NORMEN

Code of Conduct for Information Security and Data Protection in the Health and Care Services Sector

Version 7.0

Applicable from 01/10/2025

Published with the support of

Helsedirektoratet

Publication title:
Code of Conduct for Information Security and Data Protection in the Health and Care Services Sector

Version number
7.0

Approved by the Steering Committee for the Code of Conduct:
03/06/2025

Applicable from:
01/10/2025

Published with the support of:
Norwegian Directorate of Health

Contact:
normen@helsedir.no

This publication is available to download from:
www.normen.no

Preface

In the Norwegian health and care services sector, large volumes of data are processed as a basis for high-quality health and care services, personal health data filing systems, research and innovation.

The data must be processed to enable health and care services to be provided appropriately, and in a manner which also safeguards the trust of citizens in the sector. Ensuring a high level of information security and data protection is essential for digitalisation. The technologies, organisation and safety culture built and managed by the sector must be resilient.

Against the backdrop of threat and risk assessments, new legislation, advances in technology and past high-profile incidents, there has been increasing awareness surrounding data protection and information security in the health and care services sector.

As a result, an increased need has arisen for updated guidance and a modernised and updated Code of Conduct for Information Security and Data Protection in the Health and Care Services Sector ("the Code").

This version of the Code is the result of a revision and enhancement process. The main objectives were to update the Code to bring it into line with the requirements of the Norwegian Digital Security Act and appurtenant regulations. The health and care services sector is defined in Norway as a 'provider of services *important* to society', including digital services. This entails that essential requirements must be specified for information security in network and information systems, processes, products and services in order to prevent, detect, deter and manage undesirable or unplanned circumstances (incidents). At the same time, the Code is to remain technology-neutral and aligned with current advances in technology.

Contents

1 About the Code

1.1 What are 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 in order to provide and quality-assure health and care services, and to learn lessons from service provision. Researchers need the data in the interests of developing better services in the sector.

An Adequate level"level of patient safety requires data to be stored and shared among healthcare professionals; the data to be accurate and up-to-date; and patients⁄service users and healthcare professionals to have confidence in systems and personnel. Inadequate information and failures in transitions within and between healthcare service levels have been documented as being a key risk area for a high standard of patient safety.

See also the official circular on data management in the specialist health service (in Norwegian): “https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049“

Information security involves protecting personal health data, as well as securing networks and information systems that are essential in providing safe and appropriate health and care services. This includes technical, organisational, physical, personnel and legal measures to safeguard the integrity, availability and confidentiality of the data, regardless of where and how the data is processed.

A key objective is to build resilient systems and processes capable of withstanding both known and unforeseen threats. Information security is designed to help reduce risk and prevent, detect and manage incidents whether they are caused by human error, technical failure or deliberate attacks.

“Integrity”, means, for the purposes of this Code, that personal health data shall be protected against accidental or unauthorised modification or deletion. Integrity is a prerequisite for good and appropriate healthcare.

“Availability”, means, for the purposes of this Code, that personal health data that is to be processed is available at the time and place it is needed. For healthcare professionals, 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. This fulfils the legal and ethical duty of confidentiality and respect for privacy concerning information given by or about an individual in a medical or care setting, which is an important factor in maintaining the trust of citizens in the health and care services.

“Security measures” means technical, organisational, physical and personnel measures deemed conducive to achieving satisfactory information security and data protection in the sector based on risk assessment.

The General Data Protection Regulation (GDPR) also uses the term “resilience” as well as integrity, availability and confidentiality. “Resilience”, means, for the purposes of this Code,

the ability of an organisation and information systems to restore normal conditions following a physical or technical incident, for example. Resilience is achieved through appropriate technical and organisational measures that enable prevention, detection, scalability, management 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, to respect for their personal integrity and personal privacy, are pivotal. Data protection is therefore closely linked to the right of individuals to privacy, self-determination and self-expression.[1]

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 refers to as “security of processing”. 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 resilience.

1.2 What is the Code?

The Code is a sector-wide code of conduct compiled and administered by organisations and enterprises in the health 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 (Norwegian version at: lovdata.no)

The Code is intended to help ensure appropriate information security and data protection measures on the part of individual organisations, and in infrastructure and network and information systems in the sector generally. A further objective of the Code is to help prevent, detect, deter and manage incidents in network and information systems, services and products used for providing digital services in the sector. Furthermore, the Code is intended to help ensure that an organisation that complies with the Code has appropriate technical, organisational, physical and personnel measures in place for information security and data protection for its processing of personal health data.

Further, the aim of the Code is to help ensure that organisations have mutual confidence that processing of personal health data by other organisations will be carried with a satisfactory level of security. Those who interact with an organisation that has undertaken to comply with the requirements of the Code must be able to trust that this organisation has appropriate technical, organisational, physical and personnel measures in place regarding information security and data protection for its processing of personal health data.

The Code is intended to ensure that patients, service 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, and is intended

to support high-quality healthcare, a high level of patient safety, quality assurance, health personnel learning and training, robust data protection and a patient-centred health service.

1.3 Who does the Code apply to?

The Code applies to any organisation that has undertaken to comply with it under a formal agreement.

1.4 Relationship between the Code and applicable legislation

The legislation imposes requirements regarding information security and data protection. These requirements apply independently of the Code. Relevant supervisory authorities are mandated to verify each organisation's compliance with these regulatory requirements.

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

The applicable 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. This includes matters relating to the use of personal health data for purposes other than the provision of health and care services. This encompasses specific requirements for data filing systems subject to certain regulations, the legal basis for the processing of personal health data, and record-keeping obligations and requirements. Information security is also regulated in legislation other than that relating to the processing of personal data.

Applicable legislation imposes requirements regarding information security in network and information systems, products, services and processes used in providing health and care services, and personal data protection. The requirements of the Digital Security Act and appurtenant regulations apply to organisations such as the regional health authorities, national e-health solutions such as systems for ordering and dispensing medicines, as well as municipalities with more than 50,000 inhabitants or more than 20,000 users who are dependent on health and care services.

The aim is to prevent, detect and deter incidents, and ensure that businesses have appropriate technical, organisational, physical and personnel security measures in place. Other requirements in the Code apply to all organisations in the health and care services sector that have committed to comply with it under a formal agreement. The scope of the Code is limited by the provisions of the Norwegian Security Act.

The Code's requirements elaborate on and supplement applicable regulations. Compliance with the requirements of the Code can be used to demonstrate an organisation's regulatory compliance.

The Code includes limited references to applicable legislation. Statutory and regulatory requirements in the Code are presented 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, technical, physical and personnel measures deemed appropriate for achieving a satisfactory level of information security and data protection in the sector.

When selecting organisational, technical, physical and personnel security measures, the organisation shall consider the measures in relation to the organisation's scale, nature, complexity and scope with respect to the processing of personal health data, patient safety and the risk landscape, etc. The measures shall be selected based on risk assessments, and the measures shall be proportionate. This may mean that large organisations processing personal data on a large scale should establish more measures than small organisations processing personal data on a small scale, and where the risks are less complex and more manageable.

The Code provides a guide for small healthcare enterprises detailing best practices in information security and personal data protection for small enterprises.

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

Although the Code is not exhaustive with regard to the processing of personal health data where the purpose is not the provision of health and care services (e.g. processing of health data for statistical purposes, health analyses, research, quality improvement, planning, management and emergency preparedness in health and care services administration and health and care services provision), relevant requirements regarding information security and data protection as described in the Code apply nonetheless. The requirements for information security and data protection are essentially the same in legislation governing both personal health data filing systems for therapeutic purposes and other applications of personal health data. Organisations shall assess which requirements in the Code apply based on the specific processing of personal health data (section 3.1 Proportionality in selection of information security
measures).

Organisations also process personal data concerning their own employees. The Code is not exhaustive as regards such processing. Organisations shall safeguard the privacy of their employees in accordance with applicable acts 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 the right to access data concerning themselves (see Article 15, GDPR).

The Code contains requirements covering the majority of information security and data protection topics: people, processes, technology and network and information systems, services and products. The Code also includes supporting documents in the form of guidance. For the guidance materials and examples of measures, see section 6.2

The Appendix "Overview of the Code's requirements" lists all the "shall requirements" in the Code that are pursuant to legal acts or regulations, as well as references to ISO 27001:2023 and 27002:2022.
https://www.helsedirektoratet.no/digitalisering-og-e-helse/normen-personvern-og-informasjonssikkerhet/normen/oversikt-over-normens-krav-og-mapping-mellom-nsms-grunnprinsipper-iso-og-ccm/_/attachment/inline/ab854945-5539-4250-983d-

29cb41036ad2:a4f39d140f431200f78dd80fe8851e190e1eb2bd/Vedlegg%20til%20Normen%20-%20Oversikt%20over%20Normens%20lovkrav.xlsx

1.6 Development and administration of the Code

The Code was compiled and is administered by a steering committee representing the health and care services sector.
Unanimity is sought on the Committee when fundamental issues are considered.

The Norwegian Directorate of Health is the secretariat for the work of the steering committee, with permanent representation of Norsk Helsenett, the Norwegian national e-health service provider.

2 Management and responsibility

The senior management of an organisation shall be responsible for ensuring that the organisation complies with applicable information security and data protection requirements. For entities subject to the Digital Security Act, this entails establishing and maintaining an appropriate level of security in line with the requirements of the Act.

For organisations not subject to the Digital Security Act, the Code requires that the organisation's data processing maintains an appropriate level of safety commensurate with the risk and nature of the processing.

Where the Code uses the term "appropriate" level of security, for organisations subject to the Digital Security Act, this should be understood to mean "appropriate" in the sense used by the GDPR, for example. In other words, this is a level of security that is commensurate with the risk and in compliance with regulatory requirements.

