NORMEN

Code of conduct for information security and data protection in the healthcare and care services sector

Version 6.1

Applicable from 21/11/2022

Published with the support of

Direktoratet for e-helse

Publication title:
Code of conduct for information security and data protection in the healthcare and care services sector

Version number
6.1

Approved by the Steering Committee:
21/09/2022

Applicable from:
21/09/2022

Published with the support of:
Norwegian Directorate of eHealth

Contact:
sikkerhetsnormen@ehelse.no

Download the publication here:
www.normen.no

Preface

In the healthcare and care services sector, large quantities of data are processed as a basis for the development and provision of high-quality healthcare and care services, health records, research and innovation.

This data must be processed to enable healthcare and care services to be provided appropriately and in a manner which also safeguards the trust of citizens in the sector. A high level of information security and data protection is essential for digitalisation. The sector must build and manage robust technology, organisation and security culture.

Set against the backdrop of new legislation, technological advances and high-profile incidents in recent years, there has been increasing awareness surrounding data protection and information security in the healthcare and care services sector. As a result, it has become apparent that there is a need for updated guidance and a modernised and updated Code of conduct for information security and data protection in the healthcare and care services sector (the Code).

This version of the Code is the result of a protracted revision and development process. The main objectives were to ensure that the requirements of the Code are comprehensive as regards the new requirements of the General Data Protection Regulation (GDPR), as well as being technology-neutral and compatible with current technology. A further important objective was to simplify the text and make the Code easier to read and more user-friendly. Amongst other things, new requirements have been incorporated, text has been deleted and requirements have been clarified or amended. The scope of the Code has been altered and the requirement for proportionality has been made clearer. The text has been reviewed and simplified, and some text has been deleted and moved to the guidance.

Contents

1 About the Code

1.1 What is information security and data protection?

The sharing of relevant patient data is a prerequisite for the provision of high-quality healthcare services. This data is needed to provide healthcare, quality assure healthcare and care services and learn lessons. Researchers need the data to develop better healthcare services.

A high level of patient safety requires data to be stored and shared between health personnel, the data to be accurate and up to date, and patients/healthcare users and health personnel to have confidence in systems and personnel. Inadequate information and failure in transitions within and between healthcare service levels have been documented as being a key risk area as regards good patient safety.[1]

Information security[2] is about managing risk relating to information and the processing of personal data. The integrity, availability and confidentiality of the information shall be ensured. Good information security is crucial to the provision of appropriate healthcare services.

> "Integrity" means, for the purposes of this Code, that personal health data is to be protected against accidental or unauthorised modification or deletion. Integrity is a prerequisite for high quality and appropriate healthcare.
>
> "Availability" means, for the purposes of this Code, that personal health data that is to be processed is accessible at the time and place where it is needed. For health personnel, access to information is a prerequisite for providing high-quality and appropriate healthcare.
>
> "Confidentiality" means, for the purposes of this Code, that personal health data must be protected from disclosure to unauthorised persons. Confidentiality helps to safeguard the duty of confidentiality and data protection, which is an important factor in maintaining the trust of citizens in the healthcare and care services.

The General Data Protection Regulation also uses the term 'robustness', as well as integrity, availability and confidentiality. For the purposes of the Code, "robustness" means the ability of the organisation and information systems to restore normal conditions following a physical or technical incident, for example. Robustness is achieved through appropriate technical and organisational measures which facilitate the prevention, detection, scalability, handling and restoration of personal data security and information security in general.

Data protection can be defined and described in various ways. However, from any perspective, the individual's inviolability and right to respect from other people, respect for

---

[1] "Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten": https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

2 For more information about the term 'information security', see the Norwegian Digitalisation Agency's web page (https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet) and the Norwegian Data Protection Authority's web page (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/)

their own integrity and personal privacy are pivotal. Privacy is therefore closely linked to the right of individuals to a private life, self-determination and self-expression.[3]

The theme for the Code is the aspects of data protection which concern the protection of personal data. The General Data Protection Regulation (GDPR) regulates personal data protection. Personal data shall be processed according to the principles of Article 5 of the GDPR (see section 2.2), and the rights of data subjects shall be safeguarded.

A key aspect of this is what Article 32 of the GDPR calls 'security of personal data'. This is the same as information security regarding personal data.

Within the framework of applicable legislation, the Code endeavours to achieve a balanced approach to confidentiality, availability, integrity and robustness.

1.2 What is the Code?

The Code is an industry code which has been prepared and is administered by organisations and enterprises in the healthcare and care services sector.

This version of the Code does not have the status of a Code of Conduct under Article 40 of the GDPR.

The Code is intended to contribute to a satisfactory level of information security and data protection amongst individual organisations, in joint systems and infrastructure and within the sector generally. The Code is intended to help ensure that an organisation which complies with and follows the Code has appropriate technical and organisational measures in place regarding information security and data protection for its processing of personal health data.

A further aim of the Code is to help ensure that organisations can have mutual confidence that the processing of personal health data by other organisations will be carried out with a satisfactory level of security. Those who interact with an enterprise that is obliged to comply with the requirements of the Code shall be able to be confident that the enterprise concerned has appropriate technical and organisational measures in place regarding information security and data protection for its processing of personal health data.

The Code is intended to ensure that patients, healthcare users, employees and other data subjects are guaranteed a high level of data protection.

The Code is an aid in the efforts of individual organisations relating to information security and data protection.

The Code is intended to support high-quality healthcare services, a high level of patient safety, quality assurance, the training of health personnel, strong data protection and the patient's healthcare service.

[3] For more about this, seehttps://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/ and www.datatilsynet.no

1.3 Who does the Code apply to?

The Code applies to any organisation which has undertaken to follow the Code through an agreement.

1.4 Relationship between the Code and the legislation

The legislation imposes requirements regarding information security and data protection. These requirements apply independently of the Code, and relevant supervisory authorities (particularly the Norwegian Data Protection Authority and the Norwegian Board of Health Supervision) continually monitor compliance with applicable regulations by individual organisations.

The Code does not cover all statutory requirements regarding information security, data protection and the processing of personal health data.

The legislation contains more requirements regarding information security, data protection and the processing of personal health data than those covered by the main theme of the Code, e.g. it covers more issues relating to the use of personal health data for purposes other than the provision of healthcare and care services, specific requirements regarding data filing systems which are covered by specific regulations, the legal basis for the processing of personal and health data and the obligations and requirements that apply regarding recordkeeping. Information security is also regulated in other legislation in addition to that which applies to the processing of personal data.

The requirements of the Code expand upon and supplement the applicable regulations.

Compliance with the requirements of the Code can be used to demonstrate fulfilment of the enterprise’s obligations under the regulations.

The Code includes limited references to the law. Statutory and regulatory stipulations in the Code can be found in the appendix “Overview of requirements set out in the Code”.

1.5 About the requirements set out in the Code

The Code describes the organisational and technical measures that are deemed to be appropriate in order to achieve a satisfactory level of information security and data protection in the sector.

When selecting appropriate technical and organisational measures, the enterprise shall consider the measures in relation to the size, nature and scope of the processing of personal health data, patient safety, risks etc. The measures must be selected based on risk assessments and the measures must be proportionate. This may mean that larger organisations that process personal data on a large scale should establish more measures than smaller organisations that process personal data on a small scale and where the risks are less complex and more manageable.

The Code provides further guidance for small healthcare enterprises on how small enterprises can work with information security and data protection in practice.[4]

The Code differentiates between "shall" and "should" requirements. "Shall" requirements apply to all. enterprises must consider whether or not "should" requirements apply to them.

The Code is not exhaustive with regard to the processing of personal health data where the purpose is not the provision of healthcare and care services[5], but relevant requirements regarding information security and data protection set out in the Code apply. The fundamental requirements regarding information security and data protection are essentially the same in legislation that regulates both personal health data filing systems for therapeutic purposes and other uses of personal health data. The enterprise shall assess which requirements in the Code apply based on the specific processing of personal health data.[6]

Organisations also process personal data concerning their own employees. The Code is not exhaustive as regards the processing of information concerning employees. The enterprise shall safeguard the privacy of employees in accordance with applicable laws and regulations. It is particularly important that data concerning employees' use of information systems (logging) is processed only pursuant to law, in order to avoid unnecessary monitoring of employees. Employees have a right to access data that concerns themselves (see Article 15 of the General Data Protection Regulation).

The Code contains requirements which cover most themes within information security and data protection; people, processes and technology. The Code also includes supporting documents in the form of guidance. The guidance material provides guidance and examples of measures; see Chapter 6.2.

The Appendix "Overview of the requirements set out in the Code" includes all "shall requirements" in the Code, statutory and regulatory stipulations, references to ISO 27001 and 27001 Annex A (2017), as well as other aids used when drawing up the Code.

1.6 Development and administration of the Code

The Code has been prepared and is administered by a steering committee from the healthcare and care services sector.[7]

Unanimity within the steering committee is sought when fundamental issues are considered.

The Directorate for eHealth is the secretariat for the work of the steering group, with permanent representation from the Norwegian health net (Norsk Helsenett).

[4] The Code's Guidance for small healthcare enterprises
[5] For example, the processing of health data for statistical purposes, health analyses, research, quality improvement, planning, governance and preparedness within the healthcare and care services administration and the healthcare and care services service.
[6] Section 3.1 Proportionality in connection with the selection of measures
[7] List of members: https://www.ehelse.no/normen/om-normen#Styringsgruppe

2 Management and responsibility

The senior management of the enterprise shall be responsible for ensuring that the enterprise complies with applicable requirements relating to information security and data protection and that the enterprise's information processing provides appropriate security levels with regard to the risk and nature of the processing.[8] This responsibility should be addressed as part of the work relating to corporate governance and quality improvement. This responsibility includes establishing guidelines for the assessment and management of risk, [9] including establishing criteria to accept risk, as well as ensuring well-functioning governance and control.

The enterprise shall document all measures.

Organisations that are covered by both the Code and the Regulation on management and quality improvement within the healthcare and care services sector (*forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten*) should use the provisions of this Regulation as a basis to ensure compliance with the requirements set out in applicable health and care legislation regarding information security and data protection.

2.1 Roles and responsibilities regarding information security and data protection

The senior management of the organisation shall ensure that roles and functions are established with sufficient resources and expertise to perform the tasks necessary in order to fulfil the responsibility. These tasks can be performed either by their own employees or by external parties.

The person responsible for a function or unit should also be responsible for following up information security and data protection within the function or unit.

The organisation shall decide which roles and functions regarding information security and data protection are necessary. It shall be clear who is responsible and what they are responsible for. Everyone shall be familiar with the tasks they are responsible for performing, and possess sufficient knowledge of the relevant responsibilities and tasks of others, and who has authority to make decisions.

Larger enterprises should have their own information security manager or security enterprise linked to the enterprise's management.

---

[8] cf. Article 32 of the GDPR: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate."

[9] Cf. ISO 27001 2017 Section 6.1.2, in particular Item a, and 6.1.3, cf. Section 15 of the regulations relating to electronic communication with and in public administration (based on recognised standards).

