and follow-up Fact sheet 22 – Control and security regarding external *access* Fact sheet 24 – Communication via open networks

Implications for		References to fact sheets and guidelines
Organization	Supplier	
deleted and any added authorizations are deleted. "Directly into from an external source" means that the traffic must pass via a security mechanism (e.g. a proxy service or terminal server).		

2.5 Encryption of external communication

This section presents a description of the requirements for encryption as a tool for ensuring confidentiality.

2.5.1 Encryption solution (chapter 5.4.4 of the Code)

"Security measures shall prevent persons who are not *authorized* from gaining *access* to *health and personal data* through ensuring that:

- All communication, whether via wireless communication or via lines, shall be secured through encryption in accordance with the Data Inspectorate's recommendations in force at any one time."[1]

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* must ensure that communication between the *supplier* and the *organization* is encrypted. All communication between the *supplier's* secure network and the *organization's* network within which *health and personal data* is processed must be encrypted. In the event of malfunctions in the encryption solution between the *supplier* and the *organization*, the communication must cease and the *supplier* must be notified of the *non-conformity*. Further communication must not be possible until the encryption is operational again. An encryption strength which corresponds to the use of organizational certificates in accordance with the applicable "Specification of requirements for PKI within the public sector" is satisfactory. [2]	The *supplier* must document the encryption solution that is used and that it fulfils the requirements laid down in the "Specification of requirements for PKI within the public sector".	Fact sheet 24 – Communication via open networks Fact sheet 26 – Securing of wireless technology Fact sheet 49 – Requirements concerning the use of PKI in connection with external communication

[1] For the current recommendation, see footnote 2
[2] http://www.difi.no/artikkel/2010/04/kravspesifikasjon-for-pki

2.6 Preventing malicious software

This section presents a description of the requirements for preventing the transfer of malicious software between *organization* and *supplier*.

2.6.1 Solution for malicious software (chapter 5.8.3 of the Code)
"The *organization* shall, in order to safeguard confidentiality, integrity, availability and quality for *health and personal data*, ensure that:

The *supplier's* equipment that is used for online connection using a communication network or portable equipment that is connected to the *organization's* equipment, does not contain malicious software, viruses, etc., and that the equipment is secured against *access* from intruders."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall have a solution to prevent the transfer of malicious software from the *supplier* to its own network and equipment. The solution shall be continuously updated with new *security updates*.	The *supplier* shall have a solution which prevents the transfer of malicious software from its own network to the *organization's* network and equipment. The solution shall be continuously updated with new *security updates*.	Fact sheet 19 – Measures to prevent malicious software

2.7 Access to and securing of equipment for remote access

This section presents a description of the requirements for the securing of areas so that unauthorized persons cannot gain *physical access* to equipment and solutions containing *health and personal data*.

2.7.1 Access regulation (chapter 5.8.3 of the Code)
"The *supplier* may only be granted *access* by special permission from the *organization* in each individual instance and only be given *access* to required devices."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall establish procedures for access regulation as and when necessary.	All *access* shall be specifically assessed in each individual case and only be granted in cases where there is an official need.	Fact sheet -17 – Physical protection of areas and equipment

2.7.2 Physical security measures (chapter 5.4.2 of the Code)
"Security measures shall prevent persons who are not *authorized* from gaining *access* to *health and personal data* – either through the access-regulated control of premises with equipment or through the equipment being protected against misuse and screens, printouts, etc. being protected against unauthorized access."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Equipment which is located on the *organization's* premises must be protected against misuse and unauthorized *physical access*.	The *supplier* must ensure that equipment which has active connections to *professional systems* is adequately protected so that unauthorized persons cannot gain *physical access* to the solution and thereby *access* to *health and personal data*, e.g. the locking of workstations when the workplace is left unattended. Computer screens must be protected against access by unauthorized persons. The *supplier* must establish a procedure for managing any printouts with regard to access by unauthorized persons.	Fact sheet 17 – Physical protection of areas and equipment

2.8 Authorization

This section presents a description of the requirements for authorization of the *supplier's service associates* which are to have *access*. This section also describes the requirements for a *register of authorizations*.

2.8.1 Responsibility for allocating authorization (chapter 5.2.2 of the Code)

"The *data controller* is responsible for ensuring that *authorizations* are assigned, administered and controlled."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
In connection with the allocation of *authorizations*, the statutory *duty of secrecy* must be assessed and fulfilled. *Service associates* which perform different roles in connection with *remote access* shall *be authorized* for each role, regardless of their other roles.	The *supplier* may not override *authorizations* granted by the *organization*, e.g. by giving itself *authorizations* in connection with the use of *administrator rights*.	Fact sheet 14 – Access control

2.8.2 Procedure for allocating authorization (chapter 5.2.2 of the Code)

"A procedure shall be established for the granting and managing of access rights."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The procedure for allocating *authorizations* for internal systems shall ensure: • The statutory *duty of secrecy* shall be assessed and fulfilled	The *supplier* shall have a procedure to grant and revoke *authorization* for *access* to equipment and software used for *remote access*. *Authorization* may only be granted in	Fact sheet 14 – Access control

Implications for		References to fact sheets and guidelines
Organization	Supplier	
• Only technical personnel with a specific need for *access* may be *authorized* for large quantities of *health and personal data*. Measures shall be implemented so that possible misuse may be detected.	accordance with the actual tasks the individual *service associate* at the *supplier* will carry out. *Authorization* may only be granted to *service associates* who have signed the statement of secrecy. It is not permitted to grant joint *authentications* to a group of *service associates*. All *service associates* shall have unique *authentication* for equipment which is used for *remote access*.	

2.8.3 Authorization register (chapter 5.2.2 of the Code)

"The *data controller* shall ensure that an *authorization register* is created. This register shall contain at least the following:

- information on who has been assigned *authorization*
- for which role the authorization has been assigned
- the purpose of the *authorization*
- time of granting and, if applicable, revocation of the *authorization*
- information on which *organization* the *authorized person* is linked to

Records of granted *authorizations* must be archived for a minimum of five years from the date on which the *authorization* was withdrawn."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* shall keep a *register of authorizations* for the *organization's* own systems in accordance with the requirement.	It is recommended that the *supplier* keeps a *register of authorizations* for the *supplier's* and, if applicable, the subcontractor's solution for *remote access*. The archiving requirement of five years also applies in the event the agreement is discontinued. The information in the *register of authorizations* shall be available to the *organization*.	Fact sheet 47 – *Register of authorizations*

2.9 Authentication and access

This section presents a description of the requirements for *authentication* for *security level 4* and general *authentication* for *specialized systems*. The section also covers the use of user accounts, including the use of administrator rights. No requirement is established regarding where authorization at security level 4 must be carried out.

