Code of conduct for information security and data protection in the healthcare and care services sector
Version 5.3

Valid from 20.07.2018
Publication title:
[Code of conduct for information security and data protection in the healthcare and care services sector]

Version number:
[5.3]

Approved by the steering committee:
[31.05.2018]

Published with the support from:
The Norwegian Directorate of eHealth

Contact:
sikkerhetsnormen@ehelse.no

Download the publication here:
www.normen.no
Preface

In order to provide high-quality health and social care services, it is necessary to handle large quantities of data concerning individuals. Much of this data concerns personal and highly sensitive circumstances and is a vital factor in the quality of health and social care services. It is therefore in the interests of both organisations and users to gain access to and protect the data.

Processing data concerning patients and health care users in an appropriate manner is decisive in order to secure trust. The health service is dependent on the trust of patients, health care users, health personnel and the population in general. Patients and health care users must have sufficient confidence in the system to provide the health service with data concerning what are sometimes extremely intimate and personal circumstances. Without this data, we would be unable to provide high-quality health and social care services. Health personnel must be able to trust that the data is accurate and complete in order to provide health and social care services. The sector needs trust in order to digitalise and offer health and social care services in new ways.

Data security is a prerequisite for digitalisation. This means that data must be accurate, updated, complete and accessible. The technology and processing of data which is used by the health service may be subjected to both unintentional and intentional events. The sector must develop and manage robust technology, organisations and a security culture, and have appropriate measures in place to ensure that the system works and also manage and learn from cases where it does not work.

Information security and data protection are key terms as regards the protection of information and technology. Data protection primarily concerns the protection and safeguarding of information based on consideration for the private lives and right of determination regarding personal data. Among other things, this entails ensuring that no more information than is necessary is stored and that everyone has access to their data. Information security is about protecting information based on principles of confidentiality, integrity and availability. The establishment of an adequate level of technical and organisational information security is one of the biggest challenges faced by the health administration and the health and care services with regard to the development of digitalised health and care services.

Regulation (EU) 2016/679 of 27 April 2016 is transposed in Norwegian law through the new Personal Data Act of 2018. This also leads to certain changes and adaptations in the health legislation. Work is currently under way to adapt and develop the Code. The aims are to ensure that the requirements set out in the Code are in accordance with new legislation, to expand the scope of the Code to encompass more data protection and to update the Code with new requirements which take account of technological developments. Version 5.3 of the Code is the first step in this work. This latest version of the Code has a new structure and it has been reviewed to ensure that there are no contradictions between the Code and new legislation and certain articles from the Regulation have been incorporated. The articles which have specifically been incorporated in v5.3 are as follows:

- Art 30 - Records of processing activities
- Art 32 - Security of processing
- Art 33 and 34 - Communication of a personal data breach to the data subject
• Art 35 - Data protection impact assessment
• Art. 24 and 28 - Controller and processor
• Art. 37 and 38 - Data protection officer

In the next version, 6.0, more of the Regulation will be incorporated, including the rights of data subjects.

In version 6.0 of the Code, there will be a clearer differentiation of the requirements with respect to the organisations’ size, complexity and other circumstances which impact on vulnerability and the need for security measures.

For the current version of the Code (5.3), the following guidance for readers is provided for smaller organisations (such as medical centres and physiotherapy practices):

• **Chapter 2 Management and responsibility**
  Sections 2.1 and 2.2 must be read by everyone. It is a pivotal point that the controller is responsible for the processing of personal data within an organisation. For other sections from 2.3 to 2.7, it is recommended that you read these in the light of the introduction to section 2.3 regarding how the management system should be adapted to the organisation.

• **Chapter 3 Risk management**
  The sections up to and including 3.3 must be read by everyone, but it should be noted that the scope of the risk assessments must be adapted to the organisation concerned. The points in section 3.4 should be seen as a checklist for determining whether a data protection assessment would be appropriate. However, the preparation of a data protection impact assessment and the holding of advance discussions with the Norwegian Data Protection Authority as described in sections 3.4 and 3.5 will often be less relevant for small organisations.