The senior management of public sector organisations shall ensure that a Data Protection Officer is appointed. For a private enterprise, senior management shall appoint a Data Protection Officer when necessitated by the scope, nature and purpose of information processing. This also applies to small enterprises. The Data Protection Officer may be an employee of the enterprise or an external party and perform the tasks on the basis of a service agreement.

The Data Protection Officer shall be given sufficient resources and access to relevant expertise in order to perform their tasks. The Data Protection Officer shall not have any conflicts of interest with respect to any other roles that the person performs within the enterprise, nor shall the Data Protection Officer receive any instructions regarding how the tasks are to be performed.

2.2 The controller's responsibilities

The controller is the entity which, alone or together with other enterprises, determines the purpose of the processing of personal health data and the means that are to be used.

The GDPR uses the term 'controller', which corresponds to the Norwegian term 'dataansvarlig' used by the Norwegian healthcare sector.

The controller shall:

- delegate authority and tasks (see section 2.1)
- establish and comply with the governing system (see section 2.4)
- conduct risk assessments and data protection impact assessments as and when necessary (see Chapter 3)
- safeguard the rights of data subjects (see Chapter 4)
- establish and document appropriate technical and organisational measures (see Chapter 5)
- enter into and follow up agreements (see section 5.7)
- manage non-conformities (see section 5.8)

The controller shall be responsible for acting in accordance with the principles of data protection. This means that personal health data shall:

- be processed lawfully (valid basis for processing)
- be processed fairly (with respect for data subjects' interests and rights)
- be processed in an open manner (clear, predictable and understandable information) with regard to the data subject (patient/healthcare user)
- only be registered for specific purposes, which shall be legitimate (such as the documentation of healthcare)
- be available to health personnel as and when necessary in order to provide appropriate healthcare
- be used only for the purposes for which it has been registered, unless there is a basis for processing for other purposes
- be relevant, adequate, accurate and, if necessary, up-to-date for the purposes for which it has been registered
- be stored in such a way that it is not possible to identify data subjects for periods longer than necessary for the purposes
- be protected against unauthorised access, alteration, destruction and dissemination

The controller shall demonstrate that the enterprise has implemented measures to comply with the GDPR.

2.3 The processor's responsibilities

A processor is an organisation that processes personal health data on behalf of the controller. In the same way as a controller, the processor has an independent responsibility for information security and for addressing data protection concerning data subjects.

The processor shall:

- only process personal health data in accordance with the controller's instructions
- not use subcontracted processors without the authorisation of the controller
- be responsible for ensuring that subcontractors fulfil their obligations
- help the controller to ensure fulfilment of obligations regarding information security

The processor shall assist the controller with regard to data protection and information security in order to maintain an acceptable level of security.

See more about processors in Chapter 5.7.3.[10]

2.4 Management system

All organisations shall have a management system for information security and data protection (internal control).

'Management system' means formalisation of the way in which the organisation plans, carries out, evaluates/controls and corrects compliance with relevant regulations, requirements and agreements.

Information security and data protection should be covered by the overall management system within the enterprise.

The management system shall be adapted to the enterprise's size, risks, characteristics and activities, the nature, scope and purpose of the data processing and the context in which it is carried out. This means that smaller organisations will not need as comprehensive a management system as large organisations.

The senior management is responsible for the management system and shall make this system known to all employees. The enterprise's senior management shall allocate sufficient funding and resources to enable necessary activities to be carried out.

The management system shall be documented. Documents specified in the management system shall be kept up to date on an ongoing basis and archived from the date on which the document is superseded by a new current version. This could, for example, be procedures

[10] See Fact sheet 10 about processors for more guidance, as well as a template for data processing agreements.

for security audits, risk assessments, operating routines, non-conformities and the way in which they are managed, the management's review, data processing agreements etc.

Documentation of risks and measures associated with information security shall be ensured based on the security needs that apply. If documentation must be shared with other enterprises, the controller must assess whether any detailed information that may have an impact on security should be removed prior to disclosure. The documentation shall be updated and available at all times.

All public sector organisations shall describe goals and establish an information security strategy. This strategy shall form the basis for the management system.

2.5 The management’s review

The organisation’s senior management shall review the organisation’s activities relating to information security and data protection at least once a year.

Such a review may be necessary in the event of:

- changes in the processing of personal health data (records)
- changes in the organisation of work
- results of risk assessments and data protection impact assessments
- result of non-conformity management
- follow-up of suppliers and data processing agreements
- changes to acceptable levels of risk etc.

If the review indicates that the ~~level~~ of risk to which the enterprise is exposed is unacceptabl~~e~~, action plans shall be adopted in order to remedy the situation, with deadlines and the delegation of responsibility.

The management’s review shall be documented.

3 Risk management

Risk management comprises coordinated activities to guide and control an organisation with regard to risk. It encompasses obtaining an overview of information and technology within the enterprise, identifying threats, vulnerabilities and consequences for the enterprise and the data subjects, as well as analysing risk and establishing measures to maintain appropriate levels of security.

The enterprise shall establish technical and organisational measures that are appropriate in order to manage risk in a satisfactory manner. This includes safeguarding confidentiality, integrity, availability and robustness in the information systems. These considerations shall be balanced.

When evaluating an acceptable level of risk, consideration shall be given to the technical developments, implementation costs and the nature, scope and purpose of information processing, as well as the context of processing. The work associated with risk management shall take into account e.g. the type and volume of data, the size of the enterprise and the complexity of the processing.

3.1 Proportionality in connection with the selection of measures

When selecting appropriate technical and organisational measures, the enterprise shall consider the measures in relation to the nature and scope of the processing of personal health data, patient safety, risks etc.

This particularly applies in connection with the assessment of an appropriate security organisation, tasks, control tasks and measures relating to information security (such as access management, logging, physical security, preparedness etc.).

The enterprise shall ensure that there is proportionality between risk and the cost of the measure.

3.2 Minimum requirements for safeguarding confidentiality, integrity, availability and robustness

The enterprise shall ensure that its processing of personal health data has an appropriate level of security in line with the minimum requirements set out in the Code with regard to information security and any separate security measures. The Code establishes the following overall minimum requirements regarding information security (confidentiality, integrity, availability and robustness):

Requirement to safeguard confidentiality
The enterprise shall ensure that the duty of confidentiality is fulfilled and that unauthorised persons do not gain access to data.

- prevent unauthorised access to personal health data and other information of significance to information security
- restrict access for authorised personnel according to their professional needs
- maintain an overview (logs) of everyone who has gained access to personal health data and other information of significance to information security

Requirement to safeguard integrity
The enterprise shall ensure that personal health data, as well as other information of significance to information security, is protected against accidental or unauthorised modification or erasure. Integrity is a prerequisite for good and proper healthcare

- log who has corrected, registered, altered and erased data
- prevent accidental or unauthorised alteration or erasure
- ensure that personal health data is recorded for the right person
- ensure that personal health data is registered in accordance with relevant code lists and terminology
- ensure that personal health data is correct and, if necessary, updated.
- prevent copies of data from becoming a source of outdated information

Requirement to safeguard availability and robustness
The organisation shall ensure that personal health data and other information of significance to information security is available at the right time.

- ensure that personal health data is available according to professional need
- ensure appropriate and stable operation of information systems
- ensure that appropriate technical and organisational measures are in place which enable prevention, detection, scalability, management and restoration
- ensure that information systems are available in accordance with the organisation's availability requirements

Breaches of the requirements shall be treated as a non-conformity.

3.3 Overview of technology and the processing of personal health data

By establishing and maintaining an overview of the personal health data that is processed and the technology that is used, the enterprise can identify potential risk areas it should pay particular attention to.

The enterprise shall have:

- A record of the processing of personal health data.[11]
- An overview of ICT systems, infrastructure, digital services and other information of significance to information security etc. The enterprise shall also map the consequences of non-availability and classify their systems in accordance with chapter 5.9. The overview should be documented.

[11] See Fact sheet 13 concerning records for guidance and template for records for controllers and processors.

Areas for risk assessment should be based on the overview of the personal health data that is processed and the overview of technology that is used.

3.4 Risk assessment and risk management

Risk assessments are a tool for identifying incidents. Risk assessments should be based on a survey of informational values and the consequences of incidents which could impact on the availability, integrity and confidentiality of informational values. The enterprise shall assess the probability and potential consequences of an incident occurring. If the risk is unacceptable, the enterprise shall implement measures to reduce the risk.[12]

The enterprise shall carry out risk assessments, including at least before the following:

- establishment of or changes to the processing of personal health data
- establishment of new systems or data filing systems which contain or use personal health data
- establishment of organisational, technical or other changes of significance for information security
- access to health data is established or changed across enterprises

Risk assessments should be updated in the event of a change in the threat landscape. The enterprise's management shall also regularly carry out risk assessments as part of its efforts to monitor information security.

Risk assessments and risk management shall be carried out on the basis of the minimum requirements regarding confidentiality, integrity, availability and robustness, as well as the enterprise's acceptance criteria. Decisive consideration shall be given in risk assessments to the consequences for patients/healthcare users and appropriate healthcare.

Risk assessments shall be documented. When it is necessary to implement measures in order to achieve an acceptable level of risk, the measures shall be presented in a plan with clear deadlines and the names of the persons who are responsible for implementation. The plan shall be endorsed by the enterprise's management.

If technical measures for achieving an acceptable level of risk are not implemented immediately, risk-mitigating administrative measures, e.g. in the form of procedures, should be considered.

The enterprise shall ensure that it has sufficient expertise at its disposal in order to assess risk. Representatives of those providing healthcare shall be involved where relevant. Persons who carry out risk assessments shall have a clear escalation path to the management/board. The results of the risk assessment and a plan for the follow-up of measures shall be communicated with the appropriate level of detail to the organisation's management and the board, as and when relevant.

[12] See Guidance to risk management in information security and data protection for guidance.

3.5 Assessment of data protection consequences

Organisations shall always evaluate the consequences that the processing of personal health data will entail for data subjects. The enterprise shall document the lawfulness and purpose of the processing, the way in which the privacy of the data subject is safeguarded and that sufficient measures have been implemented in order to manage the risk. If it is likely that processing will entail a high level of risk for the data subjects concerned, the enterprise shall carry out a more thorough impact assessment as regards data protection, also known as a 'DPIA'[13].

3.5.1 Data protection impact assessment

Data protection impact assessments shall be carried out before the processing of personal data commences.[14]

A high level of risk regarding data protection may arise

- when health data is processed on a large scale,
- if new technology is used,
- when personal data is processed in an automated, systematic and comprehensive manner, as a basis for decisions which have legal effect or a significant impact on the data subject, and
- as a result of the nature, scope and purpose of the processing and the context in which it is carried out.

The Norwegian Data Protection Authority has produced a list of processing activities that always require a data protection impact assessment to be carried out.

Data protection impact assessments shall at least include:

- a systematic description of the processing activities involving personal health data,
- a description of the purpose of the processing of personal data,
- an assessment of whether or not the processing of personal health data is necessary and proportionate to the purpose,
- an assessment of the data protection risks for the data subject, and
- planned risk mitigation measures in order to safeguard data protection.

The controller shall consult with the Data Protection Officer, if such an officer has been designated, in connection with the performance of a data protection impact assessment.