2.9.1 Authentication with security level 4 (chapter 5.2.1 of the Code)

"In connection with the use of mobile equipment, home offices and wireless communication, the *authentication* must not involve a greater risk than for stationary equipment, and *authentication* at *security level 4* must be used."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Connections with *remote access* to systems with health and personal data will come under this requirement. If the *organization* does not have a solution which uses PKI which satisfies *security level 4*, such a technical solution shall be established and procedures drawn up.	The *supplier's service associates* with a Norwegian personal identity number or D number must order an electronic identity from the *supplier* that the *organization* uses. Electronic IDs are personal and must be ordered for each of the *service associates* who are to use the solution for *remote access* with respect to the *organization*. *Service employees* without a Norwegian personal identity number or D number will experience difficulties obtaining a Norwegian declared certificate. In connection with this, the European Commission has decided that individual EU/EEA countries must establish, maintain and publish a TL list (Trusted List), which contains the necessary information relating to issuers of security level 4 under the supervision of the country concerned (ref. link on the right of the table)	Fact sheet 49 – Requirements concerning the use of PKI in connection with external communication http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_NPT_NO_TEKSTVISNING?p_d_i=-121&p_d_c=&p_d_v=114520

2.9.2 Access control (chapter 5.2.3 of the Code)

"Only authorized personnel may gain *access* to *health and personal data."*

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Access to *specialized systems* shall be granted on the basis of a decision concerning official need. The *organization* shall ensure compliance with the duty of secrecy rules.	*Access* shall be controlled such that the duty of secrecy rules are fulfilled and so that *access* to *health and personal data* is not granted to unauthorized persons.	Fact sheet 14 – Access control

2.9.3 Use of authorization (chapter 5.5.2 of the Code)

"*Technical measures* and organizational measures shall be implemented so that persons cannot gain *access* to *health and personal data* for which they are not authorized."

Implications for		References to fact sheets and guidelines
Organization	Supplier	

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Access based on *security level 4* will provide sufficient confidentiality protection for *access* to the individual systems. The *organization* should incorporate in the agreement for *remote access* the requirement that access and authentication mechanisms are personal and must not be loaned to other *service associates*.	The *supplier* must train *service associates* in the correct use of the authentication mechanisms. As a rule, *administrator rights* to equipment within the *organization* should not be granted to *service associates*. This may nevertheless be acceptable provided that the *organization* has approved the *service associate* and approves the individual connection concerned for *remote access*.	Fact sheet 14 – Access control

2.10 Processing of health and personal data obtained from the organization

This section presents a description of the requirements applicable in cases where the supplier is to transfer *health and personal data* from the *organization* to the *supplier*. The section also describes the transfer of *health and personal data* abroad.

2.10.1 Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)
"The *data processor* has an independent responsibility for information security in accordance with the Personal Health Data Filing System, section 16 and the Personal Data Act section 13. The agreement must specifically regulate security aspects. The *data processor's* independent duty to comply with the Personal Data Filing System Act section 16 and the Personal Data Act section 2 must be emphasised. In addition, criteria shall be established for acceptable risk for the *data processor*, and it must be stated that the *data controller* must be secured right of access to verify compliance with the requirements."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
When the *supplier* downloads data containing health and personal data from the *organization*, a data processor agreement shall be established with the *supplier* before transfer takes place. Under references are templates and guidance for a data processor agreement. Fact sheet 10 also contains a template. These templates must be adapted to the situation concerned. A data processor agreement may be valid for an extended period of time. The purpose and what can be transferred must be specified in the agreement. The data processor agreement may form an appendix to the agreement concerning *remote access*.	Data containing *health and personal data* may not be processed except as specified in the data processor agreement. Computer files that contain *health and personal data* that are retrieved from the *organization* for troubleshooting purposes shall only be processed by an authorized *service associate*. If it is possible to anonymize the *health and personal data*, it is recommended to do so. If data is pseudonymised, the Code shall apply in full for identifiable *health and personal data*. Data files may only be stored on the equipment of a *supplier* that has installed the necessary *technical measures* in order to prevent persons without *authorization* from gaining *access* to *health and personal data*.	Fact sheet 10 – Use of *data processor* (external operating unit) Templates from the Data Inspectorate: http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/ Concerning anonymization and pseudonymising, see the guideline: Personal privacy and information security in research projects within the health and healthcare sector

Implications for		References to fact sheets and guidelines
Organization	Supplier	
	Data files must be erased by agreement between the parties when the purpose of retrieving the data files has been fulfilled. This also applies to any backup copies.	For the secure deletion of data, see: www.nsm.stat.no

2.10.2 Transfer of health and personal data abroad (chapter 1.0 of the Code)

"The Code has been developed on the basis of the provisions of the Personal Data Act concerning sector-based codes of conduct (cf. the Personal Data Act section 42 third paragraph no. 6). These provisions are in turn based on Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the *processing* of personal data and on the free movement of such data. The Directive has been implemented in Norwegian legislation based on Norway's obligations under the EEA Agreement."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Personal data may be transferred to countries within the EU and EEA areas by agreement between the *organization* and *supplier*. It may also be transferred to countries approved by the European Commission, as well as certain companies in the USA that have joined Safe Harbor. An *organization* may also transfer *health and personal data* to other countries if the European Commission has determined that the country has an adequate level of protection. The easiest way to transfer *health and personal data* to other countries is to use the standard contracts provided by the EU.	It is a requirement that the *supplier* can only transfer health and personal data to a specific address. "Address" means to a specified physical location and to one or more specified physical computer(s). The *supplier* must be in a position to document ownership of an address that is situated outside the EU/EEA area.	See the Data Inspectorate's website www.datatilsynet.no for forms and procedures

2.10.3 Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)

"If a *data processer* processes *health and personal data* from a number of *organizations*, the *data processor* must, with the aid of *technical measures* which cannot be overridden by the users, ensure that: divisions are established between the *organizations* in accordance with a risk assessment."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Ensure that the matter is taken care of through the agreement concerning *remote access*.	The *supplier* shall establish a solution in accordance with the agreement concerning *remote access*. The requirement is that data containing *health and personal data* shall be logically separated from other customers and the *supplier's* internal networks in general. It is not sufficient to separate data using only authentication solutions. For example,	

Implications for		References to fact sheets and guidelines
Organization	Supplier	
	employees from a legal unit must not be able to gain *access* to another legal unit's *personal health data* through knowledge of user IDs and passwords. A risk assessment must document the measures that will be used.	

2.11 Remote administration

This section describes the configuration and use of a solution for remote administration.

2.11.1 Configuration control (chapter 5.5.1 of the Code)
"Configuration control shall be regulated through an agreement in connection with the use of remote access for maintenance and updates."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Use of *remote administration* shall be agreed with the *supplier*. The agreement shall describe how the configuration control will be safeguarded. The tool that is used must have active configuration control that cannot be overridden by the service associate. In connection with the use of tools for *remote administration*, the *organization* shall configure the solution so that the *supplier* cannot use functions other than those agreed in advance. Connection and use of tools for *remote administration* should generally be accepted from the *organization* as an active action in each case.	The *supplier* shall relate to the *configuration* that has been agreed and the procedure for change management. The *supplier* shall only use the solution for *remote access* as agreed in advance.	

2.12 Requirements for incident registration

This section presents a description of the requirements for *incident registration* for all components/solutions that are used in connection with *remote access*.