• **Chapter 4 Data protection and patient rights**
  The chapter presents an overview of relevant provisions based on statutory requirements.

• **Chapter 5 Information security**
  These are the specific requirements regarding information security that are set out in the Code. All security measures must be appropriate and be chosen on the basis of risk assessments.

31 May 2018
# Table of contents

Preface.............................................................................................................................................. 4  

1 About the Code................................................................................................................................... 9  
1.1 Background to the Code.................................................................................................................. 9  
1.2 The EU’s General Data Protection Regulation (GDPR) .............................................................. 10  
1.3 Purpose............................................................................................................................................ 10  
1.4 Target group - who the Code applies to......................................................................................... 11  
1.5 Scope - what the Code regulates ................................................................................................. 11  
1.6 Development and administration of the Code............................................................................ 11  

2 Management and responsibility............................................................................................................. 12  
2.1 Responsibility and organisation of data protection and information security ......................... 12  
2.2 Responsibilities of the controller.................................................................................................. 13  
2.3 The management system.............................................................................................................. 13  
2.4 Information security goals ........................................................................................................... 15  
2.5 Information security instructions .................................................................................................. 16  
2.6 Data protection officer.................................................................................................................. 16  
2.7 The management’s review ......................................................................................................... 17  

3 Risk management................................................................................................................................. 18  
3.1 Record of the processing of personal health data and personal data ........................................ 19  
3.2 Overview of ICT equipment.......................................................................................................... 20  
3.3 Risk assessment............................................................................................................................ 20  
3.4 Data protection impact assessment............................................................................................. 22  
3.4.1 Additional assessment criteria................................................................................................. 23  
3.5 Advance discussions with the Norwegian Data Protection Authority........................................ 23  

4 Data protection and patient rights........................................................................................................ 24  
4.1 Duty of confidentiality .................................................................................................................. 24  
4.2 Rights of data subjects.................................................................................................................. 24  
4.2.1 Access to personal data and logs............................................................................................ 25  
4.3 Disclosure of personal health data and personal data................................................................ 25  
4.3.1 To parties other than the organisation’s and the administrative agency’s own employees......................................................................................................................... 25  
4.3.2 To the organisation’s management and to administrative systems ..................................... 26  
4.3.3 For educational and quality assurance purposes................................................................... 27  

5 Information security............................................................................................................................. 28
5.1 Employees, competence and attitude-forming campaigns ........................................ 28
  5.1.1 Terms and conditions ....................................................................................... 28
  5.1.2 Training and competence ............................................................................... 28
  5.1.3 Termination of employment ........................................................................... 28
5.2 Access control ...................................................................................................... 29
  5.2.1 Authorisation .................................................................................................. 30
  5.2.2 Authentication ................................................................................................. 32
  5.2.3 Control of access rights .................................................................................. 32
5.3 Physical security and the handling of equipment ..................................................... 33
  5.3.1 Keys/access cards ............................................................................................ 33
  5.3.2 User equipment (computers and printers - desktop) ....................................... 33
  5.3.3 Operating equipment (servers and network equipment) ................................. 33
  5.3.4 Mobile equipment and home offices ............................................................... 33
  5.3.5 Encryption ....................................................................................................... 34
  5.3.6 Medical equipment ......................................................................................... 34
5.4 Secure IT operation ............................................................................................... 34
  5.4.1 Configuration control ..................................................................................... 34
  5.4.2 Change management ....................................................................................... 35
  5.4.3 Back-up ........................................................................................................... 35
  5.4.4 Logging ............................................................................................................ 35
  5.4.5 Management and handling of technical vulnerabilities .................................... 36
  5.4.6 Security audit of information systems ............................................................ 37
5.5 Communication security ...................................................................................... 37
  5.5.1 Management of network security .................................................................. 37
  5.5.2 Safeguarding of network services ................................................................ 37
  5.5.3 Message exchange ........................................................................................ 38
  5.5.4 E-mail, text and social media ........................................................................ 38
  5.5.5 Internet connection ......................................................................................... 39
5.6 Digital communication with patients/health care users ......................................... 39
5.7 Suppliers and agreements ..................................................................................... 40
  5.7.1 Suppliers of communication services ............................................................. 40
  5.7.2 Processor ....................................................................................................... 41
  5.7.3 Suppliers ......................................................................................................... 43
  5.7.4 Security providers .......................................................................................... 43
  5.7.5 Collaboration between organisations concerning personal health data and personal data filing systems for therapeutic purposes ..................... 44
  5.7.6 Access to health data across organisations ................................................... 45
5.8 Handling of information security breaches .................................................. 45
  5.8.1 Breach management ............................................................................. 45
  5.8.2 Notification of data subjects .............................................................. 46
5.9 ICT readiness ......................................................................................... 47