Measures which reduce the risk for data protection shall be planned. If the processing of personal health data will entail a high level of risk which cannot be mitigated through reasonable measures, the controller shall request an advance discussion with the Norwegian Data Protection Authority before the processing is commenced.

---

[13] Data Protection Impact Assessment

[14] For further information and guidance on when to conduct a data protection impact assessment, please refer to the Norwegian Data Protection Authority's website.

4 Fundamental considerations regarding the processing of personal health data

Patient care requires the processing of health data about the patient. The duty to document patient care is intended to help ensure that patients and healthcare users receive high-quality healthcare and care services and to support health personnel in connection with the provision of healthcare to individual patients. The safeguarding of patient privacy is also important as regards patient safety in that medical records must be relevant, accurate and up-to-date.

The health sector has numerous laws and regulations which contain specific rules regarding the processing of personal health data, and these supplement the requirements of the personal data legislation. Health legislation is largely based on the rights of patients and healthcare users and the obligations of organisations. The Code is delimited to encompass key rights and obligations in the legislation that concern the processing of personal data.[15]

The duty of confidentiality of health personnel is a key aspect of data protection and a prerequisite for the essential relationship of trust between patients and health personnel.

4.1 Basis for processing

Personal data may only be processed when permitted by law. All processing of personal data shall have a lawful basis. In the GDPR, this is known as a 'basis for processing'.

The processing of special categories of personal data, such as health data, is essentially prohibited under the GDPR. However, exceptions apply, e.g. when consent is given, when healthcare and social services covered by the duty of confidentiality are provided, when public health considerations render it necessary, and for research purposes.[16]

Before the processing of personal health data commences and in the event of changes to such processing, the controller shall ensure that a valid basis for processing exists. The basis for processing shall cover all types of processing that is performed: collection, recording, storage, erasure, disclosure etc. If the data is to be used for any purpose other than the original purpose, this must have a separate basis for processing.

Article 6 of the GDPR refers to six grounds for processing:[17]

- The data subject has consented to the processing.
- Processing is necessary for the performance of a contract to which the data subject is party.

[15] The Directorate of Health's circulars on the Health Personnel Act and the Patient and User Rights Act
[16] See more grounds for processing (Articles 6 and 9 of the GDPR) at www.datatilsynet.no
[17] Fact sheet 56 – purpose and basis for processing.

- Processing is necessary for compliance with a legal obligation (in accordance with applicable legislation).
- Processing is necessary in order to protect the vital interests of the data subject or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercising of official authority vested in the controller.
- Processing is necessary for the purposes of legitimate interests which override the interests of the data subject as regards privacy.

The following questions are relevant in any assessment of the basis for processing:

- What is the purpose of the processing?
- Is the processing regulated by a law or regulation?
- What processing will be carried out?
- Is the processing necessary to provide appropriate healthcare and care services?

The duty to keep records gives the organisation a legal obligation to process personal health data. Most processing of personal data in the healthcare and care services sector is therefore statutory. In addition to documentation requirements, the legislation also contains a number of other rules regarding processing, e.g. disclosure of data

Other processing of personal data by the enterprise may be based on other grounds for processing. Examples of such grounds for processing are an agreement with the data subject in connection with the follow-up of employees and if the enterprise performs tasks which do not constitute healthcare, both consent and an agreement may constitute a basis for processing.

If several grounds for processing may apply, the enterprise shall identify one basis per purpose.

It is the controller that must assess the basis for processing.

The basis for processing shall be documented. This can be done in the record[18].

4.2 Duties and requirements in connection with the processing of personal health data

Data subjects have many rights regarding the processing of personal health data. The organisation shall facilitate technical and organisational measures to ensure that data subjects are able to assert their rights.

This chapter covers duties and requirements under both data protection legislation and health legislation. The chapter heading indicates where text only applies to data filing systems for therapeutic purposes.

[18] See section 3.3 and Fact sheet 13 on records for guidance and a template for records for controllers and processors.

4.2.1 The duty of confidentiality

The organisation shall ensure that all personnel who are granted access to personal health data and other confidential information are familiar with their duty of confidentiality.

The enterprise shall ensure that personnel fulfil their duty of confidentiality. This should at least be ensured through:

- access control, logging and subsequent controls,
- securing of information systems,
- procedures, training and information, and
- design of physical premises.

Breaches of confidentiality constitute a non-conformity and are linked to both administrative and criminal sanctions.

4.2.2 Information for data subjects

The enterprise shall be obliged to provide information to data subjects in a concise, transparent, understandable and readily accessible manner[19] and in clear and simple language.

The information shall be provided in writing or otherwise, including electronically if appropriate. At the request of the data subject, information may be provided verbally, provided the data subject identifies themselves.

When collecting information, the controller shall inform the data subject, in an understandable manner, of their rights and how the personal data is processed.

4.2.3 Access

The term ‘access’ is used in a number of contexts. Right of access may apply under health legislation, under data protection legislation and under the Freedom of Information Act. The Code makes no reference to access under the Freedom of Information Act.

The organisation shall ensure that the data subject is able to gain access to data that has been recorded about them. This access also applies to logs of the names and organisations of persons who have obtained information, and what information they obtained and when.

The organisation shall ensure that the data subject is able to find out what personal data about him- or herself the organisation processes. This also includes finding out the names of persons from other organisations who have obtained the information.

The organisation shall ensure that the person who invokes his or her rights is identified.

[19] The requirements regarding universal design must also be taken into account in this regard.

4.2.3.1 Access to personal health data filing systems for therapeutic purposes

Patients are normally entitled to gain access to all data relating to themselves that is contained in personal health data filing systems for therapeutic purposes. This also applies to audio recordings, X-rays, video recordings etc.

Upon request, health personnel shall provide an explanation of specialist terms etc. Provision shall be made to enable Sami-speaking, foreign language-speaking and disabled persons to exercise their right of access. Such measures shall be documented.

The general rule is that all patients over the age of 16 have an independent right of access. Children aged between 12 and 16 have a limited independent right of access, as they have the right to be consulted and may limit or deny access by parents or others with parental responsibility for them. Children under 12 years of age have no right of access, but parents or others with parental responsibility for a child have a right of access on behalf of their child.

Patients may be denied access to information in all or parts of a personal data filing system for therapeutic purposes if it is absolutely necessary in order to prevent risk to life or severe injury for the patient themselves, or access is obviously inadvisable out of consideration for persons who are close to the person concerned. Compelling reasons must apply in order for access to be denied, and there must be a real danger of consequences of a certain magnitude.

The controller shall provide access within 30 days at no cost to the patient.

4.2.4 Correction and erasure

Data subjects have the right to have inaccurate or incomplete information corrected without undue delay.

The archive legislation contains provisions concerning storage and archiving. The Code makes no reference to this topic here.

4.2.4.1 Correction and erasure of data in personal health data filing systems for therapeutic purposes

Correction shall take place through re-entry or through the addition of a dated correction. Corrections shall not be made through the erasing of information.

If information is inaccurate or misleading and is burdensome for the person concerned as a result, or is obviously not necessary in order to provide healthcare, a patient may request that the information be erased.

As a general rule, correction and erasure shall be carried out by the person who signed the information. If such correction or erasure would be difficult for the health personnel who signed the information to do, correction or erasure may be done by health personnel designated by the controller.

Any information that is recorded under the wrong person shall be erased unless there are compelling reasons[20] in the public interest why erasure should not be carried out.

[20] See more in the Directorate of Health's circular on the Health Personnel Act.

The controller shall notify any person who has received corrected or erased personal data of all correction or erasure of the personal data concerned. The controller shall notify the data subject of the abovementioned recipient if the data subject so requests.

If a request for correction or erasure is denied, the patient shall be notified of their right of appeal.

The controller shall give an electronic reply if personal data is processed electronically.

4.2.5 Release and disclosure of data in personal health data filing systems for therapeutic purposes

4.2.5.1 The right to object to release and disclosure of data

The patient or healthcare user has the right to object to the disclosure or release of data. This may apply to the transfer or release of data to the patient themselves, to guardians and/or to health personnel. The enterprise shall have an overall responsibility for safeguarding the rights of patients.

As a general rule, data may not be transferred or released if there is reason to believe that the patient or healthcare user would object were they to be asked.

Transfer and release may still take place if there are compelling reasons for such transfer or release.

Patients and healthcare users cannot object to statutory transfer of data. This also applies to the statutory transfer of data to central registers.

The enterprise therefore has a responsibility for ensuring that patients are made aware of their right to object to the release and disclosure of data. It may be appropriate to include this data in other information to which the patient is entitled.

The names of anyone to which data has been disclosed and the enterprise they are affiliated with shall always be documented.

4.2.5.2 Release and disclosure of health data between organisations in connection with the provision of healthcare

Unless the patient or healthcare user objects, health personnel shall grant collaborating personnel access to necessary and relevant health data insofar as such access is necessary in order to provide a patient with healthcare in an appropriate manner.

Upon discharge from a health institution, the patient should be given the opportunity to state who their medical records should be sent to.

4.2.5.3 To the organisation’s management and to administrative systems

When it is necessary in order to provide healthcare or for internal control purposes or the quality control of services, any party that provides healthcare may disclose the data to the organisation’s management. The information shall be necessary and relevant for the intended purpose.

The information shall not be directly personally identifiable insofar as is possible.

Health personnel shall provide the patient's national ID number and data concerning diagnosis, any medical needs, services, admission and discharge dates and relevant administrative data to the organisation's internal patient administration systems.

4.2.5.4 For educational and quality assurance purposes

Confidential health data may not be disclosed when the purpose is education or quality assurance for health personnel who have previously provided health and social care services to the patient during a specific treatment pathway, but will not be involved in the provision of any further health and social care services. This may only take place if the patient does not object. This may for example encompass situations where ambulance personnel have transported a patient to hospital, personnel have treated a patient in an Accident & Emergency department at a hospital or an employee at a nursing home has helped to admit the patient to a hospital. By obtaining the data, the treatment provider can assess whether the investigations, assessments and treatments that have been carried out were appropriate (see Section 29(c) of the Health Personnel Act).

The disclosure of data shall be limited to data that is necessary and relevant for the purpose. The patient's record shall state the data has that been disclosed and who it has been disclosed to.

4.2.6 Storage of health and personal health data

The general rule under the GDPR is that personal data must be stored until its purpose has been fulfilled. The data shall then be erased or anonymised.

4.2.6.1 Storage period in connection with the provision of healthcare

Health data shall be stored until there is no longer considered to be any need for it given the nature of the healthcare concerned. The same applies to data concerning who has gained access to or received health data which is linked to the name or national ID number of the patient or healthcare user concerned (logs).

The data shall then be erased if it is not to be retained under the Archive Act, the Health Archive Act or any other legislation.

4.2.6.2 Destruction of documents in personal health data filing system for therapeutic purposes etc. after digitalisation

When paper documents are digitalised in an appropriate manner, physical original documents may be destroyed. 'Appropriately digitalised' means that all text is legible and that all text, pages, images and figures have been scanned. Electronic personal health data filing systems for therapeutic purposes shall reflect the original.

4.2.6.3 personal health data filing system for therapeutic purposes upon termination and transfer of activity etc.