2.12.1 Incident registration (chapter 5.5.2 of the Code)
"To detect breaches or attempted breaches of the regulations, incident registers shall be maintained of at least the following:

- Authorized use of the information systems must be recorded.
- The security barriers must record incidents pertinent to security, including attempted unauthorized use of the information system.

- Network operating systems shall record all cases of attempted unauthorized use.
- All information systems shall record all cases of attempted unauthorized use.
- The use of emergency access to personal health data filing systems for therapeutic purposes shall be recorded.
- The incident registers shall be protected from change and deletion by unauthorized personnel.

At least the following shall be recorded in incident registers:
- unique identifier for the *authorized* user
- the role that the *authorized* user performs in connection with the *access*
- activity affiliation
- organizational affiliation of the person who is authorized
- the type of information to which *access* has been given
- the basis for the *access*
- time and duration of the *access"*

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Incident registration must be implemented such that it is possible to detect and resolve security breaches. In the *organization's* systems and networks, the following incidents must be recorded in connection with authorized use: • unique identifier for the *authorized* user • the role that the *authorized* user performs in connection with the *access* • organization affiliation • organizational affiliation of the person who is authorized • the type of information to which *access* has been given • the basis for the *access* • time and duration of the *access* In the event of remote access from the *supplier*, the following incidents shall also be registered: • Initiated traffic with respect to IP addresses and port number • Which data/data files have been downloaded to the *supplier* (data files) or uploaded to the *organization* (application files and patches) • Unique identifier for the person at the *supplier* who has used the relevant *remote access* The following incident registration shall be carried out concerning attempted unauthorized use:	All or part of the *incident registration* may be carried out by the *supplier* by agreement. The incident register may be the sum of the *supplier's incident register* and the *organization's incident register*.	Fact sheet 15 – Incident registration and follow-up

Implications for		References to fact sheets and guidelines
Organization	Supplier	
• The user identity that was used • Time (date and time) • IP address or other identification of PC/workstation which was used (e.g. MAC address or NAT address)		

2.13 Incident register review requirements

This section presents a description of the requirements for the review of and archiving period for *incident registers*.

2.13.1 Review of incident registers (chapter 5.2.6 of the Code)
"All authorized use and attempted unauthorized use of the information systems shall be recorded and the register retained for at least two years. It must be easy to analyse the *incident registers* using analysis tools for the purpose of detecting breaches.

Procedures to analyze *incident registers* shall be established such that incidents are detected before they can have serious consequences, ideally within one week."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *supplier* must prepare written routines for the review of the various *incident registers*. All incident registers shall be retained in electronic form for at least two years. The agreement between the *organization* and the *supplier* shall provide for the analysis of *incident registers*. It is particularly important to secure incident registers in the *specialized systems* with respect to the *supplier* having *access* to these systems in connection with other systems work within the *organization*. If unauthorized incidents are detected, a non-conformity report must be sent to the *supplier* immediately.	The *supplier* must prepare a written procedure for the review of the various *incident registers*. All incident registers shall be retained in electronic form for at least two years. The agreement between the *organization* and the *supplier* shall provide for the analysis of *incident registers*. If unauthorized incidents are detected, a non-conformity report must be sent to the *organization* immediately.	Fact sheet 15 – Incident registration and follow-up Fact sheet 3 – Overview of recommended procedures in the governance system

2.14 Analysis tools

This section describes the recommendations concerning the use of computer tools for analyzing the *incident registers*.

2.14.1 Analysis of incident registers (chapter 5.5.2 of the Code)
"It shall be possible to analyze all incident registers using suitable tools and, when necessary, to compare them against the *register of authorizations* and attendance register."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
The *organization* should use analysis tools for reviewing *incident registers*.	The *supplier* should use analysis tools for reviewing *incident registers*.	Fact sheet 15 – Incident registration and follow-up

2.15 Access to incident registers held by supplier

This section describes the requirements to ensure that the *organization* has *access* to the *supplier's incident registers*.

2.15.1 Access to the supplier's incident registers (chapter 5.3.4 of the Code)
"Procedures shall be established to ensure that the rights of the registered person as regards access to incident registers are safeguarded."

Implications for		References to fact sheets and guidelines
Organization	Supplier	
Through the agreement with the *supplier*, the *organization* shall have *access* to *incident registers* held by the *supplier*. The agreement must state how this shall take place.	The *supplier* shall establish a procedure to ensure that the *organization* and the registered person are given *access* to *incident registers*.	Fact sheet 50 – Access to incident registers Fact sheet 3 – Overview of recommended procedures in the governance system

3 TECHNICAL SOLUTIONS

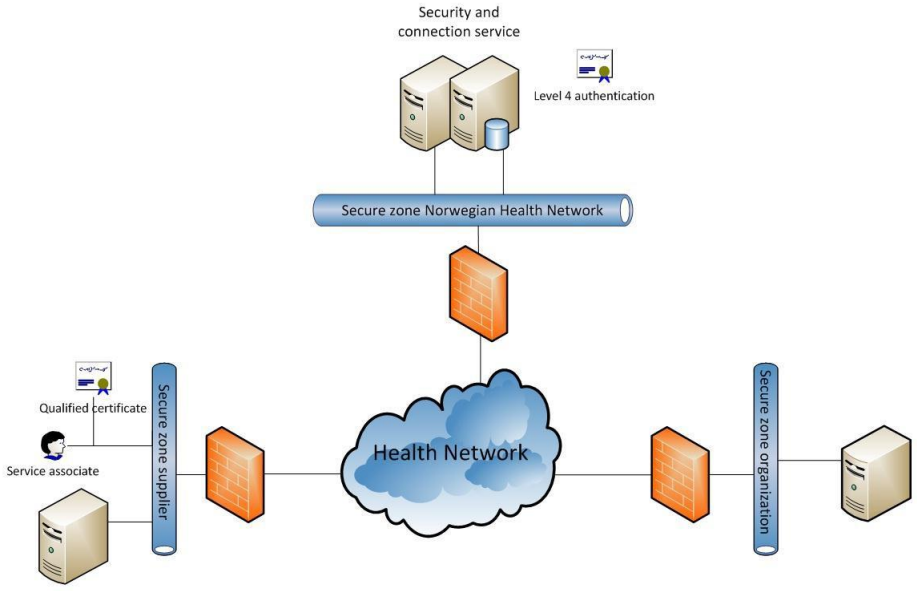
This chapter describes proposals for technical solutions that fulfil the requirements of the Code. The guideline illustrates a selection of solutions, but there may be other solutions that fulfil the requirements.

The examples below predominantly show solutions where the *supplier* connects to the *organization* via *remote access*. There are many solutions which automatically initiate contact with the *supplier's technical solution* (e.g. for reporting the status of information systems and infrastructure, the sending of error messages, etc.). On the basis of such contact, the *supplier* may initiate a connection with *remote access*. The actual solution for automatic contact is not described in the examples. Such solutions should be considered as any information system within the *organization* which has a connection to external networks.