Furthermore, management shall ensure that all the necessary organisational, technical, physical and personnel security measures are implemented to reduce risk and maintain an appropriate level of security within the organisation. This responsibility should be addressed as part of corporate governance and quality improvement activities.

Responsibilities include:

- establishing guidelines for risk assessment and risk management,[2] and include defining risk acceptance criteria; and
- ensuring effective management and control.

Organisations shall document all implemented information security and data protection measures.

Organisations subject to both the requirements of the Code and the Regulation on management and quality improvement within the health and care services sector (*Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten*) should rely on the provisions of that Regulation as a basis for ensuring their compliance with the information security and data protection requirements of applicable health and care services legislation.

2.1 Roles and responsibilities regarding information security and data protection

The senior management of an organisation shall ensure that roles and remits are established with sufficient resources and expertise for performing the tasks necessary in order to fulfil the responsibility for information security and data protection. These tasks can be performed by the organisation's own employees or a contracted third party.

The individual responsible for a remit or unit should also be responsible for enforcing information security and data protection within that remit or unit.

The organisation decides which roles and remits are necessary for information security and data protection. It shall be clear who is responsible and what they are responsible for. Everyone shall be familiar with their duties and be adequately informed of the responsibilities and duties of others, and of who has the power to make decisions.

Large organisations should have a designated information security manager or a security organisation linked to the organisation's management.

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 as necessitated by the scope, nature and purposes of its information processing. This also applies to small enterprises. The Data Protection Officer may be an employee of the enterprise or an external contractor performing the tasks on the basis of a service agreement.

The Data Protection Officer shall be afforded sufficient resources and access to relevant expertise to perform their duties. The Data Protection Officer shall not have any conflicts of interest with any other roles they may have within the enterprise, and shall not receive instructions on how tasks are to be performed.

2.2 The controller's responsibilities

The controller is the organisation which, either alone or jointly with other organisations, 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, maintain and comply with the governing system (see section 2.4);
- conduct risk assessments and draw up a plan for risk management (see Chapter 3);
- carry out data protection impact assessments (DPIA) for processing operations as and when necessary (see Chapter 3);
- safeguard the rights of data subjects (see Chapter 4);
- establish, document and implement organisational, technical, physical and personnel security measures (see Chapter 5);
- conclude and enforce agreements (see section 5.7);
- report and manage non-conformities (see section 5.8);
- implement measures for physical security (see section 5.2);
- ensure that security measures are made known to staff and suppliers (see section 5.1.2);
- ensure adequate expertise in information security and data protection, and training as required (see section 5.1.2); and
- establish and document contingency plans and carry out drills (see section 5.9).

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

- be processed lawfully (legal basis for processing);
- be processed fairly (respecting the interests and rights of data subjects);
- be processed transparently (clear, predictable and comprehensible information) with regard to the data subject (patient/user);
- be registered only for specific purposes that shall be legitimate (such as the documentation of healthcare);
- be available to healthcare professionals 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, kept 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 of time longer than necessary for the purposes; and
- be protected against unauthorised access, alteration, destruction and dissemination.

The controller shall document that the organisation has implemented the necessary measures for GDPR-compliance.

2.3 Data processor's responsibilities

Under the Code, a processor is an organisation that processes personal health data on behalf of the controller. Like the data controller, the processor has an independent responsibility for information security and for addressing data protection for 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; and
- assist the controller in ensuring fulfilment of information security obligations

The processor shall assist the controller with data protection and information security by ensuring a risk-based approach. This means that the processor shall assist in ensuring that an appropriate level of security is maintained, and that the necessary measures are implemented.

For further details of processor responsibilities, see section 5.7.4.

2.4 Management system

All organisations shall have a management system for information security and data protection (internal control). 'Management system' means formalisation of how the organisation plans, carries out, evaluates, controls and rectifies activities for compliance with relevant regulations, safety requirements, agreements, services and products.

Information security and data protection should be integral to the overall management system within the organisation. The management system must be appropriate for the organisation's size and function according to a risk-based approach. It should consider the organisation's risks, characteristics, and activities, as well as the nature, scope, purpose, and

context of information processing. This means that smaller organisations do not require a management system as comprehensive as that of larger organisations.

See The Code's guide on internal control for information security for guidance on what should be included in a management system and the Code's guide for small healthcare enterprises.

The organisation's management is responsible for establishing objectives and strategies for information security, establishing a management system and a security organisation with roles and responsibilities, and for ensuring that this is integrated as part of overarching corporate governance. The organisation's manager must allocate sufficient funds and resources for implementation of all necessary activities to establish and maintain an appropriate level of security within the organisation.

The management system shall be approved by the organisation's manager and reviewed at least annually with a view to improving the organisation's data security work.

The management system shall be made known to all employees on a need-to-know basis, and to suppliers and subcontractors.

The management system shall be documented. Documents specified in the management system shall be updated on an ongoing basis, continuously improved and archived from the date on which the document is superseded by a new current version. This may include procedures for security audits, risk assessments, operational procedures, non-conformities and the way in which they are managed, the management's review, data processing agreements, etc.

Documentation of information security risks and measures shall be ensured based on prevailing security needs. If documentation must be shared with other organisations, the controller must assess whether detailed information that may have an impact on data security must be redacted prior to disclosure. The documentation shall be up-to-date and available at all times.

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

2.5 The management's review

The organisation's senior management is responsible for ensuring that the organisation maintains an appropriate level of security and complies with applicable information security and data protection requirements. The management shall review the organisation's management system for information security and data protection at least once a year.

The basis for the review shall include assessment of:

- the status of activities in the previous management review;
- changes in the processing of personal health data (records);
- changes in the organisation of the work;
- results of risk assessments and the status of risk management plans;
- results of data protection impact assessments (DPIA);
- results of audits;

- results of non-conformity management;
- follow-up of suppliers and data processing agreements; and
- changes in acceptable levels of risk.

The outcome of management's review shall include decisions on any need for changes to the management system. If the review indicates that the organisation's risk exposure is unacceptable, action plans shall be adopted to remedy this, with deadlines and assignment of responsibility. The management's review shall be documented.

3 Risk management

Risk management comprises coordinated activities to guide and control a business with regard to risk. This includes obtaining an overview of information and technology within the organisation, identifying threats, vulnerabilities and the consequences of potential incidents for both the organisation and the data subjects, analysing the risk and establishing measures to maintain an appropriate level of security.

The organisation shall establish and implement security measures that are appropriate for managing risk in a satisfactory manner. This includes safeguarding the confidentiality, integrity, availability and resilience of network and information systems. These considerations shall be balanced.

When evaluating an acceptable level of risk, consideration shall be given to advances in technology, implementation costs and the nature, scope, purpose and context of data processing. Risk management efforts shall take into account, for example, the type and volume of data, the size of the organisation and the complexity of the processing.

3.1 Proportionality in selection of information security measures

When assessing and selecting security Controls, organisations shall consider the measures in relation to the nature, scope and complexity of the organisation’s processing of personal health data and patient safety. When assessing technological security measures, the organisation’s operating environment, user environment, system performance versus risk in the organisation’s networked systems and information systems.

The security measures shall collectively ensure a level of security aligned with the risk picture, and shall aid incident prevention, detection, management and mitigation. This applies in particular to the assessment of an appropriate security organisation, service provider tasks, control tasks and measures relating to information security, network and information systems, services, products and processes (such as access management, logging, incident response, physical security, supply chains, procurement, etc.).

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

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

Organisations shall ensure that their processing of personal health data has an appropriate level of security in line with the minimum requirements for information security set out in the Code and any organisation-specific information security objectives. The Code imposes the following general minimum requirements for information security (confidentiality, integrity, availability and resilience):

Requirement to safeguard confidentiality
The organisation shall ensure that the duty of confidentiality is fulfilled, and otherwise ensure that unauthorised persons do not gain access to data by:

- preventing unauthorised access to personal health data and other information of significance for information security;
- restricting access by authorised personnel based on official need; and
- maintaining an overview (logs) of everyone who has gained access to personal health data and other information of significance for information security.

Requirements to safeguard integrity
The organisation shall ensure that personal health data and other information of significance for information security is protected against accidental or unauthorised alteration or erasure. Integrity is a prerequisite for safe and appropriate healthcare

- log who has corrected, entered, 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 recorded in accordance with relevant code lists and terminology;
- ensure that personal health data is accurate and, if necessary, updated; and
- prevent copies of data from becoming a source of outdated information.

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

- ensure that personal health data is available only on the basis of official need;
- ensure reliable and stable operation of network and information systems, including resilience and post-incident capacity to restore normal conditions;
- ensure that technical, organisational, physical and personnel measures are in place to enable prevention, detection, scalability, management and restoration; and
- ensure that information systems are available in accordance with the organisation's availability requirements.

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

3.3 Overview of technology and personal health data processing

By establishing and maintaining an overview of the personal health data that is processed and the technology that is used, the organisation shall identify potential risk areas it should be especially alert to.

Organisation shall keep:

- records of personal health data processing; see The Code factsheet on keeping records of personal health data processing within organisations (Factsheet 13); and
- an overview of information systems, ICT processes, ICT services, infrastructure and other information of significance for information security, etc. Organisations shall also

map the potential impacts of system failures and classify those systems; see section 5.9. The overview should be documented.

Areas for risk assessment should be based on the overview of personal health data that is processed and the overview of information systems that are used, as well as identification of potential threats and vulnerabilities. The risk assessment should also include assessment of organisational, technical, physical and personnel measures to ensure integrity, availability and resilience.

3.4 Risk assessments and risk management

3.4.1 Risk assessments

Risk assessment is a tool and should be conducted at a level of scope that enables the organization to identify the necessary security measures. The organisations shall devise, maintain and document risk assessments. In the event of changes in the organisation that might impact information security, the risk posed by such changes shall be assessed.