In the event of the transfer or cessation of activity, personal health data filing systems for therapeutic purposes may be transferred to another organisation.

The patient/healthcare user may object to the transfer of their medical records and instead request that the entry be transferred to another specified organisation.

Data which is not to be transferred to specific health personnel or a specific organisation, and which the organisation is not to safeguard, may be delivered to an official archive, placed with another storage institution or delivered to the county governor. Data which is delivered to the county governor is retained for ten years, and may then be destroyed after consultation with the Director General or the National Archives of Norway or delivered to an official archive.

4.3 Built-in data protection

Built-in data requirement is a key requirement of the GDPR. The organisation, both the controller and their suppliers, shall require and address data protection in all development phases of a system or solution. The organisation shall ensure that the information systems fulfil the principles of data protection (see section 2.2) and safeguard the rights of data subjects.

The controller shall select suppliers which are able to provide services that fulfil statutory requirements and the requirements of the Code. Suppliers shall assist any controller which uses their products and services in fulfilling these requirements. If necessary, the parties shall enter into a dialogue to determine the appropriate measures in order to fulfil the requirements.

5 Information security

This chapter describes key security measures. All security measures shall be chosen on the basis of risk assessments. The enterprise shall assess whether it is necessary to implement more comprehensive measures than those described in this chapter.

Most security requirements in Chapter 5 also apply to the processing of personal health data for purposes other than the provision of healthcare and care services. The enterprise shall consider what measures are necessary (for example within access control and logging).

5.1 Employees, expertise and attitude-forming campaigns

5.1.1 Terms and conditions

All employees in the enterprise shall undergo continuous training regarding the requirement to fulfil the duty of confidentiality, information security and data protection. This should be included in the employment contract or otherwise agreed in writing.

The organisation shall establish a confidentiality agreement for each employee.

The enterprise should prepare a set of instructions regarding information security and data protection which covers the material requirements.

The enterprise shall have guidelines in place concerning personal use of information systems and devices.

5.1.2 Training and expertise

The enterprise shall establish measures which ensure that everyone who is given access to information systems and related information possesses sufficient expertise to use the systems and to safeguard information security and data protection regarding data subjects.

Training shall take place continually and be adapted to the various roles and user groups concerned. Follow-up should be carried out to ensure that the training measures are having the desired effect. Completed training and assessments of effects should be documented. New training initiatives shall be considered in the event of technological changes or change in procedures.

The organisation should have an up-to-date overview of employee competence and training needs.

5.1.3 Termination of employment

In the event of termination of employment, all media (including digital, paper etc.) which may contain health and/or personal data shall be returned. Access passes shall be returned and deactivated.

All access shall be blocked.

The organisation shall have procedures in place for tidying up information which the employee may have stored in their own user account.

The organisation should implement measures to make the employee aware that the duty of confidentiality will continue to apply after their employment has ceased.

5.2 Access control

Access control is about how the enterprise implements:

- authorisation for access to information systems
- authorisation for access to personal health data filing systems for therapeutic registers, which entails the granting of permission to read, record, edit (before signing), correct (after signing), erase and/or block personal health data
- authentication which protects the identification of authorised users.
- disclosure of personal health data concerning specific patients/healthcare users for authorised personnel.
- disclosure of personal health data to personnel other than the enterprise's own personnel.
- Review measures.

The enterprise shall have procedures for the authorisation, alteration and termination of access.

Within the framework of the duty of confidentiality, the enterprise shall ensure that relevant and necessary health data is available to health personnel and collaborating personnel as and when necessary in order to provide, administer or quality-assure the provision of healthcare to individuals.

The enterprise shall determine the manner in which the data is to be made available. The data shall be made available in a manner which addresses information security and data protection.

Access control shall be established for all information systems. This also applies to administrator and system users.

Only authorised personnel with official need may gain access to personal health data.

Access to personal health data filing systems for therapeutic purposes shall be granted following a specific decision based on the completed or planned establishment of measures for the medical treatment of the patient. Access shall be controlled to ensure compliance with

the confidentiality rules and so that no access to personal health data is given to anyone other than those with an official need to gain such access.

5.2.1 Authorisation

The enterprise shall be responsible for ensuring that authorisations are allocated, administered and monitored.

In connection with the allocation of authorisation, the statutory duty of confidentiality shall be assessed and safeguarded.

The controller may delegate authority in order to allocate authorisation to the individual unit's manager. This will require the managers to assess and approve the authorisation within their own area of responsibility. Allocated authorisation shall ensure that employees are able to gain access to necessary and relevant personal health data in accordance with their responsibilities and duties, insofar as the statutory duty of confidentiality does not preclude such access. Authorisation shall be reviewed in the event of any changes in responsibilities, employment or long-term absence.

If access control is based on roles, authorisation should be granted for each role, regardless of the employee's other roles.

Authorisation for access to personal health data filing systems for therapeutic purposes shall

- be time-limited and
- specify the enterprise that the authorisation covers.

In the case of the authorisation of technical personnel with a specific need to access large quantities of personal health data, measures shall be established to enable any misuse to be detected.

The following measures shall be established to prevent unauthorised access:

- If provision is made for self-authorisation, access shall be justified and registered.
- Technical measures shall ensure that persons inside or outside the enterprise are unable to alter data without the name of the person who made the change and what has been changed being logged in the information systems.
- All allocations of authorisation shall be registered in an authorisation log (see 5.2.1.1).
- Technical measures shall also ensure that persons outside the enterprise are unable to alter configurations and software without the changes being logged (see 5.4.5).
- Users with administrator access shall use a separate personal user account for administrator tasks. Operations personnel shall have personal user accounts for tasks that do not require administrator access.
- A risk assessment shall justify the need for different administrator users.

5.2.1.1 Authorisation log

The enterprise shall ensure that an authorisation log is established. The log shall at least contain the following:

- information on who has been allocated authorisation

- information on the role to which the authorisation has been allocated (if roles are used by the organisation)
- purpose of the authorisation
- time at which the authorisation was given and revoked (where applicable)
- information on the organisation to which the authorised person is linked
- authorisation of health personnel regarding access to health data in other organisations (only if access to health data in other organisations is in use)

5.2.1.2 Access to personal health data between enterprises

The enterprise shall maintain control and an overview of all processing of personal health data for which it is responsible, including the disclosure of information to other enterprises:

- A risk assessment shall be conducted in the event of the new provision or changes to the existing provision of information to other enterprises.
- Controllers and enterprises that are given access to data held by the controller shall clarify, through an agreement or otherwise, how:
    - authentication will take place securely
    - authorisation for health data held by the controller will be granted
    - logging and follow-up of logs will take place

5.2.2 Authentication

Authentication shall safeguard at least the following:

- Authorised persons shall verify their identity in a secure manner. The secure manner must be determined on the basis of a risk assessment.
- Different employment relationships shall be identified.
- No more than one person shall use the same authentication criteria.
- The allocation of authentication criteria (e.g. user name and password) shall be carried out in an appropriate manner.
- Access from home offices and/or mobile devices (and mobile networks) shall be secured through a secure authentication solution. This also applies to locations that communicate via lines over which the enterprise has no physical control.
- All default passwords (factory settings) on systems and equipment shall be changed before the processing of personal health data is commenced.
- When using wireless networks for processing personal health data, the authorised user shall be authenticated using a secure authentication solution.

If roles are used, different roles shall be identified and, where necessary, new authentication shall be given.

5.2.3 Access control audits

The enterprise’s management shall ensure that regular checks are carried out to determine who has gained electronic access.

Access control, including allocated authorisations, shall be reviewed and monitored by the individual manager:

- In the event of organisational changes, the transfer of personnel to another unit/department or change in area of work.
- At least once a year (ideally in connection with security audits).
- in the event of a security breach for what has been affected by the breach

The enterprise's management shall be informed if checks result in a suspicion that unauthorised access has taken place. The incident shall otherwise be dealt with in accordance with established procedures for non-conformity management, particularly with the aim of clarifying whether existing access controls are satisfactory.

The misuse of self-authorisation shall be followed up as a non-conformity.

If such an audit reveals that unauthorised access has taken place, the incident shall be treated as a non-conformity.

In the event of access being gained to health data across organisations, the contractual parties shall collaborate regarding access control. Any controller who has access to authorise health personnel for access shall continually monitor:

- Who within the enterprise has electronically retrieved health data from another enterprise,
- why this has been done, and
- the time period during which health data was retrieved.

If the checks indicate that an unauthorised person has retrieved health data, the enterprise from which the data was obtained and the patient/healthcare user that the data concerns shall be notified. The non-conformity shall be dealt with in accordance with established procedures for non-conformity management.

5.3 Physical security and the handling of equipment

5.3.1 Keys/access cards

A procedure shall be established for the administration of keys/access cards in the access control system.

5.3.2 ICT equipment

Security measures shall prevent unauthorised access to personal health data. This can be solved through access control to premises using equipment and by protecting the equipment against misuse or unauthorised access.

5.3.3 Infrastructure

Security measures shall ensure that only authorised personnel are able to gain access to such infrastructure.
All storage media shall be erased appropriately as and when they are taken out of use. The duty to archive data shall be fulfilled under all circumstances.

5.3.4 Mobile devices and home offices

A risk assessment shall be carried out before solutions are put into use and in the event of changes which could impact on information security. Administrative procedures shall be established regarding the use of mobile devices and home offices.

Personal health data shall only be stored locally on equipment where such storage is necessary on the basis of official need and shall always be stored encrypted.

5.3.5 Encryption

Technical measures shall be established so that all communication of personal health data outside the control of the enterprise is encrypted end-to-end. Encryption and decryption between communication points in the infrastructure shall be performed by approved equipment over which the enterprise has control. This control may be addressed by agreement.

All communication, whether wireless or wired, shall be secured through encryption.[21]

Encryption of stored personal health data may be considered a security measure.

In data filing systems which are established under Sections 10 and 11 of the Personal Health Data Filing System Act, directly personally identifiable characteristics shall be stored encrypted.

5.3.6 Medical equipment

Medical equipment which processes personal health data shall be covered by the enterprise's efforts relating to information security and data protection, e.g. in risk assessments, access control, change control and procedures regarding use, in the same way as other information systems.

[21] See for example document "NSM Cryptographic recommendations Version 1.0" https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/nsm-cryptographic-recommendations/

5.4 Secure IT operation

5.4.1 Configuration control

It is a prerequisite that the enterprise has an overview of data flow, data communication and integrations and control over all its own equipment and software used in the processing of personal health data. This also applies to equipment at regional offices and home offices and mobile devices.

The following shall be observed:

- The configuration shall ensure that the equipment and software only perform the functions that are specific to the intended purpose.
- The enterprise shall ensure that all data flow, data communication and integrations are mapped and documented.
- Only approved equipment and software shall be used for the processing of personal health data. The enterprise shall determine who has approval authority.
- Hardware and software shall be updated so that the latest and most modern security functionality is provided and necessary security measures are implemented. Updates should be verified and tested prior to implementation. Verification and testing shall be documented as part of the enterprise's change management procedures (see Chapter 5.4.2).
- Scheduled changes shall follow the organisation's procedure for configuration changes.
- Separate environments shall be used for development, testing and production, so that personal health data used in the provision of healthcare is not affected by any errors which occur during development and testing.
- The configuration of equipment and software shall be checked regularly to ensure that such equipment and software only performs the intended functions.
- The configuration shall be protected against malware.
- The configuration shall be protected against accidental actions.