3.1 Example 1 – Solution supplied by Norsk Helsenett

The example below shows the use of a tool for *remote administration* supplied by *Norsk Helsenett*. The figure illustrates that:

- The *organization* has installed a client for *remote administration* on a workstation
- The *organization* has opened for the outgoing IP address and port number for *Norsk Helsenett's* remote administration service
- *The organization* and the *supplier* initiate the connection to a defined server at *Norsk Helsenett*
- The *supplier* authenticates itself with respect to the service at *Norsk Helsenett* at *security level 4*
- The traffic is encrypted using functionality in the remote administration tool
- *Norsk Helsenett* has configured the remote administration tool on behalf of the *organization* so that the *supplier's access* is strictly limited and permitted for the actual purpose only
- All traffic shall be automatically or manually logged in the remote administration tool
- The *supplier* has support computers placed in a secure network
- The *health net* is used for communication



The table below shows who performs the security tasks in this example (chapter nos. and chapter titles are from this document):

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.1.1	Written agreement with supplier (chapter 5.8 of the Code)	☒	☒	☐
2.1.2	Statement of secrecy (chapter 5.8.3 of the Code)	☒	☐	☐
2.1.3	Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)	☒	☐	☐
2.1.4	Raising awareness of the duty of secrecy (chapter 5.1 of the Code)	☒	☐	☐
2.2.1	Risk assessment before access is granted (chapter 4.6 of the Code)	☒	☒	☐
2.2.2	Risk assessment in operations (chapter 6.2 of the Code)	☐	☒	☐
2.3.1	Training measures (section 5.6 of the Code)	☐	☒	☐
2.4.1	Internet service provider (chapter 5.7 of the Code)	☐	☒	☐
2.4.2	Limitation of traffic (chapter 5.7.1 of the Code)	☐	☒	☐
2.5.1	Encryption solution (chapter 5.4.4 of the Code)	☐	☒	☐
2.6.1	Solution for malicious software (chapter 5.8.3 of the Code)	☐	☒	☐
2.7.1	Access regulation (chapter 5.8.3 of the Code)	☐	☒	☐
2.7.2	Physical security measures (chapter 5.4.2 of the Code)	☐	☒	☐
2.8.1	Responsibility for allocating authorization (chapter 5.2.2 of the Code)	☒	☐	☐
2.8.2	Procedure for allocating authorization (chapter 5.2.2 of the Code)	☒	☒	☐
2.8.3	Authorization register (chapter 5.2.2 of the Code)	☒	☐	☐
2.9.1	Authentication with security level 4 (chapter 5.2.1 of the Code)	☐	☒	☐
2.9.2	Access control (chapter 5.2.3 of the Code)	☒	☒	☐
2.9.3	Use of authorization (chapter 5.5.2 of the Code)	☐	☒	☐
2.10.1	Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)	☐	☒	☐
2.10.2	Transfer of health and personal data abroad (chapter 1.0 of the Code)	☐	☒	☐
2.10.3	Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)	☐	☒	☐
2.11.1	Configuration control (chapter 5.5.1 of the Code)	☐	☒	☐

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.12.1	Incident registration (chapter 5.5.2 of the Code)	☐	☒	☐
2.13.1	Review of incident registers (chapter 5.2.6 of the Code)	☒	☒	☐
2.14.1	Analysis of incident registers (chapter 5.5.2 of the Code)	☒	☒	☐
2.15.1	Access to the supplier's incident registers (chapter 5.3.4 of the Code)	☒	☐	☐

For tasks and roles, see the service description for the remote access solution.

3.2 Example of technical solution – 2

The example below shows a connection via the Internet where the organization has control based on VPN.

The figure illustrates that:

- The supplier receives a PC from the organizations and uses the organization's home office solution
- The *organization* has control over, or has approved, the *supplier's* local security mechanisms, e.g. a locally installed VPN client with the *organization's* policy
- All communication is encrypted
- Access to *health and personal data* requires the user to identify themselves at *security level 4*

The table below shows who performs the security tasks in this example (chapter nos. and chapter titles are from this document):

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.1.1	Written agreement with supplier (chapter 5.8 of the Code)	☒	☐	☐
2.1.2	Statement of secrecy (chapter 5.8.3 of the Code)	☒	☐	☐
2.1.3	Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)	☒	☒	☐

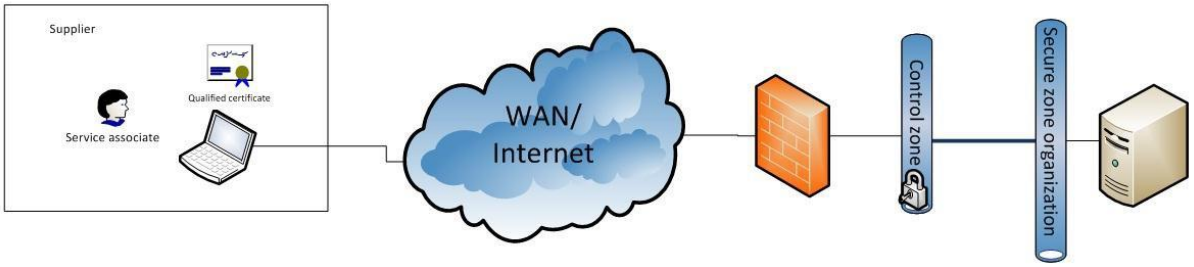
Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.1.4	Raising awareness of the duty of secrecy (chapter 5.1 of the Code)	☒	☒	☐
2.2.1	Risk assessment before access is granted (chapter 4.6 of the Code)	☒	☐	☐
2.2.2	Risk assessment in operations (chapter 6.2 of the Code)	☒	☐	☐
2.3.1	Training measures (section 5.6 of the Code)	☒	☐	☐
2.4.1	Internet service provider (chapter 5.7 of the Code)	☒	☐	☐
2.4.2	Limitation of traffic (chapter 5.7.1 of the Code)	☒	☐	☐
2.5.1	Encryption solution (chapter 5.4.4 of the Code)	☒	☐	☐
2.6.1	Solution for malicious software (chapter 5.8.3 of the Code)	☒	☐	☐
2.7.1	Access regulation (chapter 5.8.3 of the Code)	☒	☐	☐
2.7.2	Physical security measures (chapter 5.4.2 of the Code)	☐	☒	☐
2.8.1	Responsibility for allocating authorization (chapter 5.2.2 of the Code)	☒	☐	☐
2.8.2	Procedure for allocating authorization (chapter 5.2.2 of the Code)	☒	☐	☐
2.8.3	Authorization register (chapter 5.2.2 of the Code)	☒	☐	☐
2.9.1	Authentication with security level 4 (chapter 5.2.1 of the Code)	☒	☐	☐
2.9.2	Access control (chapter 5.2.3 of the Code)	☒	☐	☐
2.9.3	Use of authorization (chapter 5.5.2 of the Code)	☒	☐	☐
2.10.1	Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)	☒	☒	☐
2.10.2	Transfer of health and personal data abroad (chapter 1.0 of the Code)	☒	☒	☐
2.10.3	Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)	☒	☒	☐
2.11.1	Configuration control (chapter 5.5.1 of the Code)	☒	☐	☐
2.12.1	Incident registration (chapter 5.5.2 of the Code)	☒	☒	☐
2.13.1	Review of incident registers (chapter 5.2.6 of the Code)	☒	☐	☐
2.14.1	Analysis of incident registers (chapter 5.5.2 of the Code)	☒	☐	☐
2.15.1	Access to the supplier's incident registers (chapter 5.3.4 of the Code)	☒	☒	☐

3.3 Example of technical solution – 3

The example below shows a link via the Internet based on handling security in a control zone within the organization.