Risk assessments shall as a minimum comprise:

- mapping of the organisation's network and information systems as well as their criticality for provision of services important to society;
- identification of potential incidents that could impact the organisation's network and information systems;
- analysis of vulnerabilities related to the organisation's network and information systems;
- assessment of the likelihood of an incident occurring;
- assessment of the potential impacts of incidents; and
- analysis of the organisation's dependence on other organisations for optimal performance.

The risk assessment should be based on a mapping of information assets and the consequences of incidents impacting the availability, integrity and confidentiality of the information assets. The organisation shall assess the likelihood of an incident occurring and the consequences of that incident. If the risk is unacceptable, the organisation shall implement measures to mitigate the risk. For more information, see The Code's guidance on risk management for information security and data protection

The organisation shall carry out risk assessments, as a minimum before:

- establishing or changing the processing of personal health data;
- establishing new data processing systems or data filing systems containing personal health data;
- changing existing information systems or data filing systems that contain or utilise personal health data;
- establishing organisational, technical, physical, personnel measures or other changes of significance for information security; and
- establishing or changing access to health data between organisations.

Risk assessments should be updated in the event of changes in the threat landscape. In addition, the organisation's management shall regularly carry out risk assessments as part of its efforts to monitor information security.

3.4.2 Risk management

Based on the risk assessment, organisations shall have a plan in place for managing risk. As part of their risk management, organisations shall implement the necessary security measures for mitigating risk and maintaining an appropriate level of security.

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

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 persons responsible for implementation. The plan shall be formally approved and sponsored by the organisation's management.

If planned technical measures to achieve an acceptable level of risk cannot be implemented immediately, risk-mitigating administrative measures should be considered, e.g. in the form of procedures.

Organisations shall ensure that they have sufficient expertise at their disposal for risk assessment. Representatives of those providing healthcare should be involved where relevant. Persons carrying out risk assessments shall have a clear escalation path to the management/board. The results of the risk assessment and a plan for following up on measures shall be communicated with the appropriate level of detail to the organisation's management and, where relevant, the board.

3.5 Assessment of consequences for data protection

Organisations shall in any event assess the consequences for data subjects of processing their personal health data. Organisations shall document the lawfulness of the processing, the purpose, how the privacy of the data subject will be protected, and that sufficient risk management measures have been implemented. If processing is likely to pose a high level of risk to the data subjects concerned, the organisation shall carry out a more thorough assessment in the form of a Data Protection Impact Assessment (DPIA).

3.5.1 Data Protection Impact Assessment (DPIA)

The DPIA shall be completed before processing of personal data commences. For more information and guidance on when to conduct a DPIA, see the Norwegian Data Protection Authority's website: (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/).

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 processing is automated, systematic and extensive and informs decisions that will have legal or similar substantive effect on data subjects; or
- as entailed by the nature, scope, purpose and context of the processing.

The Norwegian Data Protection Authority has published a list of processing activities that always require a DPIA.

A DPIA shall as a minimum contain:

- a systematic description of the personal health data processing operations;
- a description of the purpose of the personal data processing;
- an assessment of the necessity and proportionality of the personal health data processing operations in relation to the purposes;
- an assessment of the data protection risks to the data subjects; and
- planned risk mitigation measures in order to safeguard data protection.

When carrying out a DPIA, the controller shall consult the DPO, if a DPO has been designated.

Measures must be planned to mitigate the data protection risk. If the processing of personal health data poses a high risk that cannot be mitigated by reasonable measures, the controller shall request an advance consultation with the Norwegian Data Protection Authority before the processing commences.

4 Fundamental considerations regarding the processing of personal health data

Patient care requires the processing of health data on patients. The duty to document patient care is intended to help ensure that patients and service users receive high-quality health and care services and to support health professionals in their 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 Norwegian healthcare sector is governed by numerous acts and regulations containing specific rules regarding the processing of personal health data, and these supplement the requirements of the personal data legislation. Healthcare legislation is largely based on the rights of patients and users and the obligations of the healthcare and service providers. The scope of the Code is limited to key rights and obligations in legislation that concern the processing of personal data.

See The Directorate of Health circulars on the Health Personnel Act and the Patient and User Rights Act

The healthcare professional's duty of confidentiality is a key aspect of data protection and a prerequisite for the trust-based interaction between patients and healthcare professionals.

4.1 Legal 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 termed a 'legal basis for processing'.

The processing of special categories of personal data, such as health data, is essentially prohibited under the GDPR. However, exceptions apply, such as when consent has been given, when healthcare and social services subject to the duty of confidentiality are provided, when public health considerations render it necessary, and for research purposes.

For more guidance on legal basis for processing (www.datatilsynet.no) ref. GDPR, Article 6 Lawfulness of processing and Article 9 Processing of special categories of personal data.

Before the processing of personal health data commences, or 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 are 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 legal basis for processing.

Article 6 of the GDPR refers to six legal bases for processing:

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

- 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 of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise 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 legal 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 treatment necessary in order to provide appropriate health and care services?

The duty to keep records gives organisations a legal obligation to process personal health data. Most processing of personal data in the health 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. data disclosure.

Other processing of personal data by an organisation may have other bases for processing. Examples of such bases for processing would be agreements with data subjects in connection with the follow-up of employees, or if an organisation performs non-healthcare tasks, both consent and an agreement may constitute a basis for processing.

If more than one legal basis for processing is applicable, the organisation shall identify one legal basis per purpose.

The controller shall determine the legal basis for processing.

The legal basis for processing shall be documented. This can be done in the record.

See section 3.3. Overview of technology and processing of personal health data and [The Code factsheet on keeping records of personal health data processing within organisations (Factsheet 13)]

4.2 Duties and obligations when processing personal health data

Data subjects have a number of rights regarding the processing of their personal health data. Organisations shall facilitate technical, organisational, physical and personnel measures to ensure that data subjects can exercise their rights.

This section covers duties and obligations under both data protection legislation and healthcare legislation. The section heading indicates where the text only applies to personal health data filing systems for therapeutic purposes.

4.2.1 Duty of confidentiality

Enterprises shall ensure that all staff granted access to personal health data and other confidential information are familiar with their duty of confidentiality.

The organisation shall ensure that staff fulfil their duty of confidentiality. This should as a minimum be ensured through:

- access control, logging and subsequent control;
- safeguarding of network and information systems;
- procedures, training and information; and
- design of physical premises.

Any breach of the duty of confidentiality constitutes a non-conformity and is associated with both administrative and criminal sanctions.

4.2.2 Information for data subjects

Organisations have a duty to provide information to the data subject in a concise, transparent, comprehensible and readily accessible manner, and in clear and plain language. Universal design requirements must also be complied with in this context.

The information shall be provided in writing or by other means, including electronically if appropriate. At the request of the data subject, information may be provided verbally provided that data subjects identify themselves.

When collecting information, the controller shall inform data subjects, in a comprehensible manner, of their rights and how their personal data will be 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.

Organisations shall ensure that data subjects are 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 accessed and when.

Organisations shall ensure that data subjects are able to find out what personal data the organisation processes about them. This also includes finding out the names of individuals from other organisations that have obtained the information.

Organisations shall ensure that any person exercising their rights is identified.

4.2.3.1 Access to personal treatment-oriented health register

Patients generally have right of access to all data relating to themselves that is held in personal health data filing systems for therapeutic purposes. Such data also includes audio and video recordings and X-rays, etc.

Upon request, healthcare professionals shall provide explanations of specialist terms, etc. Provision shall be made to enable Sami-speaking and foreign language-speaking persons and persons with disabilities 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 limited independent right of access, as they have the right to be consulted and may restrict or deny access by their parents or legal guardians. Children under 12 years of age have no right of access, but their parents or legal guardians have right of access on behalf of the child.

Patients may be denied access to information in all or parts of a personal health data filing system for therapeutic purposes if this is absolutely necessary in order to prevent risk to life or endanger the life or physical safety harm to the patient, or if access is patently inadvisable out of consideration for persons close to the individual concerned. Compelling reasons must exist 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.

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

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

Correction shall be performed by re-entering data or by the addition of a dated correction. Correction shall not be made by erasing information.

If information is inaccurate or misleading and is consequently perceived as burdensome by the person concerned, or is obviously not necessary in order to provide healthcare, a patient may request erasure of the information.

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 healthcare professional who signed the information, correction or erasure may be carried out by a healthcare professional designated by the controller.

Information recorded under the wrong person shall be erased unless compelling reasons in the public interest exist for why erasure should not be carried out.

For more information, see Directorate of Health circular concerning the Health Personnel Act

The controller shall notify any recipient of personal data that is subsequently corrected or erased of such correction or erasure. The controller shall notify the data subject of the identity of such recipients if the data subject so requests.

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

The controller should issue 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 data release and disclosure

The patient or service user has the right to object to the release or disclosure of data. This may apply to the transfer or release of data to patients themselves, to legal guardians and/or to healthcare professionals. The organisation shall have 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 service user would object if asked.

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

Patients and service users cannot object to statutory transfer of data. This also applies to the statutory transfer of data to national registries.

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

The identities of anyone to whom data has been disclosed and the organisation they are affiliated to shall always be documented.

4.2.5.2 Release and disclosure of health data between organisations for the purpose of healthcare provision

Unless the patient or service user objects, healthcare professionals shall grant collaborating professionals 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 healthcare institution, patients should be given the opportunity to state who their medical records are to be sent to.

4.2.5.3 To the organisation's management and to administrative systems

When necessary in order to provide healthcare, or for internal audit or quality control of services, a healthcare provider may disclose the data to the organisation's management. The data must be necessary and relevant for the purpose.