Configuration changes, i.e. changes to equipment or software, shall not be commissioned until the following measures have been implemented:

- Risk assessment showing that the risk is acceptable.
- Test which ensures that the expected functions are provided
- Implementation which provides protection against unforeseen events
- New configuration is documented
- Configuration changes have been approved by the organisation's manager or the person designated by the management

Configuration checks shall be regulated through an agreement concerning:

- Use by the processor.
- Use of remote access for maintenance and updates. Remote access shall only be possible via channels over which the enterprise has control.

5.4.2 Change management

All changes of significance to information security within the organisation, information systems and infrastructure shall be anchored at the relevant managerial level.

The enterprise shall prepare procedures for change management, which shall encompass the following topics:

- identification of material changes
- planning and testing of changes
- assessment of potential consequences, for example by conducting a risk assessment and, where appropriate, a data protection impact assessment
- approval procedures for changes
- communication of plans to relevant persons/roles
- back-up procedures if the change has to be cancelled or fails or incidents occur
- change log with relevant information
- training of relevant users/roles

5.4.3 Back-up

The enterprise's management shall ensure that back-up copies are made of personal health data as well as other information that is necessary for the restoration of normal operations.

Back-up copies shall be stored in a locked and fire-proof facility and kept separate from operating equipment.

Regular tests shall be carried out to ensure that back-up copies are correct and can be restored.

At least one back-up copy shall be protected against malware and incidents.

5.4.4 Logging

In order to detect actual or attempted breaches, at least the following shall be logged:

- Authorised use of information systems.
- All system and administrator use for information systems and infrastructure.
- Configuration and software changes.
- Security-relevant incidents in security barriers.
- Attempted unauthorised use of information systems and infrastructure.
- Use of self-authorisation.

At least the following shall be recorded in the logs in the event of the authorised use of personal health data filing systems for therapeutic purposes:

- The identity of the individual who has read, corrected, registered, modified or deleted personal health data.
- organisational affiliation,
- the basis for disclosure, and
- the time period of disclosure.

In the case of the processing of personal health data for purposes other than the provision of healthcare and care services, the requirements for logging shall be determined on the basis of a risk assessment.

Consideration should be given to logging the following in addition to the minimum requirements:

- the role of the authorised user at the time of access,
- organisational affiliation,
- the type of data to which access has been gained, and
- the name of the individual who has received health data that is linked to the name or national ID number of the patient or healthcare user.

It shall be possible to analyse logs using analysis tools with the aim of detecting breaches.

Procedures shall be established to analyse the logs to ensure that incidents are detected before they have serious consequences. In the event that a breach is detected, the incident shall be managed as a non-conformity.

Procedures shall be established to ensure that logs can be compared with the authorisation log as and when necessary.

The logs and authorisation log shall be protected against alteration and erasure.

Logs shall have a correct timestamp.

Logs generated in connection with the provision of healthcare shall be stored until it is considered that there is no longer any use for them.

Logs which are of significance as regards security should be stored for as long as is necessary in order to achieve its purpose.

5.4.5 Management and handling of technical vulnerabilities

The management and handling of technical vulnerabilities shall follow the relevant procedures for change management. The organisation shall have a procedure for obtaining information concerning technical vulnerabilities in equipment and software.

Management and handling shall be based on an overview of:

- ICT equipment
- software: software, supplier, version numbers, which version is installed and where, and who is responsible for the software

Procedures and operational measures shall be established which address:

- responsibility for monitoring, risk assessment, correction and coordination
- how the organisation should respond to and report vulnerabilities
- prioritisation and establishment of time line for correction
- all corrections should be tested before they are implemented

5.4.6 Security audits

The enterprise's management shall follow up to ensure that security is being safeguarded through regular and at least annual security audits. The purpose of security audits is to carry out control activities and the quality assurance of established measures and adopted procedures. An approved plan for security audits shall be established.

In order to carry out adequate security audits in organisations, the assessments should at least include:

- Delegation of responsibility and organisation of the security work
- Compliance with procedures concerning the use of information systems and the processing of personal health data
- An assessment of the effectiveness of the security measures
- Access to personal health data and measures to prevent unauthorised access
- Training and expertise regarding data protection and information security
- Review of documentation for the safeguarding of information security amongst communications partners, processors and suppliers

Results, conclusions and non-conformities derived from security audits shall be documented and dealt with by the enterprise.

5.5 Communication security

5.5.1 Management of network security

Network security is a key measure to safeguard the processing of personal health data.

Organisations shall clearly define the requirements that apply to network security, and the measures that are established shall be based on a risk assessment.

5.5.2 Connection to external networks

When connecting to external networks, technical measures shall be established to ensure that only explicitly specified permitted traffic is able to pass from the outside in and vice versa and that all other traffic is stopped.

The measures shall include at least two independent technical measures to ensure that persons outside the organisation are unable to gain unauthorised access to and/or alter or erase personal health data

5.5.3 Electronic interaction

The reference directory[22] pursuant to the regulation on ICT standards and national eHealth solutions [23]provides an overview of obligatory and recommended standards for healthcare and care services. This regulation is intended to help organisations within the healthcare and care service that provide healthcare to use ICT standards to promote secure online interaction.

A description is presented below of the requirements regarding interaction that are otherwise set out in the other chapters of the Code.

5.5.3.1 Requirements regarding electronic interaction

Clear lines of responsibility shall be established between senders, recipients and any communication mediator, and the delegation of responsibilities shall be set out in agreements between the organisations and the communication mediator. All agreements shall be established in writing.

The sender/tendering enterprise shall be responsible for:

- its own connection security which prevents unauthorised access and penetration,
- ensuring that the service cannot disseminate software which contains malware or similar and
- securing transmission encryption end-to-end.

The recipient/user enterprise shall be responsible for:

- ensuring that the service cannot be used to distribute harmful code etc.,
- its own connection security which prevents unauthorised access and penetration, and
- ensuring secure transmission encryption end-to-end.

5.5.3.2 Requirements regarding message communication based on the ebXML framework

The sender is responsible for:

- correct addressing of electronic interaction messages in accordance with the address register[24]
- ensuring that, as and when necessary, the message is signed in such a way that the enterprise cannot deny having sent it,
- non-conformity reporting in connection with erroneous sending and
- ensuring that messages are delivered in the agreed format.

The recipient shall be responsible for:

- logging receipt as and when necessary, so that the recipient cannot deny having received the message,

---

[22] Reference directory for eHealth: https://ehelse.no/referansekatalog/referansekatalogen-for-e-helse
[23] See https://lovdata.no/dokument/SF/forskrift/2015-07-01-853?q=Forskrift%20om%20IKT-standarder%20i%20helse-
[24] Norsk helsenett's address register: https://www.nhn.no/

- non-conformity reporting in connection with errors, i.e. receipt of a message which is not addressed to the enterprise, and
- ensuring that messages are received in the agreed format.

The communication mediator shall be responsible for:

- ensuring that messages are only delivered to the addressee,
- ensuring that messages cannot be altered or destroyed during transport from the sender to the recipient,
- ensuring that messages cannot be read by anyone other than the sender and recipient,
- ensuring that messages are delivered by the agreed deadlines following dispatch, and
- non-conformity reporting in connection with all the above points.

5.5.3.3 Real-time data sharing

Interaction through data sharing enables more dynamic information sharing for citizens and stakeholders in the healthcare sector. Such data sharing may involve a stakeholder requesting or updating information from another stakeholder via a data sharing interface.

The following security principles shall apply to data sharing:

- There must be secure user authentication that is trusted by enterprises that offer data sharing interfaces.
- Any enterprise that requests access shall verify that the user has the necessary authorisations for the data sharing interface in question.
- A distinction shall be made between read and write rights for different information elements based on the individual user authorisation.
- Unnecessary intermediate storage shall be avoided.
- It shall be possible to verify the legitimacy of the data sharing interface and the enterprise that is offering it.
- Common components for consumer authentication shall be used where available and appropriate

5.5.4 E-mail and SMS

The enterprise shall establish measures to prevent personal health data and other information of importance to information security from being disclosed through the use of unencrypted e-mail and SMS or other insecure channels.

Any enterprise that uses unencrypted channels shall:

- ensure, through technical and organisational measures, that e-mails do not contain identifiable personal health data
- establish logging to verify that rules are not broken. Violations shall be treated as non-conformities.
- assess whether the collective information in an SMS or e-mail could result in a breach of the duty of confidentiality

5.5.5 Connection to the internet

Technical equipment, such as medical equipment and applications that connect to the internet shall be covered by the enterprise's efforts relating to information security and data protection, including in risk assessments, access control and procedures regarding use.

The enterprise shall establish:

- technical measures which help to prevent accidental disclosure and unauthorised access to personal health data
- logging to verify that rules are not broken. Violations shall be treated as non-conformities.

5.6 Digital communication to data subjects

In this chapter, ‘digital communication’ refers to messages that are sent by the organisation to data subjects in connection with healthcare provision.

The organisation shall:

- assess and determine the basis for processing
- consider a suitable solution and communication channel for the intended purpose
- ensure that personal health data is made available in such a way that the patient/healthcare user is not dependent on storing the data on their own equipment in order to familiarise themselves with the data
- ensure that procedures are established to ensure that messages to patients are not intrusive and do not violate privacy, while at the same time providing the patient with sufficient information
- implement sufficient measures to ensure that messages are sent to the correct recipient. To ensure that the correct contact details are used for recipients, enterprises with access to the contact register should use the register.

5.7 Suppliers and agreements

The supplier shall ensure that controllers who use the supplier's products and services are able to fulfil statutory requirements and the requirements of the Code.

5.7.1 Requirements regarding suppliers’ duty of confidentiality

A supplier may handle personal health data either through processing the data on behalf of the controller, through outsourcing or through the provision of maintenance services, for example, which means that the supplier’s employees may be exposed to confidential information. The supplier shall ensure that it has procedures in place which impose on a duty of confidentiality on all employees concerning personal health data and other confidential information.

The supplier may itself administer and store confidentiality declarations for its own personnel, but the controller shall be given access as and when necessary.

5.7.2 General considerations regarding agreements and supplier monitoring

The controller shall be responsible for ensuring that requirements regarding information security and data protection are followed throughout the supply chain. In connection with the provision of services or the delivery of hardware or systems, the security requirements that are to be fulfilled in order for the controller to fulfil his or her responsibilities shall be agreed in writing with suppliers. The requirements of the Code which apply to suppliers by agreement will depend on the type of delivery concerned, for example:

- data processing, in the form of cloud services or operating services
- maintenance, for example in connection with physical service or remote access
- delivery of solutions and systems

The agreements shall include commitments which require the parties to comply with relevant requirements and measures which follow from the version of the Code of conduct for information security in the healthcare and care sector that is in force at any one time, as well as the regulation of sanctions in the event of breaches of this Code, relevant legislation and the agreement in general.