The figure illustrates that:

- The enterprise has no control over the supplier's user equipment
- All communication is encrypted
- The enterprise has a control zone which contains the necessary security mechanisms and prevents direct communication from the supplier's user equipment to the enterprise's systems, e.g. VDI/TS
- Access to patient data requires the user to identify themselves at security level 4



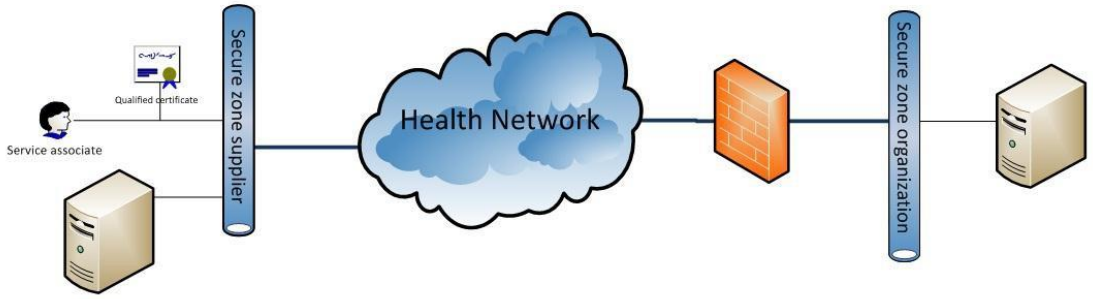
The table below shows who performs the security tasks in this example (chapter nos. and chapter titles are from this document):

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.1.1	Written agreement with supplier (chapter 5.8 of the Code)	☒	☐	☐
2.1.2	Statement of secrecy (chapter 5.8.3 of the Code)	☒	☐	☐
2.1.3	Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)	☒	☒	☐
2.1.4	Raising awareness of the duty of secrecy (chapter 5.1 of the Code)	☒	☒	☐
2.2.1	Risk assessment before access is granted (chapter 4.6 of the Code)	☒	☐	☐
2.2.2	Risk assessment in operations (chapter 6.2 of the Code)	☒	☐	☐
2.3.1	Training measures (section 5.6 of the Code)	☒	☐	☐
2.4.1	Internet service provider (chapter 5.7 of the Code)	☒	☐	☐
2.4.2	Limitation of traffic (chapter 5.7.1 of the Code)	☒	☐	☐
2.5.1	Encryption solution (chapter 5.4.4 of the Code)	☒	☐	☐
2.6.1	Solution for malicious software (chapter 5.8.3 of the Code)	☒	☐	☐

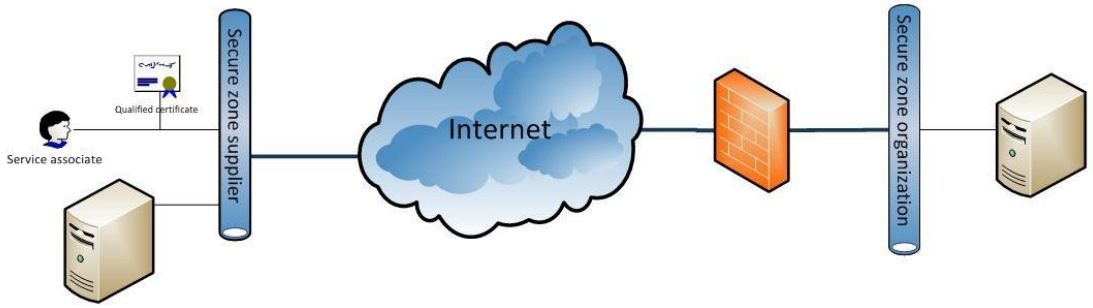
Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.7.1	Access regulation (chapter 5.8.3 of the Code)	☒	☐	☐
2.7.2	Physical security measures (chapter 5.4.2 of the Code)	☐	☒	☐
2.8.1	Responsibility for allocating authorization (chapter 5.2.2 of the Code)	☒	☐	☐
2.8.2	Procedure for allocating authorization (chapter 5.2.2 of the Code)	☒	☐	☐
2.8.3	Authorization register (chapter 5.2.2 of the Code)	☒	☐	☐
2.9.1	Authentication with security level 4 (chapter 5.2.1 of the Code)	☒	☐	☐
2.9.2	Access control (chapter 5.2.3 of the Code)	☒	☐	☐
2.9.3	Use of authorization (chapter 5.5.2 of the Code)	☒	☐	☐
2.10.1	Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)	☒	☒	☐
2.10.2	Transfer of health and personal data abroad (chapter 1.0 of the Code)	☒	☒	☐
2.10.3	Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)	☒	☒	☐
2.11.1	Configuration control (chapter 5.5.1 of the Code)	☒	☐	☐
2.12.1	Incident registration (chapter 5.5.2 of the Code)	☒	☒	☐
2.13.1	Review of incident registers (chapter 5.2.6 of the Code)	☒	☐	☐
2.14.1	Analysis of incident registers (chapter 5.5.2 of the Code)	☒	☐	☐
2.15.1	Access to the supplier's incident registers (chapter 5.3.4 of the Code)	☒	☒	☐

3.4 Example of technical solution – 4

Site-to-Site VPN solution via Norsk Helsenett



Site-to-Site VPN solution via the Internet



Communication between the Supplier and customer takes place via an IPsec-secured VPN connection.

The communication may be routed either via Norsk Helsenett or via the Internet.

Authentication of service associates takes place at security level 4 at the supplier, e.g. PKI log-on.

Example of use:

1. Customer reports error on a system to a supplier
Supplier's service associate logs on to the system via the supplier's remote diagnosis system. This log-in gives limited access to the system. Using tools on the system, the service associate can analyse error logs. After some analysis, it is concluded that a job must be carried out on the system. The customer then opens up extended access so that the service associate can perform the necessary tasks. This could be a change to the configuration, the uploading of software patches or the downloading of special files. After the service has been completed, the system is restored to limited access and the service associate logs off.

2. Customer system is in need of software update
The supplier has an update for the software on the customer's system. This could be an antivirus patch, a Windows hotfix or another bug fix for the system. The supplier's remote

diagnosis system will send the update to the customer's system. The customer brings up a message on the system indicating that an update is available and must actively decide whether or not this update should be installed. After installation, the customer's system will automatically report back to the supplier's remote diagnosis system that the update has been implemented.