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

Healthcare professionals shall provide the patient's national ID number and data concerning diagnosis, 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 be disclosed for education and quality assurance purposes for the benefit of healthcare professionals who have previously provided healthcare to the patient on a specific treatment pathway, but who will not be involved in the provision of any further health and care services. This disclosure is permissible only if the patient does not object. This would, inter alia, include situations where ambulance workers have transported a patient to hospital, or medical staff have treated a patient in a hospital accident & emergency department, or nursing home staff have assisted in the hospitalisation of a resident. By obtaining the data, the treatment provider can assess whether the investigations, assessments and treatment that were carried out were appropriate (see Section 29c of the Health Personnel Act).

Disclosure of data shall be limited to data that is necessary and warranted for the purpose. The patient's medical record shall state which data has been disclosed and to whom it has been disclosed.

4.2.6 Storage of personal health data

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

4.2.6.1 Retention period when providing healthcare

Health data shall be retained until it is no longer deemed necessary to retain given the nature of the healthcare involved. The same applies to data concerning who has gained access to or received health data linked to the national ID number of the patient or service user concerned (logs).

If the information is not to be retained in accordance with the Archive Act, the Health Archive Act or other legislation, it shall be erased.

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

When paper documents have been digitalised appropriately, hard-copy originals may then be destroyed. 'Digitalised appropriately' means that all text is legible, and that all scanned text, pages, images and figures are accurately rendered. Electronic personal health data filing systems for therapeutic purposes shall reflect the original record.

4.2.6.3 Personal health data filing systems upon termination and transfer of activity, etc.

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

Patients/service users have the right to object to the transfer of their medical records, and to have such records transferred to another specified organisation.

Data that is not to be transferred to a specific healthcare professional or to a specific organisation, and which the original organisation is not required to safeguard, may be submitted to an official archive, placed with another storage facility or transferred to the county governor's office. Data transferred to the county governor's office is retained for ten years and may then be destroyed following consultation with the Director General of the National Archives of Norway or submitted to an official archive.

4.3 Data protection by design and by default

Data protection by design and by default is a key requirement of the GDPR. Health sector organisations, through both their controller and their suppliers, shall require and address data protection in all phases of system or solution development. Organisations shall ensure that information systems adhere to data protection principles (see section 2.2) and that they safeguard the rights of data subjects.

Controllers shall select suppliers capable of providing services that fulfil statutory requirements and the requirements of this 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 identify appropriate measures in order to fulfil the requirements.

5 Information security

This chapter describes key security measures to ensure the protection of personal health data and provides an overview of the measures required to achieve an adequate level of security. Security measures shall be assessed and implemented on the basis of risk assessments.

Most of the security requirements in Chapter 5 also apply to the processing of personal health data for purposes other than the provision of health and care services. On the basis of a risk assessment, organisations shall determine which security measures are necessary and whether it is necessary to implement more comprehensive measures than those described in this chapter.

5.1 Security measures for employees

5.1.1 Terms and conditions

All employees in the organisation shall undergo continuous in-service training on the fulfilment of requirements regarding the duty of confidentiality, information security and data protection. This should be stipulated in the employment contract or otherwise agreed in writing.

The organisation should obtain a declaration of confidentiality from each employee.

The organisation should draw up an information security and privacy policy that covers the essential requirements.

The organisation shall establish policies on personal use of information systems and devices.

5.1.2 Training and expertise

Organisations shall ensure that staff who are granted access to the organisation’s data and/or systems possess sufficient expertise and have been familiarised with relevant security measures.

Training shall take place on a continuous basis and be adapted to the various roles and user categories. Follow-up should be carried out to ensure that the training measures have the desired effect. Completed training and assessment of effects should be documented. New training initiatives shall be considered in the event of changes in technologies or procedures.

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

5.1.3 Termination of employment

Upon termination of employment, all media (including digital, paper, etc.) that may contain health and/or personal data shall be returned. Access passes shall be returned and deactivated. All access to the organisation's network and information systems shall be blocked to ensure that the former employee, supplier or contractor concerned no longer has access.
The organisation shall have procedures in place for clearing out any information that an employee has stored in their own user account.

The organisation should implement measures to make the employee aware that the duty of confidentiality continues after the termination of their employment.

5.2 Access control

Access control covers how the organisation implements:

- authorisation for access to information systems;
- authorisation for access to personal health data filing systems for therapeutic purposes, which entails granting permissions to read, record, edit, correct, erase or block personal health data;
- authentication to ensure identification of authorised users;
- disclosure to authorised employees of personal health data concerning specific patients/service users;
- disclosure of personal health data to personnel other than the organisation's own staff; and
- control measures.

Health sector organisations shall have procedures in place for authorisation, alteration and termination of access. Within the constraints of the duty of confidentiality, organisations shall ensure that relevant and necessary health data is available to healthcare employees and collaborating workers as and when necessary, in order to provide, administer or quality-assure the provision of healthcare to individuals

The organisation decides how the information should be made available. Such data shall be made available by a means that safeguards information security and data protection.

Access control shall be established for all access to network and information systems. This also applies to users with administrator and system rights.
Only authorised employees shall be granted access to personal health data, and only based on official need.

Access to personal health data filing systems for therapeutic purposes shall be granted following a specific decision based on whether measures have been or will be established for medical treatment of the patient. Access shall be controlled to ensure fulfilment of the duty of confidentiality rules and so that access to personal health data is not granted to anyone other than those with an official need to access it.

Organisations shall likewise implement the necessary security measures for employees, suppliers and contract staff who may gain access to the organisation's network and information systems. Measures for access control, user authentication and in-system access management shall ensure appropriate access management for network and information systems.

5.2.1 Authorisation

Organisations are 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 powers to allocate authorisation to the individual unit manager. This entails that managers assess and approve authorisations within their own area of responsibility. Allocated authorisation shall ensure that employees are able to access necessary and relevant personal health data in line with their responsibilities and duties insofar as the statutory duty of confidentiality does not preclude such access. Authorisations shall be reviewed in the event of changes in responsibilities or employment, or long-term absence.

If in-system access management is based on roles, authorisation shall 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 which organisations the authorisation is valid for.

For the authorisation of technical employees with a specific need to access large volumes of personal health data, measures shall be implemented 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 within or external to the organisation are unable to alter data without the identity of the person who made the change, and details of the change, being logged in the information systems.
- All allocations of authorisation shall be recorded in an authorisation audit log (see 5.2.1.1).
- Technical measures shall also ensure that persons within and external to the organisation are unable to alter configurations and software without the changes being logged (see 5.4.4).
- Users with administrator access shall use a personal separate user account for administrator tasks. Systems administrators 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 audit logs

The organisation shall ensure that an authorisation audit log is established. The audit log shall as a minimum contain:

- data on who has been allocated authorisation;

- data on the role to which the authorisation has been allocated (whether the role is used in the organisation);
- the purpose of the authorisation;
- time of allocation and, if applicable, revocation of the authorisation;
- data on which organisation the user is affiliated with; and
- authorisation of healthcare professionals for accessing health data in other organisations (only if access to health data in other organisations is practised).

5.2.1.2 Access to personal health data between organisations

Organisations shall monitor and oversee all processing of personal health data processing for which it is responsible, including the disclosure of data to other organisations:

- A risk assessment must be carried out when implementing or altering data disclosure to other organisations.
- Controllers and organisations granted access to data held by the controller shall clarify, by formal agreement or otherwise, how:
    - user authentication will be affected by secure means (e.g. two- or multifactor authentication);
    - access to health data held by the controller will be authorised; and
    - logging and control of logs will be performed.

5.2.2 Authentication

Authentication shall as a minimum fulfil the following:

- Access to network and information systems, for both standard users and administrators, shall be secured by means of user authentication that provides adequate protection. Persons granted access shall confirm their identity in a secure manner. What is considered a secure authentication method shall be assessed and determined based on a risk assessment.
- Different employment relationships shall be identified.
- No more than one person shall use the same authentication criteria.
- Allocation of user credentials for authentication criteria (e.g. passwords) shall be carried out in an appropriate manner.
- Access from home offices or mobile devices (and mobile networks) shall be secured by a robust authentication solution (e.g. two- or multifactor authentication)
- This also applies to locations that communicate via lines over which the organisation has no physical control.
- All default passwords (factory settings) on systems and equipment shall be changed before processing of personal health data commences.
- When using wireless networks for processing personal health data, authorised users shall be authenticated by means of a secure authentication solution.

If roles are used, different roles shall be identified and, if necessary, new authentication shall be allocated.

5.2.3 Access control audits

The organisation's management shall ensure that regular management and monitoring is performed of who has electronic access to using the organisation's network and information systems. Review and audit of access management, including access authorisations, shall be performed by the individual manager:

- in the event of organisational changes, staff transfers to another unit/department or a change in responsibilities;
- at least annually (ideally in connection with a security audit); and
- in the event of a security breach for what has been affected by the breach.

If an audit results in a suspicion that unauthorised access has occurred, the organisation's management shall be notified. Any such incident shall otherwise be dealt with in accordance with established procedures for managing non-conformities, particularly with a view to clarifying whether existing access controls are satisfactory. Any misuse of self-authorisation shall be followed up as a non-conformity. If audit reveals that unauthorised access has occurred, this must be treated as a non-conformity.

If health data is accessed across organisations, the contract parties shall coordinate their access management. Any controller with powers to authorise healthcare professionals for access shall continuously monitor:

- who within the controller's own organisation has retrieved health data electronically from another organisation;
- the grounds for such retrieval; and
- the time frame within which the health data has been retrieved.

If this monitoring reveals that health data has been wrongfully retrieved, the organisation from which the data was retrieved and the patient/service user that the data concerns shall be notified. Such incidents shall be dealt with in accordance with established procedures for non-conformity management.