6 Appendices ............................................................................................... 48
  6.1 Definitions ............................................................................................. 48
  6.2 Supporting documents ........................................................................... 55
    6.2.1 Fact sheets ...................................................................................... 56
    6.2.2 Guidelines ...................................................................................... 56
    6.2.3 Templates ...................................................................................... 56
  6.3 References ............................................................................................ 56
  6.4 History of the Code .............................................................................. 57
1 About the Code

1.1 Background to the Code

The Code is an industry Code prepared and administered by organisations and businesses within the sector, with the aim of contributing to satisfactory levels of information security, and data protection within individual organisations and the sector generally and contributing to the establishment of mechanisms where organisations can be confident that other organisations also process health- and personal health data and personal data with an appropriate level of security.

The data protection and health legislation impose requirements regarding information security and data protection. These requirements apply independently of the Code and relevant supervisory authorities (particularly the Norwegian Data Protection Authority and the Norwegian Board of Health Supervision) continually monitoring compliance with the applicable regulations by organisations. The data protection and health legislation also imposes other requirements concerning the processing of personal health data and personal data in addition to those covered by the Code, e.g. issues relating to secondary use, specific requirements for registered persons which are covered by their own regulations, the legal basis for the processing of personal health data and personal data and the obligations and requirements that apply regarding recordkeeping and other documentation. In addition, the impending Norwegian Security Act will also be of importance in the future.

The Code sets out requirements that detail and supplement the currently applicable regulations. The requirements set out in the Code are requirements which the health service believe are pivotal to the sector’s technical and organisational measures regarding information security and data protection.

The Code is a self-regulatory measure which can be used by anyone within the healthcare sector. Compliance with the requirements of the Code can be used to demonstrate fulfilment of the organisation’s obligations under the regulations. Through agreements, organisations operating in the sector may undertake to follow the requirements of the Code. Such agreements give other organisations cause to be confident that a particular organisation has established satisfactory levels of information security and data protection.

The Code contains requirements which cover most areas within information security and data protection; people, processes and technology. The Code also includes supporting documents in the form of guidance. This will be discussed further in Chapter 6.2.
1.2 The EU’s General Data Protection Regulation (GDPR)

Section 1 of the Norwegian Personal Data Act implements the EU’s General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The General Data Protection Regulation is implemented in Norwegian legislation based on Norway’s obligations under the EEA Agreement.

In version 5.3 of the Code, certain articles from the General Data Protection Regulation have been incorporated. The scope of the adaptations will therefore vary from chapter to chapter. All the requirements of the Code have been reviewed with the aim of ensuring that there is no contradiction between the Code and the new Personal Data Act.

Measures to protect personal data, including those that are referred to in the General Data Protection Regulation as “data security”, have a strong focus in the Regulation. The measures must be “appropriate”. This means that, in order to identify the right measures, consideration must be given to the specific characteristics of the data, the scope of the information being processed and the specific characteristics of those who will process the data. The measures must be selected based on risk assessments and they must be proportionate. This may mean that a small organisation that processes limited amounts of personal data should establish different measures compared to a larger organisation that processes large amounts of personal data.