3. Proactive monitoring of key parameters
The customer's system sends regular reports to the supplier's remote diagnosis system with information on the status of the system. These reports may contain data concerning temperature, pressure, level, spare database capacity, error messages which occur, etc.

The table below shows who performs the security tasks in this example (chapter nos. and chapter titles are from this document):

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.1.1	Written agreement with supplier (chapter 5.8 of the Code)	☐	☒	☐
2.1.2	Statement of secrecy (chapter 5.8.3 of the Code)	☐	☒	☐
2.1.3	Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)	☒	☒	☐
2.1.4	Raising awareness of the duty of secrecy (chapter 5.1 of the Code)	☐	☒	☐
2.2.1	Risk assessment before access is granted (chapter 4.6 of the Code)	☒	☒	☐
2.2.2	Risk assessment in operations (chapter 6.2 of the Code)	☒	☒	☐
2.3.1	Training measures (section 5.6 of the Code)	☐	☒	☐
2.4.1	Internet service provider (chapter 5.7 of the Code)	☒	☐	☐
2.4.2	Limitation of traffic (chapter 5.7.1 of the Code)	☒	☒	☐
2.5.1	Encryption solution (chapter 5.4.4 of the Code)	☐	☒	☐
2.6.1	Solution for malicious software (chapter 5.8.3 of the Code)	☐	☒	☐
2.7.1	Access regulation (chapter 5.8.3 of the Code)	☐	☒	☐
2.7.2	Physical security measures (chapter 5.4.2 of the Code)	☐	☒	☐
2.8.1	Responsibility for allocating authorization (chapter 5.2.2 of the Code)	☐	☒	☐
2.8.2	Procedure for allocating authorization (chapter 5.2.2 of the Code)	☐	☒	☐
2.8.3	Authorization register (chapter 5.2.2 of the Code)	☐	☒	☐
2.9.1	Authentication with security level 4 (chapter 5.2.1 of the Code)	☐	☒	☐
2.9.2	Access control (chapter 5.2.3 of the Code)	☐	☒	☐
2.9.3	Use of authorization (chapter 5.5.2 of the Code)	☐	☒	☐

Chapter no.	Chapter title	Performed by:		
		Organization	Supplier	Not relevant
2.10.1	Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)	☒	☒	☐
2.10.2	Transfer of health and personal data abroad (chapter 1.0 of the Code)	☒	☒	☐
2.10.3	Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)	☐	☒	☐
2.11.1	Configuration control (chapter 5.5.1 of the Code)	☐	☒	☐
2.12.1	Incident registration (chapter 5.5.2 of the Code)	☐	☒	☐
2.13.1	Review of incident registers (chapter 5.2.6 of the Code)	☒	☒	☐
2.14.1	Analysis of incident registers (chapter 5.5.2 of the Code)	☒	☒	☐
2.15.1	Access to the supplier's incident registers (chapter 5.3.4 of the Code)	☒	☒	☐

4 AGREEMENTS AND PROCEDURES

4.1 Agreements and routines in general

A written agreement shall be established between the *organization* and the *supplier*. The agreements shall include obligations which require the parties to fulfil the requirements and measures that follow from the applicable Code for information security at the time in question, as well as the regulation of penalties in the event of a breach of the Code and the agreement in general.

Individual tasks must be documented in procedures (see section 4.3 for determining which procedures must be established).

4.2 Agreements

When the *organization* enters into an agreement with the *supplier* regarding maintenance and updates, an agreement type must be used that has the correct legal wording. In such agreements, it is important that the *organization* ensures that the requirements of the Code are addressed.

Recommended elements of the agreement:

No.	Element	Incorporated
1.	Who the agreement concerns	☐Yes ☐No
2.	The purpose of the agreement or special agreement	☐Yes ☐No
3.	Responsible individuals/roles	☐Yes ☐No
4.	The *organization* will have access to the *supplier's* documentation of security objectives and strategy	☐Yes ☐No
5.	The *organization* will have right of access to the *supplier's* solution for compliance with the Code	☐Yes ☐No
6.	The *organization* will have right of access to the *supplier's* incident registers	☐Yes ☐No
7.	*Duty of secrecy* for the *supplier's* personnel	☐Yes ☐No
8.	The procedures that apply to the *remote access* solution	☐Yes ☐No
9.	Procedures for *non-conformity* management	☐Yes ☐No
10.	Consequences in cases of agreement breaches	☐Yes ☐No
11.	Summary of which systems *remote access* applies to	☐Yes ☐No
12.	Description of equipment that the *supplier* can use for *remote access* and ownership of the equipment	☐Yes ☐No
13.	Impact assessment in the case of deliberately dropped connections while using the remote connection	☐Yes ☐No

4.3 Procedures

Both the *supplier* and *organization* must establish procedures before *remote access* is established. The procedures must be available for both parties.

Relevant procedures:

No.	Element	Fact sheets	Incorporated	Responsibility
1.	Signing of statement of secrecy and confirmation that the security directive has been read and accepted		☐Yes ☐No	
2.	Training of *service associates*		☐Yes ☐No	
3.	Administration of *authorization* for equipment used for *remote access*	14	☐Yes ☐No	
4.	Use of solution for *security level 4*	24	☐Yes ☐No	
5.	Non-conformity management in connection with *remote access*	8	☐Yes ☐No	
6.	*Incident registration* and follow-up of incident registers	15	☐Yes ☐No	
7.	Erasing of files retrieved from the *organization*	34	☐Yes ☐No	
8.	Destruction of storage media upon disposal	34	☐Yes ☐No	
9.	Tasks that may be carried out upon connection/establishment of *remote access* (see the checklist in section 5 Appendices)		☐Yes ☐No	
10.	Granting of *authorization* for network, equipment and systems		☐Yes ☐No	
11.	*Authentication* of *service associates* at *supplier*	14	☐Yes ☐No	
12.	Control of granted *authorizations*		☐Yes ☐No	
13.	Tasks that must be performed upon connection/establishment of *remote access* (see the checklist in section 5 Appendices)		☐Yes ☐No	

The following procedures may be relevant in connection with training:

No.	Procedure
1.	Configuration control
2.	Ordering, alteration and deletion of user accounts
3.	Establishment and maintenance of *register of authorizations*
4.	Prevention of the destruction of software
5.	*Incident registration*
6.	Deletion of *health and personal data*
7.	Use of portable computer equipment
8.	Requirements for ICT suppliers in connection with *remote access*
9.	Handling of mobile storage media (internally at the *supplier*)
10.	Use of wireless technology
11.	Connection of *suppliers* for *remote access*

No.	Procedure
12.	Statement of secrecy and form for *authorization* of *service associates* for *remote access*
13.	Non-conformity management