Through relevant agreements, the organisation shall ensure that the supplier has satisfactory management systems in place with regard to security audits and non-conformity management.

5.7.3 Outsourcing of services

In the event of the contracting out of services (outsourcing) covering ICT functions or other functions of significance to information security or data protection, the agreement shall at least cover the following points relating to information security and data protection:

- Documented risk assessment showing that the acceptance criteria of the outsourcing enterprise and the level of security set out in the Code have been established. When outsourcing ICT services to other countries, the circumstances in the host country should be assessed because they may impact on the risk assessment.
- The tasks that are of significance to security which are covered, and the responsibility for such tasks.
- Description of the supplier's solution and interface with respect to the organisation in the form of a configuration map.

The agreement shall ensure that the enterprise is also granted the right to audit the supplier's activities relating to the agreement. Audits may be conducted by an agreed third party.

The enterprise shall establish an appropriate plan to safeguard information security and data protection upon conclusion of the service delivery. Upon termination of the contract, a signed declaration shall be provided by the supplier confirming that all data belonging to the enterprise has been returned or erased by the agreed time.

5.7.4 Processor

Processors shall only process personal health data and other confidential information in accordance with instructions issued by the controller. The manner in which the processor may process data on behalf of the controller shall be regulated in an agreement.

The controller may only use processors who provide adequate guarantees that it will implement appropriate technical and organisational measures which ensure that the processing fulfils the requirements of the Personal Data Act. “Adequate guarantees” means that the processor fulfils the requirements set out in applicable laws and regulations, as well as the requirements of the Code that are relevant to the contractual relationship concerned.

5.7.4.1 The processor’s subcontractors

The processor shall not engage subcontractors without the prior specific or general permission of the controller. If general, written permission is obtained, the processor shall notify the controller of any plans to substitute subcontractors. The controller shall be entitled to object to such changes.

The processor shall be responsible for ensuring that its subcontractors fulfil their obligations.

Subcontractors have an independent responsibility regarding information security and for addressing data protection concerning data subjects. The agreement with the supplier shall stipulate that subcontractors are subject to the same obligations as the processor under the data processing agreement. This shall be regulated in an agreement between the processor and the subcontractor. The agreement shall be made available to the controller upon request.

5.7.4.2 Scope of data processing agreements

Processor agreements[25] can be either an independent agreement between the parties concerned or an integral part of another contract. Processor agreements shall be established in writing.

The processor’s independent responsibility for information security and for addressing data protection concerning data subjects shall be clarified.

The agreement shall state that the processor undertakes to fulfil statutory requirements and the requirements of the Code.

5.7.4.3 Processor’s overview of processing activities

The processor shall maintain an overview[26] (record) of all categories of processing activities that are carried out on behalf of a controller.

The controller shall ensure that the processor receives the information necessary to enable the processor to obtain such an overview.

---

[25] The contents of the processor agreement are regulated in Article 28 of the Regulation. See Fact sheet 10 for more information.
[26] See Fact sheet 13 for more information.

5.7.4.4 The processor's other obligations

If the processor processes personal health data from a number of enterprises, the processor shall ensure, through technical measures which cannot be overridden by the controller's users, that barriers are established between the enterprises in accordance with the completed risk assessment.

The processor shall notify the controller without undue delay that non-conformities have occurred. The processor shall assist the controller in meeting the 72-hour deadline for submitting any notifications to the Norwegian Data Protection authority.

5.7.5 Maintenance, remote access or physical service

In addition to complying with other requirements in the Code, the enterprise shall, through agreements, ensure that:

- The supplier's equipment that is used for an online connection via a communication network or personal equipment connected to the enterprise's equipment has no malware which contains viruses etc. and that the equipment is protected against access by unauthorised parties,
- all access and physical access shall be authorised by the enterprise. Access shall be logged and controlled and
- availability of personal health data shall insofar as is possible be maintained when the supplier performs work on the enterprise's equipment/software.

5.7.6 System suppliers

Enterprises in the healthcare and care services sector which use information systems that process personal health data shall require privacy by design to be part of the solutions.

To enable enterprises to fulfil their responsibilities as a controller, information systems shall have functionality that fulfils applicable statutory requirements and the relevant requirements of the Code.[27]

5.7.7 Supplier monitoring

Information security and data security linked to procurement and supplier monitoring shall form part of the organisation's information security management system. All phases of supplier management, from procurement to conclusion of the agreement, shall be covered.

The enterprise shall ensure:

- clarity regarding responsibilities and roles,
- ensuring that specialist resources within information security and data protection participate in procurements and supplier management, and

[27] See the appendix "Overview of the Code's requirements"

- ensuring that the enterprise's management (and the board if relevant) are normally involved in decisions concerning the use of private suppliers and/or the outsourcing of services with a certain scope.

The establishment of requirements and necessary security measures in connection with the use of suppliers shall be based on a comprehensive risk assessment. The risk assessment shall always encompass scenarios that include the supplier's authorised and, where applicable, unauthorised access to personal health data and other confidential information.

The organisation shall ensure that relevant security requirements are included in all procurements. The organisation shall ensure that it has sufficient client expertise at its disposal.

5.7.8 Transfer of data to other countries

Organisations which transfer personal data to other countries shall ensure that the level of protection stipulated in the Personal Data Act is not undermined in connection with the transfer.

All EU/EEA countries have transposed the General Data Protection Regulation and thereby ensured that personal data are processed responsibly. The European Commission has also recognised that some third countries[28] provide an adequate level of protection for personal data. Personal data may therefore be freely transferred to these states. This assumes that the other conditions of the Personal Data Act are met. See section 5.7.5, particularly the requirements regarding risk assessments and country risk assessments.

Special requirements may apply if suppliers or services established outside the EU/EEA are to be used. These requirements are intended to ensure that the information is subject to the same level of protection as in the EU/EEA. When the enterprise transfers personal data to states outside the EU/EEA, known as "third countries", it shall use one of the grounds for transfer stipulated in the Regulation.[29]

When transferring data to countries outside the EU/EEA, the organisation shall ensure that it has sufficient expertise (e.g. legal expertise) at its disposal in order to implement this in accordance with applicable requirements.

5.7.9 Cloud services

The use of cloud services in the processing of personal health data requires the controller to carry out comprehensive risk assessments, and otherwise follow the requirements for agreements and supplier monitoring stipulated in the Code.

Some particularly important considerations are that:

[28] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[29] The Norwegian Data Protection Authority's guidance concerning the transfer of data to other countries, www.datatilsynet.no

- the distribution of responsibility between the controller and the processor has been clarified, and adapted to the delivery model being used
- the controller has an overview of where data is processed geographically, so that the requirements of section 5.7.8 can be addressed
- the controller shall ensure that any standard agreements that the cloud provider may have are not in breach of applicable statutory requirements and the requirements of the Code
- the controller shall have an appropriate plan in place to safeguard information security and data protection upon conclusion of the cloud service

5.8 Handling of information security breaches

5.8.1 Non-conformity management

Incidents (such as breaches of procedures, data protection or information security) shall be treated as a non-conformity. Non-conformities shall be processed in order to restore the normal state, remove the cause of the non-conformity and prevent repetition.

The enterprise shall have procedures in place for detecting and managing non-conformities. The processing of non-conformities shall be documented.

The enterprise shall collect factual information concerning the sequence of events to enable corrective measures to be established. The effects of corrective measures shall be assessed and any other measures implemented as and when necessary.

In the event of serious or repeated non-conformities, a new risk assessment shall be carried out.

Non-conformity reports containing personal data or information of importance to information security shall be secured.

The Code addresses the reporting of non-conformities relating to data protection and information security to the Norwegian Data Protection Authority and the Norwegian Board of Health Supervision. Some non-conformities shall be reported to other supervisory authorities and agencies.

5.8.2 Breaches of personal data security

Breaches of personal data security are non-conformities which result in unintended or unlawful destruction, loss, alteration, unlawful distribution of or access to personal data that is transferred, stored or otherwise being processed.

5.8.2.1 Notification to the Norwegian Data Protection Authority

In the event that a non-conformity constitutes a breach of personal data security, the non-conformity shall be reported to the Norwegian Data Protection Authority within 72 hours, unless the breach would not have resulted in a risk to the rights of natural persons.

For detailed rules, exceptions to the reporting obligation and the reporting method, see https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

5.8.2.2 Notification of data subjects

If the non-conformity is likely to entail or will entail a high risk for the data subject, the organisation shall notify the person concerned.

The enterprise shall provide the data subject with at least the following information:

- Description of the breach.
- Name and contact details for the Data Protection Officer or other point of contact where more information may be obtained.
- Description of the likely consequences of the breach.
- Description of the measures that the enterprise has implemented or is proposing to implement in order to manage the breach, including (where relevant) measures to reduce any harmful effects of the breach

Wherever possible, the enterprise shall contact the data subject directly.

5.8.3 Notification of the Norwegian Board of Health Supervision

Organisations that provide healthcare and care services shall notify the Norwegian Board of Health Supervision of any non-conformities arising from errors and non-conformities in information systems. The duty of notification shall be triggered:

- in the event of death or very serious injury to a patient or healthcare user,
- as a result of the provision of healthcare and care services and
- when the outcome is unexpected based on foreseeable risks.

In the event of such incidents, the enterprise shall:

- follow up and inform patients and relatives,
- review the incident and
- identify and follow up with risk mitigation measures.

For detailed rules and reporting methods, see https://www.helsetilsynet.no/tilsyn/varsel-om-alvorlige-hendelser/oversikt/

5.9 Emergency procedures

The non-availability of information systems could harm the enterprise, the enterprise's authorised users, the patient/healthcare user in connection with the provision of healthcare and the data subject.

The enterprise shall ensure that the necessary personal health data is available.

In order to establish emergency procedures to safeguard availability in the event of non-availability, the enterprise shall map the consequences of non-availability. This shall be assessed for both the enterprise and its authorised users.

Systems shall be classified according to the following prioritisation:

1. Systems where the non-availability of a service could be critical, e.g.
   - life-threatening for a patient
   - critical for the organisation's operation
2. Systems where the non-availability of a service could have severe consequences, such as:
   - increased risk of treating patients incorrectly
   - deferment of medical investigations and treatment which could impact on life or health
   - considerable additional work for personnel
   - lost revenue for the organisation
3. Systems where the non-availability of a service could have moderate consequences, such as:
   - delays to medical investigations and treatment without any serious health consequences
   - some additional work for personnel
   - lost revenue for the organisation
   - decreased reputation
   - reduced confidence
   - loss of efficiency
4. Systems where protracted non-availability could be accepted
5. Low priority systems

A review shall also be carried out to determine the other systems and infrastructure that the classified systems are dependent on. These shall have the same classification and security level as the classified systems.

For each classification, the management shall determine the acceptable level of risk to availability. As a minimum requirement, the maximum down-time shall be determined.

The enterprise shall establish emergency procedures based on the classification of the information systems:

- Alternative operation without the use of the information systems.
- Alternative operation with partial support from the information systems.

The emergency procedures shall be practised, tested, revised and updated at least once a year.

6 Appendix

6.1 “Overview of the Code’s requirements”

The Appendix “Overview of the Code’s requirements” contains requirements with "shall" in the Code, to make it easy to verify whether the enterprise is following the Code.