5.3 Physical security and management of equipment

5.3.1 Keys/access cards

A procedure shall be established for 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 achieved by access control at 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 the organisation's infrastructure, network systems and information systems.
Procedures, policies and physical security measures shall be established to maintain appropriate security for network and information systems.

Physical security measures shall as a minimum include:

- Measures to prevent unauthorised access to sites, physical and technical infrastructure which network and information systems use or depend on.
- Measures to identify and protect buildings, rooms and adjacent premises and areas that are important for the security level of network and information systems.
- Measures to safeguard external dependencies, including data communication and power supply.

All storage media shall be securely erased when they are decommissioned. This also applies to health data and data that is no longer needed for the purpose for which it was collected. The duty to retain and archive personal health data shall always be fulfilled in accordance with healthcare legislation and the provisions of the Archives Act.

5.3.4 Mobile devices, home offices and remote working

A risk assessment shall be carried out before mobile devices, home offices and other remote working arrangements are implemented, and in the event of changes that could impact information security. Procedures and policies shall be established for remote working, e.g. home offices and mobile remote working from different premises and geographical locations. Likewise, when employees, suppliers and hired personnel perform remote work, security measures shall be implemented to protect information, network and information systems, products and services that are processed or stored outside the organisation's premises.

Personal health data shall only be stored locally on devices when necessary based on official need, and shall always be stored encrypted.

5.3.5 Encryption

Technical measures shall be defined and established so that all transmission of personal health data outside the organisation's control is encrypted. Encryption and decryption between communication points in the infrastructure shall be performed using approved equipment over which the organisation has control. This control may be exercised by agreement.

All communication, whether wireless or wired, shall be secured by means of encryption.

See for example the Norwegian National Security Authority (NSM) document "NSM Cryptographic recommendations Version 1.0"
(www.nsm.no)

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

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

5.3.6 Medical devices and welfare technology

Medical devices and welfare technology that process personal health data shall be comprised by the organisation's information security and data protection activities, including in risk assessments, access management, change control and procedures for use, in the same way as for other information systems.

5.4 Secure IT operations

5.4.1 Configuration control

Organisations are expected to maintain an overview of data flows, data communication and integrations, and control over all their own hardware 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 hardware and software only perform functions specific to the intended purpose
- Organisations shall ensure that all data flows, data communication and integrations are mapped and documented.
- Only approved devices and software shall be used for processing personal health data. Organisations shall determine who has approval authority.
- Hardware and software shall be updated so that state-of-the-art 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 organisation's change management procedures (see section 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 occurring during development and testing.
- The configuration of equipment and software shall be regularly checked to ensure that it 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 hardware or software, shall not be operationalised until the following measures have been effected:

- risk assessment showing that the risk is acceptable;
- testing to verify that expected functions are provided;
- implementation that provides protection against unforeseen events;
- new configuration has been documented; and
- configuration changes have been approved by the organisation's manager or the person so authorised by the management.

Configuration control shall be regulated by a formal agreement concerning:

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

5.4.2 Change management

Formal responsibility for all changes affecting information security in the organisation, network and information systems and infrastructure shall be vested in the relevant management level.

The organisation shall detail procedures for change management, which shall cover the following topics:

- identification of major 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 (DPIA);
- approval procedures for changes;
- communication of schedules to relevant individuals/roles;
- backup procedures if the change has to be cancelled or fails or if incidents occur;
- change log containing relevant information;
- training of users/roles affected by the change; and
- ensure that network and information systems are continuously enhanced, including that updates are quality-assured, installed and tested on an ongoing basis.

5.4.3 Back-up

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

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

Regular tests shall be performed 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 of network and information systems and infrastructure.
- Configuration and software changes.
- Security-relevant incidents in security barriers.
- Attempted unauthorised use of network and information systems and infrastructure.
- Use of self-authorisation.

As a minimum, the following shall be recorded in logs of authorised use of personal health data filing systems for therapeutic purposes:

- the identity of the person who has read, corrected, entered, modified or deleted personal health data;
- organisational affiliation;
- the basis for data disclosure; and
- the times and dates of disclosure.

For personal health data processed for purposes other than the provision of health and care services, logging requirements shall be informed by a risk assessment.

Consideration should be given to logging the following, over and above the minimum requirements:

- the role of the authorised user at the time of access;
- organisational affiliation;
- the type of data for which access has been authorised; and
- the name of the individual to whom disclosure was made of health data linked to the patient's or service user's name or national ID number.

The logs shall be readily analysed using analysis tools with the aim of detecting breaches.

Procedures shall be established for log analysis, so that any incidents are detected before they have serious consequences. If any breach is detected, it shall be managed as a non-conformity.

There shall be procedures in place to, when necessary, cross-check the logs against the authorization register.

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

Logs shall be correctly time-stamped.

Logs generated in connection with the provision of healthcare shall be stored until they are assumed to no longer be needed.

Logs with relevance for security should be retained for as long as necessary in order to achieve their purpose.

5.4.5 Management of technical vulnerabilities

Management of technical vulnerabilities shall follow the procedures for change management. The organisation shall have a procedure for obtaining information about technical vulnerabilities in network and information systems, equipment and software.

Management shall be based on an overview of:

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

Procedures and operational measures shall be established to address:

- responsibility for monitoring, risk assessment, rectification and coordination;
- responsibility for security monitoring of network and information systems to detect incidents;
- how the organisation should respond to and notify vulnerabilities;
- prioritisation and establishment of timeline for correction; and
- all corrections should be tested before they are implemented.

5.4.6 Security audits

The organisation's management shall verify that security is being safeguarded by means of regular and at least annual safety audits. The purpose of security audits is to carry out control activities and quality assurance of established measures and procedures. An approved plan for security audits shall be established.

In order to conduct adequate security audits in organisations, the assessments should as a minimum comprise:

- Delegation of responsibility and organisation of security tasks.
- Adherence to procedures concerning use of network and information systems and the processing of personal health data.
- Assessment of the effectiveness of the security measures
- Access to personal health data and measures to deter unauthorised access
- Training and expertise in data protection and information security
- Review of documentation on information security within communications partner, processor and supplier organisations

Outcomes, conclusions and non-conformities from security audits shall be documented and addressed by the organisation.

5.5 Communication security

5.5.1 Information security management in network and information systems

Information security in network and information systems is a pivotal measure in safeguarding the processing of personal health data.

Organisations shall clearly define the security requirements that apply to network and information systems. The measures that are established shall be based on a risk assessment and include technological security measures adapted to the scale, complexity, operating environment, user environment, function and risk exposure of an organisation's network and information systems.

The security measures for network and information systems shall as a minimum include:

- use of two- or multifactor authentication to secure access for both users and administrators;
- access management based on official need to protect the content of network and information systems;
- control over who has access to the organisation's network and information systems;
- segmentation of services based on the principle of least privilege (PoLP);
- measures to ensure that systems can withstand interruptions and recover rapidly without significant reduction in service quality;
- capacity management to withstand congestion and equipment failure;
- continuous enhancement and quality assurance of updates, including installation and testing; and
- monitoring of network and information systems to detect security incidents

5.5.2 Connection to external networks

When connecting to external networks, technical measures shall be put in place to ensure that only explicitly permitted traffic can pass from the outside in or vice versa, and that other traffic is stopped.

This measure shall include at least two independent technical measures to reduce the risk of external persons gaining unauthorised access to, or being able to alter or erase, personal health data.

5.5.3 Online interaction

The reference directory for e-health, pursuant to the regulation on ICT standards and national eHealth solutions (*forskrift om standarder og nasjonale e-helseløsninger*), provides an overview of mandatory and recommended standards for the health and care services. This regulation is intended to support health and care service providers in adopting ICT standards for promoting secure electronic (online) interaction.

Below is a description of the requirements for interaction that are not presented elsewhere in the Code.

5.5.3.1 Requirements for electronic interaction

Clear lines of responsibility shall be established between senders, recipients and any intermediary service, and the responsibilities shall be defined in agreements between the organisations and intermediaries. All agreements shall be in writing.

The sender/tendering organisation shall be responsible for:

- its own connection security which prevents accidental disclosure and intrusion;
- ensuring that the service cannot propagate software containing malware and the like; and
- secure end-to-end transmission encryption.

The recipient/user organisation shall be responsible for:

- ensuring that the service cannot be used to distribute malware, etc.;
- its own connection security which prevents accidental disclosure and intrusion; and
- ensuring end-to-end transmission encryption.

5.5.3.2 Requirements regarding message exchange based on the ebXML framework

The sender is responsible for:

- correct addressing of electronic interaction messages in accordance with the address register (NHN.no);
- ensuring that, as and when necessary, messages are signed in such a way that the organisation 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;
- non-conformity reporting in the event of errors, i.e. receipt of a message that is not addressed to the organisation; and
- ensuring that messages are received in the agreed format.

The communication intermediary is 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;
- 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 for all of the above.

5.5.3.3 Real-time data sharing

Interaction by means of data sharing enables more dynamic sharing of information for citizens and stakeholders in the healthcare sector. This type of data sharing may involve a stakeholder requesting or updating information from another stakeholder via a data sharing interface.

The following security principles apply to data sharing:

- There must be secure user authentication that is trusted by the organisations hosting data sharing interfaces.
- An organisation requesting 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 privileges 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 organisation hosting it.
- Common components for authentication of the consumer shall be used where available and appropriate.
- Common components for authentication of the consumer shall be used where available and appropriate.

5.5.4 Email and SMS text messages

The organisation shall establish measures to prevent personal health data and other information of importance to information security from being disclosed through the use of unencrypted email and SMS text messages or other non-secure channels.

Any organisation that uses unencrypted channels shall:

- ensure, by means of technical and organisational measures, that email does not contain identifiable personal health data;
- establish logging to verify that rules are not violated (rule violations shall be treated as non-conformities);
- assess whether the combined information in a text message or email message could result in a breach of the duty of confidentiality.