5 APPENDICES

5.1 Checklist for establishment of connection

Chapter no.	Chapter title	Executed	Comments
2.1.1	Written agreement with supplier (chapter 5.8 of the Code)	☐Yes ☐No	
2.1.2	Statement of secrecy (chapter 5.8.3 of the Code)	☐Yes ☐No	
2.1.3	Security audits and non-conformity management (chapters 5.8.3, 6.1 and 6.3 of the Code)	☐Yes ☐No	
2.1.4	Raising awareness of the duty of secrecy (chapter 5.1 of the Code)	☐Yes ☐No	
2.2.1	Risk assessment before access is granted (chapter 4.6 of the Code)	☐Yes ☐No	
2.2.2	Risk assessment in operations (chapter 6.2 of the Code)	☐Yes ☐No	
2.3.1	Training measures (section 5.6 of the Code)	☐Yes ☐No	
2.4.1	Internet service provider (chapter 5.7 of the Code)	☐Yes ☐No	
2.4.2	Limitation of traffic (chapter 5.7.1 of the Code)	☐Yes ☐No	
2.5.1	Encryption solution (chapter 5.4.4 of the Code)	☐Yes ☐No	
2.6.1	Solution for malicious software (chapter 5.8.3 of the Code)	☐Yes ☐No	
2.7.1	Access regulation (chapter 5.8.3 of the Code)	☐Yes ☐No	
2.7.2	Physical security measures (chapter 5.4.2 of the Code)	☐Yes ☐No	
2.8.1	Responsibility for allocating authorization (chapter 5.2.2 of the Code)	☐Yes ☐No	
2.8.2	Procedure for allocating authorization (chapter 5.2.2 of the Code)	☐Yes ☐No	
2.8.3	Authorization register (chapter 5.2.2 of the Code)	☐Yes ☐No	
2.9.1	Authentication with security level 4 (chapter 5.2.1 of the Code)	☐Yes ☐No	
2.9.2	Access control (chapter 5.2.3 of the Code)	☐Yes ☐No	
2.9.3	Use of authorization (chapter 5.5.2 of the Code)	☐Yes ☐No	
2.10.1	Transfer of health and personal data to a supplier (chapter 5.8.2 of the Code)	☐Yes ☐No	
2.10.2	Transfer of health and personal data abroad (chapter 1.0 of the Code)	☐Yes ☐No	
2.10.3	Separating health and personal data from a number of organizations (chapter 5.8.2 of the Code)	☐Yes ☐No	
2.11.1	Configuration control (chapter 5.5.1 of the Code)	☐Yes ☐No	
2.12.1	Incident registration (chapter 5.5.2 of the Code)	☐Yes ☐No	
2.13.1	Review of incident registers (chapter 5.2.6 of the Code)	☐Yes ☐No	
2.14.1	Analysis of incident registers (chapter 5.5.2 of the Code)	☐Yes ☐No	
2.15.1	Access to the supplier's incident registers (chapter 5.3.4 of the Code)	☐Yes ☐No	

5.2 Example of risk assessment for organization

In this example, the general acceptance criteria in Table 1 in "Fact sheet 5 – Determining acceptance criteria for accessibility, confidentiality, integrity and quality" have been used as a basis.

RISK ASSESSMENT

Organization: Helsevirksomheten AS	
Assessed by: ICT manager	**Date:** 31 May 2012
Purpose of the risk assessment:	Creating a remote access solution

	Issues assessed (undesired incident/scenario)	**Probability** 1 = Unlikely; 2 = Less likely; 3 = Possible; 4 = Likely	**Consequence** 1 = Insignificant; 2 = Moderate; 3 = Serious; 4 = Critical	**Risk level**	**Measure Always Yes when High**
1.	Unauthorized *access* to the *organization's* network due to lack of authentication using *security level 4* (level 2 only used)	☐ 1 ☐ 2 ☐ 3 ☒ 4	☐ 1 ☐ 2 ☒ 3 ☐ 4	☐ Low ☐ Medium ☒ High	☒ Yes ☐ No
2.	No or inadequate encryption of data communication	☐ 1 ☐ 2 ☒ 3 ☐ 4	☐ 1 ☐ 2 ☒ 3 ☐ 4	☐ Low ☐ Medium ☒ High	☒ Yes ☐ No
3.	No or inadequate *incident registration* of firewall	☐ 1 ☒ 2 ☐ 3 ☐ 4	☐ 1 ☒ 2 ☐ 3 ☐ 4	☒ Low ☐ Medium ☐ High	☐ Yes ☒ No
4.	Lack of change/configuration management with the consequence of unintended downtime	☐ 1 ☐ 2 ☒ 3 ☐ 4	☐ 1 ☐ 2 ☒ 3 ☐ 4	☐ Low ☐ Medium ☒ High	☒ Yes ☐ No

	Description of measures *(No. 1 has the highest priority)*	**Significance/ Remarks**	**Ref. line no. above**
1.	Establish solution for authentication at security level 4	Investigate technical solution Install and implement procedures Ensure that suppliers order security level 4	1
2.	Establish obligatory encryption from firewall receipt	Activate approved encryption	2
3.	Establish procedure for change management and documentation of faults	New procedures in quality system Training of associates and service associates	4

5.3 Example of risk assessment for the supplier

In this example, the general acceptance criteria in Table 1 in "Fact sheet 5 – Determining acceptance criteria for accessibility, confidentiality, integrity and quality" have been used as a basis.

RISK ASSESSMENT

Organization: Fagsystemleverandøren AS	
Assessed by: Remote access manager	**Date: 3**1 May 2012
Purpose of the risk assessment:	Connection of remote access to Helsevirksomheten AS

	Issues assessed (undesired incident/scenario)	**Probability** 1 = Unlikely; 2 = Less likely; 3 = Possible; 4 = Likely	**Consequence** 1 = Insignificant; 2 = Moderate; 3 = Serious; 4 = Critical	**Risk level**	**Measure Always Yes when High**
1.	Unauthorized delivery of *health and personal data* with consequences for confidentiality	☐ ☐ ☒ ☐ (1 2 3 4)	☐ ☐ ☒ ☐ (1 2 3 4)	☐Low ☐Medium ☒High	☒Yes ☐No
2.	Transfer of malicious software from the *supplier* to the *organization*	☐ ☒ ☐ ☐ (1 2 3 4)	☐ ☒ ☐ ☐ (1 2 3 4)	☒Low ☐Medium ☐High	☐Yes ☒No
3.	No or inadequate encryption of data communication with the consequence that authentication data and health and personal data may go astray	☐ ☐ ☒ ☐ (1 2 3 4)	☐ ☐ ☒ ☐ (1 2 3 4)	☐Low ☐Medium ☒High	☒Yes ☐No
4.	No or deficient *incident registration*	☒ ☐ ☐ ☐ (1 2 3 4)	☐ ☐ | ☐ (1 2 3 4)	☒Low ☐Medium ☐High	☐Yes ☐No
5.	The processing of *health and personal data* obtained from the *organization* will be carried out on an open network with the supplier due to a lack of logical separation in the *supplier's* network	☐ ☒ ☐ ☐ (1 2 3 4)	☐ ☐ ☒ ☐ (1 2 3 4)	☐Low ☒Medium ☐High	☒Yes ☐No

	Description of measures *(No. 1 has the highest priority)*	**Significance/ Remarks**	**Ref. line no. above**
1.	Prepare procedures for the use of remote access and carry out training	Involve all relevant service associates	1
2.	Establish approved encryption	Implement encryption in VPN	3
3.	Establish logical separation in the network/remote access solution between the various customers and between the supplier's own organization	Investigate technology. Procure and install solution Implement procedure and training	5

5.4 Suggested content for maintenance agreement

The suggestions may be used as appendices to the government's standard agreements (see http://www.difi.no/statens-standardavtaler-ssa).