The requirements table has been designed with security audits in mind. It can also be used in other contexts in which a systematic overview of the Code’s requirements is needed. Examples may include procurements, for a supplier to demonstrate compliance or in connection with the auditing or development of a system.

6.2 Definitions

No rights or obligations must be deduced from the definitions alone. They must be considered in the context in which they are used in the Code.

-A-

“**Access**” means, for the purposes of this Code, that personal health data concerning one or more specific patients/healthcare users is, or is made, available to authorised personnel. The decision to grant access to a personal health data filing system for therapeutic purposes shall be made after a specific evaluation based on the provision of health and social care services to the patient. Access to administrative systems in connection with the provision of services to patients/healthcare users shall be established based on official need. Access relating to quality assurance and administrative tasks shall also be determined based on official need.

“**Availability**” means, for the purposes of this Code, that personal health data that is to be processed is accessible at the time and place where the information is needed.

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

“**Acceptable risk**” means, for the purposes of this Code, the level of risk that is acceptable to the enterprise of an incident occurring which could result in a breach of the applicable requirements regarding confidentiality, integrity and availability/robustness in a specific case. The level of risk will depend on the probability of an incident occurring and the consequences of such an incident. Each enterprise shall conduct a specific assessment of how it will achieve an acceptable level of risk using acceptance criteria for risk.

“**Acceptance criteria for risk**” means, for the purposes of this Code, the management’s guidelines for when a risk is acceptable. Acceptance criteria describe how risks will be accepted and may consist of decision-making processes, who is authorised to accept risks of various scopes within given frameworks, or levels describing how large a risk is acceptable.

“**Anonymised**” means, for the purposes of this Code, personal health data from which the name, national identity number and other unique personal characteristics have been removed, in such a manner that the data can no longer be linked to an individual person (see Section 2(3) of the Personal Health Data Filing System Act).

"Appropriate level of security" means the security level achieved by implementing appropriate security measures (technical and organizational). Which measures are considered appropriate will depend on the risk, and account must be taken of the technical development, implementation costs, nature of the processing, scope, purpose of processing and the context in which the processing is carried out. The appropriate level of security must ensure confidentiality, integrity, availability and resilience of the information systems in a balanced way, where great emphasis is placed on the risk to the patient/user and the performance of proper health care.

“**Authentication**” means, for the purposes of this Code, the process that is carried out in order to verify a claimed identity.

“**Authorisation log**” means, for the purposes of this Code, a log of issued authorisations that is maintained by the controller.

-C-

“(**The**) **Code**” means this document. Other documents relating to the Code, such as fact sheets and guidelines, are not covered by the term.

“**Confidentiality**” means, for the purposes of this Code, that personal health data must be protected from disclosure to unauthorised persons.

“**Configuration**” means, for the purposes of this Code, the information system’s design, including both technical equipment and software.

“**Configuration change**” means, for the purposes of this Code, a change in the construction of the information system as a result of the installation, upgrading or removal of equipment or software.

“**Consent**” from the data subject means, for the purposes of this Code, any voluntary, specific and unequivocal expression of will where the person concerned gives their consent through a statement or clear confirmation for personal data that concerns the person to be processed.

“**Controller**” means, for the purposes of this Code, a natural or legal person, a public authority, an institution or any other body which either alone or together with others determines the purpose of the processing of personal data and the means that are to be used. If the data responsibility is not specifically stipulated in the law or in a regulation issued pursuant to the law, see Section 2(e) of the Personal Health Data Filing System Act), Section 2(e) of the Patient Records Act and Article 4 of the General Data Protection Regulation (the term ‘controller’ is used here). It should be noted that it is the organisation that is the controller as regards the processing of personal health data. The responsibility shall be fulfilled by the general management of the enterprise and the enterprise is the party that is subject to the relevant obligations.

-D-

"**Data protection impact assessment**" means, for the purposes of this Code, a systematic process which identifies and evaluates potential data protection consequences from the perspective of all stakeholders in a project, initiative, proposed system or process.

"**Data protection officer**" means, for the purposes of this Code, a formally appointed contact person for data protection and information security internally with respect to the controller (the organisation's management) and employees and external parties with respect to the Norwegian Data Protection Authority and the data subject (patients, including in studies and inhouse employees).

"**Data subject**" means, for the purposes of this Code, the person to which data may be linked. Examples of terms used to refer to data subjects are applicant, patient/healthcare user, participant in research project, relative and service recipient. Employees may be covered by the term.

"**Duty of confidentiality**" means, for the purposes of this Code, a statutory or agreed obligation to prevent others from accessing or gaining knowledge of personal health data; see Section 21 of the Health Personnel Act, Section 17 of the Personal Health Data Filing System Act, Section 15 of the Patient Records Act, Section 12-1 of the Health and Care Services Act, Section 6-1 of the Specialist Health Service Act and Section 13 to 13(e) of the Public Administration Act, in addition to other information pertinent to information security. The duty of confidentiality includes both a passive obligation to remain silent and an obligation to actively prevent unauthorised persons from gaining knowledge of confidential data.

-F-

"**Filing system/register**" means, for the purposes of this Code, any structured collection of personal data which is accessible in accordance with specific criteria, regardless of whether the collection is located centrally, decentralised or distributed on a functional or geographic basis. A database or spreadsheet is a technical solution for implementing a filing system/register.

-H-

"**Health and social care services**" means, for the purposes of this Code, actions which have preventive, diagnostic, health-preserving, rehabilitating or care purposes and which are carried out by health personnel.

"**Healthcare user**" means, for the purposes of the Code, a person who requests or receives services that are covered by the Health and Care Service Act which do not constitute health and social care services; see Section 1-3(f) of the Patient and Users' Rights Act.

“**Health data**” means, for the purposes of this Code, personal data concerning a natural person’s physical or mental health, including data regarding the provision of medical services, which provides information on health status; see Article 4 (15) of the General Data Protection Regulation.

“**Home office**” means, for the purposes of this Code, the processing of personal health data on a computer provided by the organisation, e.g. at home, a holiday home, hotel room etc. The use of computers not provided by the organisation (e.g. at an internet café or a public computer in a hotel or at an airport) is not covered by the definition of home office.

-I-

“**Information Systems**" means, for the purposes of this Code, a system for collecting, storing, processing, transferring and presenting information. Examples of information systems in the healthcare and care service are: case and documentation systems, archive systems, personal health data filing system for therapeutic purposes, e-mail, security systems, network operating systems, database systems, storage systems, backup systems, infrastructure, medical support systems, medical equipment and laboratory systems.

“**Infrastructure**" means, for the purposes of this Code, the technical solution (components and basic software) that is used for the collection, storage, processing, presentation and transmission of personal health data (e.g. desktops, laptops, mobile phones, servers, network equipment (firewalls and routers), printers, storage networks, apps etc.).

“**Integrity**” means, for the purposes of this Code, that personal health data is to be protected against accidental or unauthorised modification or deletion.

“**Internal control**” means, for the purposes of this Code, planned and systematic actions intended to ensure that the activities of the enterprise are planned, organised, executed and maintained according to the requirements specified in, or pursuant to, existing legislation.

“**Including electronically**” means, for the purposes of this Code, that data (such as documents, logs, diagrams etc.) stored on a computer is also covered by the context.

-L-

“**Log**” means, for the purposes of this Code, a logical filing system in which incidents and activities in the information system are recorded; see the next definition.

“**Logging**” means, for the purposes of this Code, the registration of incidents in an information system, partly with the aim of preventing, detecting and hindering the reoccurrence of information security breaches.

-M-

"**Municipality**" means, for the purposes of this Code, a legal entity such as a municipal or county authority.

-N-

"**Nature of the processing**" means, for the purposes of this Code, the organisation's specific types of processing activities.

"**Norsk Helsenett**" means, for the purposes of this Code, Norsk Helsenett SF.

"**Non-conformity"** means, for the purposes of this Code, any processing of personal health data which is not in accordance with applicable regulations, guidelines or procedures, as well as other security breaches. Any breach of security which results in unintended or unlawful destruction, loss, alteration, unlawful distribution of or access to personal data that is transferred, stored or otherwise processed.

-O-

"**Official need**" means, for the purposes of this Code, that individuals with specific duties require necessary personal health data in order to provide medical or care services or administrate such assistance. If the patient has blocked access to all or part of their personal health data, specific legal authority will be required in order to gain access to the data.

"**Organisational measures**" means, for the purposes of this Code, non-technical measures. Examples of such measures include procedures, training and changes to the organisation and functions in order to perform tasks.

"**Organisation**" means, for the purposes of this Code, a legal entity such as a health trust, health administration, municipality, hospital, medical practice, dental clinic, pharmacy, pharmaceutical chain, X-ray institute, independent laboratory, university, university college, foundation etc. or processor/supplier which is obligated through an agreement to comply with the Code.

"**Other information of significance to information security**" means, for the purposes of this Code, information where unauthorised access or other security breaches would entail a risk to the enterprise, e.g. configuration files, results of risk assessments, preparedness plans, password files, network maps etc.

-P-

"**Patient**" means, for the purposes of this Code, a person who contacts the health and care services requesting healthcare, or to whom the health and care service provides or offers healthcare, as the case may be; see Section 1-3(a) of the Patient and Users' Rights Act.

"**Patient safety**" means, for the purposes of this Code, protection against unnecessary harm/injury as a result of the provision or non-provision of health services.

“**Personal data**” means, for the purposes of this Code, any data concerning an identifiable natural person (“the data subject”); an identifiable natural person is a person who can be either directly or indirectly identified, particularly with the aid of an identifier, e.g. a name, an identification number, location data, an online identifier or one or more elements which are specific to the aforementioned natural person’s physical, physiological, financial, cultural or social identity.

“**Personal health data**” is, for the purposes of this Code, a common term for health data or personal data within the scope of the Code.

“**Personal health data filing system**” means, for the purposes of this Code, filing systems, lists etc. in which health data is systematically stored so that data concerning an individual person can be retrieved; see Section 2(d) of the Personal Health Data Filing System Act.

“**Personal data security”** means, for the purposes of this Code, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage through the use of appropriate technical or organisational measures.

“**Processor**” means, for the purposes of this Code, a natural or legal person, public authority, institution or any other body that processes personal data on behalf of the controller. It should be noted that a processor is an external person or organisation outside the controller’s organisation. This means that the controller’s own employees are not the controller’s processors.

“**Processing**” means, for the purposes of this Code, any operation or series of operations which is or are performed on personal data, whether automated or not, e.g. collection, registration, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure through transfer, distribution or any other form of disclosure, compilation or coordination, limitation, erasure or destruction.

“**Processing basis**” means, for the purposes of this Code, a legal basis for the processing of personal data. This could for example be consent or an authority laid down in law. What constitutes a valid basis for processing is set out in Articles 6 and 9 of the General Data Protection Regulation.