5.5.5 Connection to the internet

Technical equipment, e.g. medical devices or applications that connect to the internet, shall be included in the organisation’s efforts to safeguard information security and data, including in risk assessments, access control and procedures for use.

Organisations shall establish:

- technical measures to help prevent accidental disclosure and unauthorised access to personal health data;
- logging to verify that rules are not violated. Rule violations shall be treated as non-conformities.

5.6 Digital communication to data subjects

In this section, 'digital communication' refers to messages sent by organisations to data subjects in connection with healthcare provision.

Organisations 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/service user is not dependent on storing the data on their own devices in order to familiarise themselves with the data;
- ensure that procedures are established so that messages to patients are not intrusive and do not violate privacy, while at the same time providing the patient with sufficient information; and
- implement sufficient measures to ensure that messages are sent to the correct recipient. To ensure that the correct contact details are used for recipients, organisations with access to the Common Contact Register (digdir.no) should use this.

5.7 Supplier relationships

Controllers have overarching responsibility for fulfilling statutory requirements and requirements in this Code. Suppliers shall aid controller fulfilment of these requirements through the use of supplier infrastructure, products and services. This means that suppliers shall implement the necessary procedures and security measures to ensure compliance with the requirements of the Code.

Controllers shall have guidelines for administering supplier agreements and an up-to-date list of such agreements at all times. Supplier agreements shall be regularly evaluated and revised to ensure that information security requirements are being met.

5.7.1 Requirements regarding supplier confidentiality

Suppliers may process personal health data by doing so on behalf of a controller, through outsourcing, or through the provision of maintenance services, for example, which entail that supplier employees may be exposed to confidential information. Suppliers shall ensure that they have procedures in place that impose a duty of confidentiality on all employees concerning personal health data and other confidential information.

Suppliers are permitted to administer and store non-disclosure agreements for their own employees, but controllers shall be given access to these as and when needed.

5.7.2 General considerations regarding supplier agreements and supplier monitoring

Controllers are responsible for ensuring that information security and data protection requirements 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 met in order for a controller to fulfil its responsibilities shall be agreed in writing with suppliers. The requirements of the Code applicable to suppliers under an agreement will depend on the type of supplier service provided, such as:

- data processing, in the form of cloud services or systems administration;
- maintenance, such as physical services or remote access; or
- supply of solutions and systems.

The agreements shall include pledges by the parties to comply with relevant requirements, including required measures, in accordance with the version of this Code in force at any time, as well as rules on sanctions for any breach of the Code, applicable legislation and the supplier agreement in general.

Through supplier agreements, organisations shall ensure that their suppliers have management systems in place for information security and data protection that comprise security audits and non-conformity management. Organisations shall ensure that suppliers and other parties who perform services that could impact the security of network and information systems perform those services in compliance with the organisation's information security requirements.

Organisations shall require security measures from suppliers with the potential to impact network and information systems to the extent necessary for maintaining an appropriate level of security.

5.7.3 Outsourcing of services

Where ICT functions or other functions pertinent to information security or data protection are outsourced, the supplier agreement shall as a minimum include the following provisos for information security and data protection:

- A documented risk assessment demonstrating that the outsourcing organisation's acceptance criteria and the level of security set out in the Code have been implemented. When outsourcing ICT services to other countries, conditions in the host country should be examined because they may impact the risk assessment.
- Which tasks with security implications are covered by the agreement, and who has responsibility for them.
- A description of the supplier's solution and interface with the organisation in the form of a configuration map.

The agreement shall ensure that the organisation 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 organisation shall ensure that it has a robust plan for safeguarding information security and data protection upon expiry of the supply agreement. Upon termination of the

agreement, the supplier shall have issued a signed declaration to the organisation that all data proprietary to the organisation has been returned or erased by the agreed date.

5.7.4 Processors

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

A controller may only use processors who provide adequate guarantees that they will implement the necessary security measures to ensure that their processing meets the requirements of the Personal Data Act. 'Adequate guarantees' mean that the processor meets any regulatory requirements and the requirements of the Code applicable to the contractual relationship concerned.

5.7.4.1 Subcontractors to processors

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

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

Subcontractors and others who perform services for or on behalf of an organisation and who may gain access to that organisation's network and information systems have an independent responsibility to comply with information security and data protection requirements. 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 formalised in an agreement between the processor and subcontractor. The agreement shall be made available to the controller upon request.

5.7.4.2 Scope of data processing agreements

A data processing agreement can be either an independent agreement between the parties or an integral part of another contract. Data processing agreements shall be established in writing.

The content of a data processing agreement is regulated by Article 28, GDPR Processor (www.lovdata.no). For more information on the use of processors, see Code Factsheet 10 on use of processors.

The processor's independent responsibility for information security and for addressing data protection for data subjects shall be set out in detail.

The agreement shall state that the processor undertakes to comply with statutory requirements, as well as to applicable requirements in the Code.

5.7.4.3 Processor's overview of processing operations

Processors shall maintain an overview (record) of all categories of processing activities carried out on behalf of a controller.

For further details, see Code Factsheet 13.

The controller shall ensure that the processor receives the necessary information to enable the processor to maintain such a record.

5.7.4.4 Other obligations on the part of processors

If a processor processes personal health data from multiple organisations, the processor shall employ technical measures that cannot be overridden by the controller's users to ensure that barriers are established between those organisations in accordance with a completed risk assessment.

The processor shall notify the controller without undue delay of any non-conformity. The processor shall assist the controller in meeting the 72-hour deadline for notifying any personal data breach 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 organisation shall, through agreements, ensure that:

- the supplier's equipment used for an online connection via a communication network, or portable devices connected to the organisation's equipment, is free from malware containing viruses, etc. and that the equipment is protected against access by unauthorised parties;
- all logical and physical access has been authorised by the organisation; and access is logged and controlled; and
- the availability of personal health data is maintained as far as possible when the supplier carries out work on the organisation's hardware/software.

5.7.6 System suppliers

Organisations in the health and care services sector intending to use information systems that process personal health data shall require privacy by design in the solutions.

To enable organisations to fulfil their responsibilities as a controller, the information systems shall incorporate features compliant with statutory requirements and applicable requirements in the Code[3].

See also Code requirements in relation to public procurement requirements, requirements in ISO 27001 and controls in ISO27002 (Appendix to the Code).

[3] See the Appendix "Overview of the Code's requirements".

5.7.7 Supplier monitoring

Information security and data protection in the context of 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 organisation shall ensure:

- clarity regarding responsibilities and roles;
- that information security and data protection specialists are involved in procurements and supplier management; and
- that the organisation's management (and board of directors where relevant) is ordinarily involved in decisions regarding the use of private sector suppliers and outsourcing of large-scale services.

Requirements and necessary security measures when using suppliers shall be based on a comprehensive risk assessment. The risk assessment shall always consider scenarios involving the supplier's authorised and, potentially, 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 procurement expertise at its disposal.

5.7.8 Transfer of data outside Norway

Organisations that transfer personal data abroad shall ensure that the level of protection required by the Norwegian Personal Data Act is not undermined by such transfers.

All EU/EEA Member States have implemented the GDPR, thus ensuring that personal data is processed securely. In addition, the European Commission has recognised that certain third countries[4] provide an adequate level of personal data protection. Personal data can therefore be freely transferred to those third countries. However, this requires that the other conditions of the Norwegian Personal Data Act are met. See section 5.7.5, particularly the requirements regarding risk assessments and country risk assessments.

See also Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection (commission.europa.eu).

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 data is subject to the same level of protection as in the EU/EEA. If an organisation transfers personal data to third countries (i.e. outside the EU/EEA), it must base this on one of the grounds for transfer stipulated in the GDPR.

See also (the Norwegian Data Protection Authority's guidance on data transfer to third countries at www.datatilsynet.no)

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

When transferring data to third countries, organisations shall ensure that they have sufficient expertise (e.g. legal expertise) at their disposal to ensure their regulatory compliance.

5.7.9 Cloud services

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

Key requirements to be met:

- The division of responsibilities between the controller and processor has been clarified and adapted to the delivery model used.
- The controller has an overview of where data is processed geographically, so that the requirements of section 5.7.8 can be met.
- The controller shall verify that the cloud provider's standard agreements, if any, are not in breach of applicable statutory requirements and the requirements of the Code,
- The controller has established a robust plan for safeguarding information security and data protection upon termination of the cloud service agreement

5.8 Management of information security breaches

5.8.1 Non-conformity management

Incidents such as breaches of procedures, data protection, information security or network and information systems) shall be treated as non-conformities. Non-conformities shall be dealt with in order to restore normal conditions, remove the cause of the non-conformity, and prevent recurrence.

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

The organisation shall gather factual information concerning the sequence of events to enable corrective action to be taken. The effects of corrective actions shall be assessed and any other measures implemented as and when necessary.

In the event of serious or recurrent 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 reporting of non-conformities relating to data protection and information security to the Norwegian Data Protection Authority, the Norwegian Board of Health Supervision and the Norwegian National Security Authority (NSM).

5.8.2 Breach of personal data security

Personal data breaches are non-conformities that result in unintended or unlawful destruction, loss, alteration, unlawful disclosure 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 notified to the Norwegian Data Protection Authority within 72 hours, unless the breach is unlikely to pose a risk to the rights and freedoms of natural persons.

For detailed rules, exceptions from the reporting obligation and reporting procedure, see https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/ (in Norwegian)

5.8.2.2 Notification of data subjects

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

As a minimum, the organisation shall provide the data subject with the following information:

- Description of the breach
- Name and contact details of 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 measures that the organisation has taken or proposes to take to address the breach, including (where relevant) actions to mitigate any harmful effects of the breach

The organisation should, as far as possible, contact the data subject directly.