In the text below, the term 'customer' is used to refer to the *organization*, so that the relevant appendix is correct in relation to the remaining content of the agreement.

Suggested content for appendices in maintenance agreements:

During the establishment and use of a solution for *remote access*, requirements in the "Code of conduct for information security" (the Code) of 2 June 2010 shall apply.

Both the *supplier* and the customer have an independent responsibility to comply with the Code.

The customer must have full access to the *supplier's*:

- Security objectives and strategy
- Technical and organizational solutions for *remote access*
- Procedures that apply for *remote access*
- Results of risk assessment and security audits
- Incident registers

The requirements of the Code shall be addressed by *the supplier* (ref. chapter 5.8.3 of the Code):

- The *supplier's* personnel have signed a statement of secrecy requiring an absolute *duty of secrecy* with respect to all *health personal data*
- The *supplier* complies with the *Code* with respect to the *data controller's* obligations regarding security audits and non-conformity management
- The *supplier's* equipment that is used for online connection using a communication network or portable equipment connected to the *organization's* equipment does not contain malicious software, viruses etc., and that the equipment is secured against *access* from unauthorized persons
- The *availability* of *health and personal data* shall as far as possible be maintained when the *supplier* performs work on *the organization's* equipment/software, so that *the organization's* processing of tasks is maintained

The following elements have been incorporated in the agreement:

No.	Element	Incorporated
1.	Who the agreement concerns	☐Yes ☐No
2.	The purpose of the agreement or special agreement	☐Yes ☐No
3.	Responsible individuals/roles	☐Yes ☐No
4.	The *organization* will have access to the *supplier's* documentation of security objectives and strategy	☐Yes ☐No
5.	The *organization* will have right of access to the *supplier's* solution for	☐Yes ☐No

No.	Element	Incorporated
	compliance with the Code	
6.	The *organization* will have right of access to the *supplier's* incident registers	☐Yes ☐No
7.	*Duty of secrecy* for the *supplier's* personnel	☐Yes ☐No
8.	The procedures that apply to the *remote access* solution	☐Yes ☐No
9.	Procedures for *non-conformity* management	☐Yes ☐No
10.	Consequences in cases of agreement breaches	☐Yes ☐No
11.	Summary of which systems *remote access* applies to	☐Yes ☐No
12.	Description of equipment that the *supplier* can use for *remote access* and ownership of the equipment	☐Yes ☐No
13.	Impact assessment in the case of deliberately dropped connections while using the remote connection	☐Yes ☐No

The following procedures have been incorporated:

No.	Element	Incorporated	Responsibility
1.	Signing of statement of secrecy and confirmation that the security directive has been read and accepted	☐Yes ☐No	
2.	Training of *service associates*	☐Yes ☐No	
3.	Administration of *authorization* for equipment used for *remote access*	☐Yes ☐No	
4.	Use of solution for strong *authentication*	☐Yes ☐No	
5.	Non-conformity management in connection with *remote access*	☐Yes ☐No	
6.	*Incident registration* and follow-up of incident registers	☐Yes ☐No	
7.	Erasing of files retrieved from the *organization*	☐Yes ☐No	
8.	Destruction of storage media upon disposal	☐Yes ☐No	
9.	Tasks that may be performed upon connection/establishment of *remote access* (see the checklist in section 5 Appendices)	☐Yes ☐No	
10.	Granting of *authorization* for network, equipment and systems	☐Yes ☐No	
11.	*Authentication* of *service associates* at *supplier*	☐Yes ☐No	
12.	Control of granted *authorizations*	☐Yes ☐No	
13.	Tasks that must be performed upon connection/establishment of *remote access* (see the checklist in section 5 Appendices)	☐Yes ☐No	

5.5 Example of elements contained in a security directive

Security directive

(The example applies to individual service associates)

Rules for the use of IT equipment and software

- The IT equipment used in connection with remote access shall be connected to the supplier's network and must be logically separated from the supplier's internal company networks and other customers.
- It is not permitted to connect or use private IT equipment or software for <the organization>.
- As a service associate, you are obliged to prevent unauthorized persons from gaining access to the solutions that may be used with the <organization>.
- The downloading of health and personal data from the <organization> is not permitted unless regulated by a data processing agreement and in line with the methods specified in the data processor agreement.

User accounts and passwords

- You are obliged to protect authentication information (e.g. user names and passwords, etc.) in order to prevent them from being disclosed to others.
- Unauthorized access to remote access and the <organization's> technical systems or infrastructure by using the authentication of another service associate is not permitted.
- There are rules governing the requirements for passwords in the <organization>, which must be followed.

The workplace – security on the premises – logging out

- Always log out or activate a password-protected screensaver when you leave your workstation.
- Ensure that you obtain an overview of the health and personal data that you are handling. Do not allow health and personal data to be moved at random; this data must instead be protected in accordance with the applicable procedures.

Erroneous deletion of information

- In the event that you erroneously delete information, the <organization> must be notified without delay.

Incident registration

- <The organization> is obliged to register incidents concerning data traffic and activities in the network in order to maintain information security.

Extracts and copying

- Do not allow printouts to remain in the vicinity of the printer such that unauthorized persons can gain access to the content.
- Extracts of health and personal data shall be shredded in a satisfactory manner when no longer required.

Non-conformity management

- Breaches of security and accidents must be reported to the <organization> as a non-conformity without delay.
- Observe the applicable procedures for non-conformity management.

5.6 Participants in the reference group

The following people have participated in the reference group:

Name	E-mail	Role/position	Organization
Andre Meldal	andre.meldal@nhn.no	Security engineer	Norsk Helsenett SF
Frode Olsen	frode.olsen@farmait.no	IT consultant	FarmaIT
Geir Hovind	geihov@sykehuspartner.no	Section manager – risk management, security and compliance	Sykehuspartner
Hallgeir Nisja	hallgeir.nisja@hemit.no	IT security consultant/Data protection officer	Hemit – Central Norway Regional Health Authority IT
Hanne Kolflaath	hanne@acos.no	Business manager, Living conditions	Acos
Jan Gunnar Broch	jangunnar.broch@helsedir.no	Senior consultant	Directorate of Health
Kjell Inge Hestad	Kjell.Inge.Hestad@visma.no	IT manager	Visma
Ole Erik Dammen	ole.erik.dammen@ compugroupmedical.no	Contracts manager	CompuGroup Medical
Sven Egil Hauan	sven.e.hauan@siemens.com	SRS manager	Siemens
Sverre Biseth	sverre.biseth@med.ge.com	IT consultant	GE Healthcare
Nils Jensson	nils.jensson@helse-vest-ikt.no	IT consultant	Western Norway Regional Health Authority ICT