“**Personal health data filing system for therapeutic purposes**” means, for the purposes of this Code, a health record and information system or other filing system, list or similar, in which health data is systematically stored so that data concerning an individual can be retrieved as a basis for the provision of health and social care services or the administration of health and social care services to individuals; see Section 2(d) of the Patient Records Act

-R-

“**Resilience**" means, for the purposes of this Code, the ability of the organisation and the information systems to restore normal conditions following a physical or technical incident, for example. This is achieved through appropriate technical and organisational measures which facilitate the prevention, detection, scalability, handling and restoration of personal data security and information security in general.

“**Record of processing activities**” means an overview of processing activities in accordance with the provisions of Article 30 of the General Data Protection Regulation.

“**Recipient**” means, for the purposes of this Code, a natural or legal person, public authority, institution or any other body to which personal data is made available, whether or not the body is a third party. Public authorities which can receive personal data within the framework of a special investigation in accordance with European Union law or the national rights of Member States shall however not be deemed to be recipients; the processing of such data by the aforementioned public authorities shall take place in accordance with the applicable provisions concerning the protection of personal data in accordance with the purpose of the processing.

-S-

“(**The**) **sector**” means, for the purposes of this Code, the health and care services sector or one or more parts thereof.

“**Self-authorisation**" means, for the purposes of this Code, authorisation given to healthcare personnel in order to gain access to personal health data which they do not require as part of their professional duties.

“**Sensitive personal data/special categories**” means, for the purposes of this Code, data concerning:

a) racial or ethnic origin, or political opinions, philosophical or religious beliefs
b) the fact that a person has been suspected of, charged with, indicted for, or convicted of a criminal offence
c) health (personal health data)
d) sex life
e) trade union membership

“**Secure authentication system**” means, for the purposes of this Code, an authentication system which, for example, is based on the use of personal qualified certificates or any other authentication system that through a risk assessment has been shown to provide adequate security.

“**Shared component**” refers to reusable solutions covering typical needs in the field of digitalisation, such as login, authentication, registers etc.

“Subcontractor” means, for the purposes of this Code, an organisation which enters into a contractor to fulfil some or all of the obligations under a processor’s agreement.

“**Supplier**” means, for the purposes of this Code, a legal entity which provides technical or administrative services to the organisation. 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 this 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 include authentication via a personal qualified certificate or the configuration of a firewall such that it only permits specific data traffic or a message service that is designed in such a way that all messages are automatically encrypted.

"**Third party**" means, for the purposes of this Code, any other natural or legal person, public authority, institution or any body other than the data subject, the controller, the processor and the persons who have authority to process personal data under the direct authority of the controller or the processor.

6.3 Supporting documents

Linked to the Code, a series of supporting documents have been prepared in the form of fact sheets, guidelines and templates. This material covers most areas within information security.

The supporting documents are not binding and are to be considered as guideline documents only. In the event of a contradiction between the Code and supporting documents, the Code shall take precedence.

6.3.1 Fact sheets

The fact sheets describe in more detail how the organisations can fulfil certain key requirements in the Code of Contract and provide practical guidance concerning this. The fact sheets are thematic and comprise 1-4 pages.

6.3.2 Guidelines

Guidelines are supporting documents 30-50 pages long which cover a particular thematic area or sub-sector in detail.

6.3.3 Templates

In conjunction with the fact sheets and guidelines, templates have been prepared in the form of document templates and checklists which give users an editable version for use in their own organisation.

6.4 References

All laws and regulations: https://lovdata.no/

The website for the Code of Conduct for Information Security in Healthcare and Care Services: https://www.ehelse.no/normen

The Directorate of Health's circulars and guides:
https://www.helsedirektoratet.no/produkter?tema=rundskriv

PKI (Public Key Infrastructure) - Specification of Requirements:
https://www.digdir.no/standarder/pki-public-key-infrastructure-kravspesifikasjon/1697

NSM's guide to crypto requirements:
https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

NSM's basic principles for ICT security, version 2.0: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1//

Guidance to identification and traceability in electronic communication with and in the public sector: https://www.digdir.no/digital-samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992

Reference directory for eHealth. E-health standards and other requirement documents which are obligatory pursuant to a regulation or recommended by a public authority:
https://ehelse.no/standarder-kodeverk-og-referansekatalog/referansekatalogen

The Norwegian Digitalisation Agency's website on information security:
https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet

Norwegian Data Protection Authority: https://www.datatilsynet.no/

The European Union Agency for Network and Information Security (ENISA):
https://www.enisa.europa.eu/

US National Institute of Standards and Technology, NIST:
https://www.nist.gov/topics/cybersecurity

European Data Protection Board (EDPB): https://edpb.europa.eu/

6.5 History of the Code

FIRST EDITION
An increasing proportion of the work carried out within the healthcare and care services sector is based on the electronic processing of patient information. More and more communication between the organisations is also taking place electronically.

The increasing proportion of electronic data processing is opening up new opportunities, but it is also creating challenges relating to information security amongst the organisations involved. Among other things, electronic processing enables data to be made available more readily and faster both internally within an organisation and externally outside the organisation. This is an advantage, provided that the data is only made available to the right people at the right time. However, unintended consequences can arise regarding data confidentiality, and specific measures must be established to ensure that unauthorised persons are prevented from gaining access to data which is stored electronically.

Mechanisms are needed which enable everyone involved to be confident that every aspect of information security has been satisfactorily addressed by the organisations concerned.

This forms the background to the Directorate for Health and Social Affairs' initiative to ensure that the healthcare and care services sector prepares its own Code of conduct for information security. The Code has been prepared by representatives of the sector, including representatives from the Norwegian Medical Association, the regional health trusts, the Norwegian Nurses' Organisation, the Norwegian Pharmacy Association and the Norwegian Association of Local and Regional Authorities. The Norwegian Data Protection Authority, the Norwegian Board of Health Supervision, the National Insurance Service and the Directorate for Health and Social Affairs also participated in the work.

The aim of the Code is to contribute to satisfactory information security within the health sector. The Code is also intended to be an aid for individual organisations in their work relating to information security. In addition to satisfactory information security, the Personal Health Data Filing System Act, the Personal Data Act and other regulations also impose a number other requirements on the handling of patient data. These requirements are not considered in this Code.
28 June 2006.

SECOND EDITION

During the summer of 2008, the steering group for the Code decided to incorporate changes in the Code as a result of changes in legislation and regulations, and a desire to promote electronic interaction between organisations within the sector. Another new development is that Norsk Helsenett (Norwegian Healthnet), private laboratories, the Norwegian Dental Association, the Public Dental Service and the Norwegian Pharmaceutical Association have now joined the steering group for the Code. Additionally, the Ministry of Health and Care Services and the Agency for Public Management and eGovernment (Difi) have joined as observers.

The Norwegian Directorate for Health and Social Affairs has withdrawn from the steering group of its own accord.

In the autumn of 2009, the steering group decided to expand the scope of the Code. The Code now covers the healthcare, care and social services sectors.

At the same time, it was decided that issues linked to employee privacy should be included in the Code as and where appropriate.

In June 2009, the Norwegian Parliament (the Storting) amended the Personal Health Data Filing System Act. This facilitated the adoption of regulations concerning:

- access to personal health data across organisations
- the establishment of supra-organisational personal health data filing systems for therapeutic purposes
- the establishment of supra-organisational personal health data filing systems for therapeutic purposes for healthcare personnel in a formal working partnership

No such regulations have been issued and the above topics are not considered in the Code.
2 June 2010.

SECOND EDITION, VERSION 2.1

On 29 November 2012, the steering group for the Code decided to amend the requirement for security level 4 in order to permit alternative solutions, subject to the condition that a risk

assessment documents and confirms that any such alternative solution provides an adequate level of security.

THIRD EDITION

On 5 December 2013, the steering group for the Code decided to incorporate changes as a result of the regulations concerning multi-organisational patient records in formalised working partnerships. Additionally, responsibility for the register of authorisations was clarified, rules regarding the disclosure of personal health data for quality assurance and training purposes were incorporated, and reference is made to the document “Requirement specification for PKI in the public sector (*Kravspesifikasjon for PKI i offentlig sektor*) with regard to minimum requirements for encryption strength.

FOURTH EDITION

On 5 June 2014, the steering group for the Code decided to incorporate changes as a result of the repeal of the Social Services Act from 1991 (LOV-1991-12-13-81). The scope of the Code was amended to the healthcare and care services at the same time. In addition, the Code was amended to make it clear that it applies to services provided by the Norwegian Labour and Welfare Service (NAV) linked to the health net and to municipal services provided by local NAV offices which are connected to the health net.

FIFTH EDITION

On 12 February 2015, the steering group for the Code decided to incorporate changes as a result of the new Personal Health Data Filing System Act, the Patient Records Act and the Regulations concerning access to personal health data between organisations.

FIFTH EDITION, VERSION 5.1

On 4 June 2015, the steering group for the Code decided to revise the wording of the requirements concerning the documentation of measures (section 3.3) in accordance with the requirements of the Freedom of Information Act.

FIFTH EDITION, VERSION 5.2

On 9 June 2016, the steering group for the Code decided to clarify the text relating to the legislation regarding joint personal health data filing systems. Certain sentences were also revised in order to clarify the requirements.

FIFTH EDITION, VERSION 5.3

On 31 May 2018, the steering group for the Code approved a number of changes which represented the first step on the path to a major revision and development of the Code.

Regulation (EU) 2016/679 of 27 April 2016 is transposed in Norwegian law through the new Personal Data Act of 2018. This also led to certain changes and adaptations in the health legislation.

The aims of version 5.3 were to ensure that the requirements set out in the Code are compatible with new legislation, to expand the scope of the Code to encompass more data protection and to update the Code to include new requirements which take account of technological advances. The Code was given a new structure, and reviewed to ensure that there are no contradictions between the Code and new legislation. Certain articles from the Regulation were also specifically incorporated:

- Article 30 - Record of processing activities
- Article 32 - Security of processing
- Articles 33 and 34 - Communication of a personal data breach to the data subject
- Article 35 - Data protection impact assessment
- Articles 24 and 28 - Controller and processor

- Articles 27 and 38 - Data Protection Officer

6th edition, version 6.0

The Steering Committee for the Code of Conduct approved a major revision to the Code on 4 February 2020.
This version of the Code is the result of a protracted revision and development process. The main objectives were to ensure that the requirements of the Code are comprehensive as regards the new requirements of the General Data Protection Regulation (GDPR), as well as being technology-neutral and compatible with current technology. A further important objective was to simplify the text and make the Code easier to read and more user-friendly. Amongst other things, new requirements have been incorporated, text has been deleted and requirements have been clarified or amended. The scope of the Code has been altered and the requirement for proportionality has been made clearer. The text has been reviewed and simplified, and some text has been deleted and moved to the guidance. Version 6.0 was subject to an extensive consultation process.

6th edition, version 6.1

The Steering Committee for the Code of Conduct approved changes to the way in which risk is addressed in the Code on 21 November 2022. The Code switched to using acceptance criteria for risk instead of levels of acceptable risk. Furthermore, the Steering Committee decided that the Code would use the word ‘harmful’ rather than ‘malicious’ software. The definition of “personally qualified certificate” was removed.

At the same time, the entire document was reviewed and outdated references were updated.

NORMEN

Visiting address
Norwegian Directorate of eHealth
Verkstedveien 1
0277 Oslo

Contact
sikkerhetsnormen@ehelse.no