1.3 Purpose

The purpose of the Code is to help to ensure that an organisation that complies with and follows the Code has appropriate technical and organisational measures in place regarding information security and privacy and data protection for its processing of personal health data and personal data. Those who interact with an organisation that is obliged to comply with the requirements of the Code will need to be confident that the organisation concerned has appropriate technical and organisational measures in place regarding information security and data protection for its processing of health and personal data.

The Code is intended to ensure that employees, patients and health care users are guaranteed a high level of privacy and data protection.

The Code is intended as an aid in the work of individual organisations relating to information security and privacy and data protection.

Within the framework of applicable legislation, the Code strives for a balanced approach to confidentiality, availability, integrity and robustness. The Code is intended to support high-quality health services, good patient safety, data protection for employees and an active patient role. An active patient role means that the safeguarding of patients' rights regarding their own health data, and the development where digital services establish contact between health personnel and citizens, patients and users, thereby contributing to greater participation.
1.4 Target group - who the Code applies to

The Code applies to any organisation, which by an agreement, has committed to comply with the Code.

1.5 Scope - what the Code regulates

The Code describes and sets out requirements regarding the work of organisations relating to information security and privacy and data protection for personal health data and personal data which is processed in connection with the providing, administration and quality assurance of health and social care services. The Code describes the organisational and technical measures that are considered appropriate in order to achieve a satisfactory level of information security and privacy and data protection regarding such processing of personal health data and personal data.

Organisations also process personal data concerning their own employees. The Code’s security requirements do not apply directly in this context, but organisations must protect data concerning their employees in accordance with applicable laws and regulations and industry rules. It is particularly important that data concerning employees’ use of information systems (logging) is essentially used for security purposes, in order to avoid unnecessary monitoring of employees. Employees have a right to access data that concerns themselves (see the General Data Protection Regulation Article 15).

The Code regulates data subjects’ right of access to logs.

The Code’s requirements concerning management and responsibility, risk assessments and information security are relevant to both the primary use (processing of personal health data and personal data which follows from the Patient Records Act (pasientjournalloven)) and the secondary use (the Personal health data and personal data Filing System Act) of data. In version 5.3, the Code's requirements regarding privacy and data protection and patient rights apply to primary use but may also be applied to secondary use insofar as they are applicable. The next version of the Code will encompass secondary use to a greater extent.

The processing of personal health data and personal data for research purposes follows the Health Research Act (helseforskningsloven) but is also subject to all other relevant legislation on the area. Before an organisation commences a research project, an application must be submitted to the Regional Committees for Medical and Health Research Ethics (REC).

The Code regulates the organizations processing of personal health data and personal data, both manual and electronic, but is primarily directed at the electronic processing.

1.6 Development and administration of the Code

The Code is prepared and administered by a steering group from the healthcare services; see the list at https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/om-normen#styringsgruppe-for-normen

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

The Directorate for eHealth is the secretariat for the work of the steering group, with permanent representation from the Norwegian Health Net (Norsk Helsenett, NHN).
2 Management and responsibility

It is a management responsibility to ensure that the organisation complies with applicable requirements regarding data protection and information security and that this responsibility is addressed as part of the work relating to corporate governance and quality improvement. Among other things, this includes the holistic management of risk and ensuring that governance and control are effective. Data protection and information security must be managed at a sufficiently high level within the organisation.

Security measures and compliance with the fundamental principles of data protection must be documented. This is necessary in order to fulfil the requirements regarding management and quality improvement, to meet the requirements regarding internal control and to demonstrate that appropriate technical and organisational measures are being implemented to ensure that personal data is processed in accordance with this Regulation and that the measures can be implemented again and updated as and when necessary. Moreover, it is a prerequisite that measures are documented so that they can be referred to in records concerning the processing of health and personal data.