5.8.3 Notification to the Norwegian Board of Health Supervision

Organisations that provide health and care services shall notify the Norwegian Board of Health Supervision of non-conformities resulting from errors and non-conformities in information systems. The duty to notify is triggered:

- in the event of death or severe harm to a patient or service user;
- as a result of the provision of health and care services; and
- when the outcome is unexpected based on foreseeable risk.

In the event of such incidents, the organisation shall:

- follow up and inform patients and next of kin;
- review the incident; and
- identify and implement risk mitigation measures.

For detailed rules and reporting procedure, see https://www.helsetilsynet.no/tilsyn/varsel-om-alvorlige-hendelser/oversikt/ (in Norwegian)

5.8.4 Notification to the National Security Authority

The Norwegian National Security Authority (NSM) is the designated single point of contact (SPOC) for security in networks and information systems in Norway. Organisations that provide essential services and digital services shall notify the NSM within 24 hours of any non-conformity resulting from an adverse impact on the security of network and information systems. The notification shall contain the following information:

- name and contact details of the essential service provider
- the affected service
- description of the incident, including possible causes and consequences
- number of users affected
- the impact of the incident in other countries

Necessary documentation and information shall be made available to the NSM. The information in the notification shall be updated within 72 hours.

Within one month of the original notification being submitted, the organisation shall submit an incident report to the notification recipient. The report shall contain updated information about the incident and detail actions that have been taken to manage the incident.

The notification recipient may require status updates and other information in order to perform their tasks.

For definitions of network and information systems and security in network and information systems; see Chapter 6 Appendices and section 6.2 Appendices to the Code.

5.9 Emergency preparedness

The organisation shall establish and implement security measures for maintaining continuity and resilience following an incident. This includes the ability to prevent, detect, manage and restore normal conditions following physical or technical incidents that may impact information security and personal data protection.

The non-availability of network and information systems, services and solutions could harm the organisation, its authorised users, patients/service users in the provision of healthcare, and data subjects. Organisations shall ensure that essential personal health data is available.

Organisations shall prepare, maintain and document emergency preparedness plans for responding to different types of incidents and alerts. Regular security exercises shall be carried out to test the emergency preparedness plan and incident response. The emergency preparedness plans shall be drawn up on the basis of the Norwegian Government's national emergency preparedness principles (https://www.regjeringen.no) and describe the organisation and supervision of emergency preparedness, as well as the emergency measures to be implemented in the event of different incident categories. The objective is to minimise the consequences of such incidents and ensure stable operation of network and

information systems and services. Where relevant, security exercises should be carried out jointly with subcontractors or other parties who perform work for or on behalf of the organisation.

When establishing emergency preparedness plans, organisations shall map the consequences of severe disruption to all or parts of the organisation. This shall be assessed for the organisation itself, its suppliers, subcontractors and for authorised users. Systems shall be classified by priority based on the consequences of service disruption, from critical to acceptable. The classification shall include the mapping of dependencies and determination of acceptable risk to availability.

Other information systems and infrastructures on which the classified information systems are dependent shall also be mapped and documented. These shall be assigned the same classification and security level as the classified information systems.
For each classification, management shall determine the acceptable level of risk to availability and determine the maximum downtime permissible.

Based on the classification, organisations shall establish emergency preparedness plans based on alternative operation without the use of the information systems and alternative operation with partial support from the information systems. The emergency preparedness plans shall be drilled, tested, revised and updated at least once a year.

6 Appendices

6.1 “Overview of requirements set out in the Code”

The Appendix “Overview of requirements set out in the Code” contains all “shall” requirements in the Code as an aid to verification of whether an organisation is Code-compliant. In addition, this Appendix includes an overview of applicable regulatory requirements and is aligned with the international standards ISO 27001:2023 and ISO 27002:2022.

Health sector organisations may use the overview in their work to establish management systems for information security and data protection, and establish and maintain internal control and information security measures to ensure they are compliant with applicable regulatory requirements.

6.2 Definitions

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

-A-

“**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 an organisation of an incident occurring that could potentially result in a breach of the applicable requirements for confidentiality, integrity and availability/resilience in a specific instance. The level of risk will depend on the probability of an incident occurring and the consequences of such an incident. Each individual organisation shall make 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 magnitudes within given constraints, or levels describing what scale of risk is acceptable.

“**Access**” means, for the purposes of this Code, that personal health data concerning one or more specific patients/service users is available 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 healthcare to the patient. Access to specialised systems in connection with the provision of services to patients/service users shall be established based on official need. Access for the

purpose of 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 available at the time and place it is needed.

"**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).

"**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.
"**Appropriate level of security**" means the level of security achieved by implementing appropriate security measures (technical, organisational, physical and personnel-related). The nature of measures considered appropriate will depend on the risk, taking into account state-of-the-art in technology, implementation costs, and the nature, scope, purpose and context of processing. The appropriate level of security must ensure the confidentiality, integrity, availability and resilience of the information systems proportionately, where great emphasis is placed on the risk to the patient/user and the provision of a high standard of healthcare.

-C-

"(The) Code" means this document. Other documents relating to the Code, such as factsheets and guidelines, are not covered by the term.

"**Controller**" means, for the purposes of this Code, the natural or legal person, public authority, agency or other body which, either alone or jointly with others, determines the purposes and means of the processing of personal data. If the Norwegian term "data" is not specified in the context of "control" in a Norwegian statute or its appurtenant regulations; see Section 2(e) of the Personal Health Data Filing System Act, Section 2(e) of the Patient Records Act and Article 4 in the Norwegian language version of the GDPR, then a different Norwegian term for "controller" is used: "behandlingsansvarlig" (literally: 'responsible for processing'). It should be noted that organisations have controller responsibility as regards the processing of personal health data. This responsibility shall be fulfilled by the general management of the organisation, and the organisation is the party that is subject to the relevant statutory duty.

"**Consent**" means, for the purposes of this Code, any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, through a statement or clear affirmative action, signifies his or her consent to the processing of personal data relating to him or her.

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

"**Configuration**" means, for the purposes of this Code, an information system's design, and includes both hardware and software.

"**Configuration change**" means, for the purposes of this Code, a change in the design of an information system as a result of the installation, upgrading or removal of hardware or software.

-D-

"**Data protection impact assessment (DPIA)"** means, for the purposes of this Code, a systematic process to identify and evaluate potential impacts on privacy and data protection from the point of view of all stakeholders in a project, initiative, envisaged system or a process.

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

"**Data protection officer (DPO)"** means, for the purposes of this Code, a designated contact person for data protection and information security internally vis-à-vis the controller (the organisation's management) and employees, and externally vis-à-vis the Norwegian Data Protection Authority and data subjects (patients, clinical trial subjects and in-house employees).
"**Duty of confidentialit**y" 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 Sections 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 of non-disclosure 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 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-

“**Healthcare**” means, for the purposes of this Code, services which are preventive, diagnostic, health-preserving, rehabilitation or care purposes, and which are provided by healthcare professionals.
“**Personal health data**” is, for the purposes of this Code, a collective term for health data or personal data within the scope of the Code.

“**Health data**” means, for the purposes of this Code, personal data concerning a natural person’s physical or mental health, including data on the provision of healthcare, which provides information on an individual’s health status; see Article 4(15), GDPR.

“**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, in a hotel room, etc. or the like). 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 included in the definition of a home office.

-I-

“**Information system**” means, for the purposes of this Code, a system for collecting, storing, processing, transmitting and presenting information. Examples of information systems in the health and care service: record and documentation systems, archiving systems, personal health data filing systems for therapeutic purposes, email, security systems, network operating systems, database systems, storage systems, backup systems, infrastructure, medical support systems, medical device and laboratory systems.

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

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

“I**nternal control**” means, for the purposes of this Code, planned and systematic actions intended to ensure that the activities of the organisation are planned, organised, executed and maintained in accordance with requirements laid down in, or pursuant to, legislation.

“**Incident**” means any event having an adverse impact on the security of network and information systems.

“**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 events or incidents and activities in an information system are recorded; see the next definition.

"**Logging**" means, for the purposes of this Code, the recording of events in an information system with the aim of, for example, preventing, detecting and deterring (recurrence of) information security breaches.

-M-

"**Municipality**" means, for the purposes of this Code, a sub-national legal entity taking the form of a municipal or local authority and county council.

-N-

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

Network and information systems means:

- the electronic communications networks defined in Section 1-5(2) of the Electronic Communication Act
- any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data
- digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

"**Norsk Helsenett**" means, for the purposes of this Code, Norsk Helsenett SF, the national service provider of e-health solutions responsible for facilitating secure and efficient electronic interactions.

"**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-

"**Organisational measures**" means, for the purposes of this Code, non-technical measures." Examples of such measures include procedures, training and changes in 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, pharmacy chain, medical imaging and radiology service, independent laboratory, university, university college, foundation, etc. or a processor/supplier subject to a contractual obligation to comply with the Code.

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

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

-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; see Section 1-3(a) of the Patients' and Users' Rights Act.

"**Patient safety**" means, for the purposes of this Code, protecting patients against needless harm/injury from 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 such as a name, and ID number, location data, an online identifier or one or more elements which are specific to that natural person's physical, physiological, financial, cultural or social identity.

"**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, organisational and personnel measures.

"**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 on an individual person can be retrieved; see Section 2(d), Personal Health Data Filing System Act.

"**Processor"** means, for the purposes of this Code, a natural or legal person, public authority, agency 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 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 might, for example, be a consent, an authority laid down in law. What constitutes a valid basis for processing is set out in Articles 6 and 9 of the GDPR.

"**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 can be retrieved; see Section 2(d) of the Personal Health Data Filing System Act.

-R-

"**Resilience**" means, for the purposes of this Code, the ability of an organisation and its information systems to restore normal conditions following a physical or technical incident, for example. This is achieved through appropriate technical, organisational, physical and personnel measures which facilitate the prevention, detection, scalability, management 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 GDPR.

"**Recipient**" means, for the purposes of this Code, a natural or legal person, public authority, agency or other body to which personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of that data by those public authorities shall be in compliance with the applicable data protection rules according to the purpose of the processing.

-S-

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

"**Self-authorisation**" means, for the purposes of this Code, authorisation given to healthcare professionals in order to gain access to personal health data, which they do not ordinarily require for providing healthcare.

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

a) racial or ethnic origin, political opinions, religious or philosophical beliefs
b) the fact that an individual has been suspected of, charged with, indicted for, or convicted of a criminal offence
c) an individual's health status (personal health data)

d) an individual's sex life and sexual orientation
e) trade union membership

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

"**Service user**" means, for the purposes of this code, a person who requests or receives services under the Health and Care Services Act that are not healthcare; see Section 1-3(f) of the Patient and User Rights Act.

"Shared components" means open, reusable solutions meeting typical requirements in the field of digitisation, such as sign-in, authentication, logs, etc.

"S**ecurity of network and information systems"** means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.

"**Supplier**" means, for the purposes of this Code, a legal entity which provides technical or administrative services to an organisation. Examples are EPR suppliers, medical imaging service providers, suppliers of solutions for text messaging systems, ICT service providers.

"**Subcontractor**" means, for the purposes of this Code, an organisation that enters into a contract to fulfil some or all of the obligations under a processor's Data Processing Agreement (DPA).

-T-

"**Technical measures**" means, for the purposes of this Code, measures of a technical nature 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 by means of a personal qualified certificate or the configuration of a firewall such that it only permits specific data traffic, or a message service 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, agency or any body other than the data subject, the controller, the processor and persons authorised to process personal data under the direct authority of the controller or the processor.

6.3 Supporting documents

A number of supporting documents in the form of factsheets, guidelines and templates are provided to complement the Code. These materials cover most areas of information security and personal data protection.

The supporting documents are not binding and are to be regarded as guidance documents only. In the event of conflict between the Code and the supporting documents, the Code shall take precedence.

6.3.1 Factsheets

The factsheets offer detailed and practical guidance on how organisations can fulfil certain key requirements in the Code. The factsheets are thematic and 1-4 pages in length.

6.3.2 Guidelines

Guidelines are supporting documents 30-50 pages in length which cover a specialised topic or subsector in detail.

6.3.3 Templates

In conjunction with the factsheets and guidelines, a number of editable templates are provided for use by users in their own organisation.

6.4 References

All Norwegian acts and regulations: https://lovdata.no/

Norwegian Data Protection Authority (DPA): https://www.datatilsynet.no/en/

National Institute of Standards and Technology (NIST), U.S. Department of Commerce: https://www.nist.gov/topics/cybersecurity

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

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

European Union
Website of the NIS2 Directive (Directive (EU) 2022/2555)
Directive - 2022/2555 - EN - EUR-Lex

Website for this Code of Conduct for Information Security and Data Protection in the Health and Care Services Sector : https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

Norwegian Directorate of Health circulars and guidances:
https://www.helsedirektoratet.no/produkter?tema=rundskriv

Requirements specification for PKI (Public Key Infrastructure):
(https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/)

Norwegian National Security Authority (NSM) NSM Cryptographic Recommendations (in Norwegian only): https://www.nsm.stat.no/blogg/kortliste-krav-til-krypto/

NSM Guidance on Crypto Requirements (available in English):
https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

NSM guidance on ICT security, version 1.1: https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/
Framework for authentication and non-repudiation in electronic communication with and in the public sector (in Norwegian only):
https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/

Reference directory for e-health. E-health standards and other documents laying down mandatory requirements pursuant to a regulation or official recommendation :
https://ehelse.no/standarder-kodeverk-og-referansekatalog/referansekatalogen

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

6.5 History of the Code

1st EDITION
Increasingly, work carried out in the Norwegian health and care services sector is based on electronic processing of patient data. More and more communication between organisations is also taking place electronically.

The increasing volume of electronic data processing presents opportunities, but is also posing challenges as regards information security for the organisations involved. Among other things, electronic processing enables data to be made available more readily and faster both internally within an entity and externally outside the organisation. This is an advantage, provided that the information is only made available to the right person at the right time. However, unintended consequences pose a risk to the confidentiality of the information, and special measures must be put in place to ensure that unauthorised persons do not gain access to data that is stored electronically. Mechanisms are needed to provide reassurance 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 health and care services sector compiles its own Code of Conduct for Information

Security. The Code was compiled by representatives of the sector, including representatives of the Norwegian Medical Association, the regional health trusts, the Norwegian Nurses' Organisation, the Norwegian Pharmacy Association and the Norwegian Association of Local Authorities. The Norwegian Data Protection Authority, the Norwegian Board of Health Supervision, the National Insurance Service and the Norwegian Directorate of Health and Social Affairs also participated in the process.

The aim of the Code is to contribute to satisfactory information security in 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 impose a number of other requirements on the management of patient data. These requirements are not covered by this Code.
28 June 2006.

2nd EDITION

In the summer of 2008, the steering committee for the Code decided to incorporate changes in the Code as a result of legislative and regulatory changes and in the interests of promoting electronic interaction between organisations in the sector. Another new feature is that Norsk Helsenett, independent laboratories, the Norwegian Dental Association, the Public Dental Service and the Norwegian Pharmaceutical Association are now represented on the steering committee for the Code. In addition, the Ministry of Health and Care Services and the Agency for Public Management and eGovernment (Difi) have joined the project as observers.

The Norwegian Board of Health Supervision has elected to resign from the steering committee.

In the autumn of 2009, the steering committee decided to extend 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 related to employee privacy should be included in the Code as and where appropriate.

In June 2009, the Norwegian Parliament adopted amendments to the Personal Health Data Filing System Act. This paves the way for regulations on:

- access to 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 professionals in a formalised working partnership

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

2nd EDITION, VERSION 2.1

On 29 November 2012, the steering committee 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.

3rd EDITION

On 5 December 2013, the steering committee for the Code decided to incorporate changes as a result of the regulation on supra-organisational patient records in formalised working partnerships. Additionally, responsibility for the authorisations log in summary care records

was clarified, rules regarding disclosure of personal health data for quality assurance and training purposes were incorporated, and reference is made to the document “Requirements specification for PKI in the public sector” with regard to minimum requirements for encryption strength.

4th EDITION
On 5 June 2014, the steering committee for the Code decided to incorporate changes as a result of the repeal of the Social Services Act of 1991 (LOV-1991-12-13-81). At the same time, the scope of the Code was changed to the health and care services. In addition, the Code was amended to emphasise that it applies to services provided by the Norwegian Labour and Welfare Administration (NAV) linked to the Norsk Helsenett national health network and also applies to municipal services provided by local NAV offices linked to the national health network.

5th EDITION
On 12 February 2015, the steering committee 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.

5th EDITION, VERSION 5.1
On 4 June 2015, the steering committee for the Code decided to amend the wording of the requirements concerning the documentation of measures (section 3.3) in accordance with the requirements of the Freedom of Information Act.

5th EDITION, VERSION 5.2
On 9 June 2016, the steering committee for the Code decided to clarify the text relating to the legislation on joint personal health data filing systems. Certain sentences were also amended to clarify the requirements.

5th EDITION, VERSION 5.3
On 31 May 2018, the steering committee for the Code approved a number of changes which represented the first step towards a major revision and development of the Code.

The EU General Data Protection Regulation (EU) 2016/679 of 27 April 2016 was transposed into Norwegian law though a new Personal Data Act of 2018. This also resulted in certain changes and adjustments in Norwegian health legislation.

The aims of version 5.3 were to ensure that requirements set out in the Code were in line with new legislation, to extend the scope of the Code to cover more data protection and to update the Code by introducing new requirements aligned with technological advances. The Code was given a new structure, and reviewed to ensure that there are no conflicts between the Code and new legislation. Certain articles from the Norwegian version of the GDPR were specifically incorporated:

- Article 30 - Records of processing activities
- Article 32 - Security of processing
- Articles 33 and 34 - Notification and communication of personal data breaches
- Article 35 - Data protection impact assessment
- Articles 24 and 28 - Controller and processor
- Articles 37 and 38 - Data protection officer

6th EDITION, VERSION 6.0
On 4 February 2020, the steering committee for the Code of Conduct approved a major revision of the Code. This version of the Code is the result of a lengthy revision and development process. The main objectives were to ensure that the requirements of the Code

comprehensively reflect the new requirements of the General Data Protection Regulation (GDPR) while being technology-neutral and aligned with current technology. Another important objective was to simplify the wording in order to improve the Code's readability and usability. Among other things, new requirements have been added, text has been deleted and requirements have been clarified or amended. The scope of the Code has been changed, 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 material. Version 6.0 was subject to an extensive consultation process.

EDITION, VERSION 6.1 On 21 November 2022, the steering committee for the Code decided to make changes to how risk is addressed in the Code. The Code switched to using acceptance criteria for risk instead of levels of acceptable risk. Furthermore, the steering committee decided that the Code should use the Norwegian term for "malware" in place of its term for "malicious software". The definition of "personally qualified certificate" was deleted. At the same time, the entire document was reviewed and outdated references were updated.

7th EDITION, VERSION 7.0
Update to incorporate requirements that will be applicable when the Digital Security Act and Digital Security Regulation come into force. The chapter on emergency procedures has been changed to cover emergency preparedness, and requirements for digital preparedness have also been incorporated. Version 7.0 of the Code was approved by the steering committee by email on 25 September 2025.

Visiting address
Norwegian Directorate of Health
Vitaminveien 4,
N-0483 Oslo

Contact
normen@helsedir.no