2.1 Responsibility and organisation of data protection and information security

The person who has overall responsibility for an organisation must establish and maintain a satisfactory level of data protection and information security. Tasks may be performed by an organisation’s own employees or outsourced to external parties, e.g. tasks can be delegated to suppliers. This must be done through written agreements. Both the organisation (the controller) and the supplier (processor) have a responsibility to ensure that data protection and information security are safeguarded. The primary responsibility rests with the controller.

The work relating to information security within the organisation must be organised and carried out so that it is clear both who is responsible at every level and what they are responsible for.

For responsibility regarding:

- collaboration between organisations concerning health and personal data filing systems for therapeutic purposes, see point 5.7.5
- access to health data across organisations, see point 5.7.6

The work relating to data protection and information security must include management, implementation and control and must be documented in a management system (internal control) which cover data protection and information security (hereinafter ‘the management system’). Both the controller and the processor must have a management system in place.

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

2.2 Responsibilities of the controller

The controller is the party who, either alone or together with others, determines the purpose of the processing of personal data and the means that are to be used. The controller must establish and maintain a satisfactory level of data privacy and information security.

The controller must:

- Establish a management system
- Conduct risk assessments and prepare a data protection impact assessment as and where necessary
- Establish appropriate technical and organisational measures
- Safeguard the right of access of data subjects to information and ensure compliance with the rules concerning the correction and erasure of data subjects’ health and personal data
- Establish procedures for obtaining consent and the fulfilment of any opt-out from certain forms of processing of personal health data and personal data
- Ensure and document the lawfulness of processing activities
- Report breaches of data protection and information security.

2.3 The management system

The management system is the part of the organisation’s internal control system (quality system) which covers the way in which the organisation’s activities are planned, implemented, evaluated and corrected. The management system must be adapted to the organisation’s size, nature and activities, the nature, scope and purpose of the data processing and the context in which it is carried out.

In the case of small organisations, this may mean that not all the elements in the point list below are relevant. The factors of importance in the assessment are whether the organisation is so small and clear that responsibilities are self-evident or whether operators are used which are responsible for technical operations with procedures for operation of the information systems. The controller’s organisation is always responsible under any circumstances. Regarding the determination of acceptance criteria, the Code’s general requirements for the establishment of security measures described in Chapter 3 can be used as a basis. The organisation’s security goals can be based on the information security goals defined in section 2.4 below.

The organisation’s senior management must establish the management system and make it known within the organisation. For example, the management system can be structured with management, execution and review requirements and activities to guide and steer the organisation as regards data protection and information security.
The **management** part should include:

- Information security goals
- Record of processing of personal health data and personal data and keep the record up to date
- Level of acceptable risk
- Organisation/responsibility chart through at least:
  - Documenting responsibilities and tasks
  - Describing responsibilities and tasks at all levels
  - Making the levels of responsibilities known within the organisation
- Security instructions

The **execution** part should include:

- The type of suppliers that will be used and maintain an overview of them and the tasks they perform
- Agreements with partners, processors and suppliers
- Plans for the preparation of risk assessments and procedures for implementation and follow-up
- Configuration chart for the information systems and a technical description of the configuration
- Procedures for the approval of all configuration changes in information systems
- Procedures for the processing of personal health data and personal data
- Procedures and rules for use of the information systems must at least ensure that:
  - Only information which a person is authorised to access and has an official need to access must be searched for.
  - The specific procedures in connection with self-authorisation for personal health data and personal data filing systems for health purposes are followed.
  - All unauthorised access to data is followed up as a breach.
  - Authorisation criteria are protected, partly by keeping passwords secret.
  - The personal health data and personal data which is registered is relevant and necessary.
  - Registration is carried out as soon as possible after the information has been acquired.
- Procedures for operation of the information systems
- Documentation of security measures – organisational, physical and technical (see Chapter Feil! Fant ikke referansekilden.)
- Procedures linked to the use of processors, providers of communication services, equipment or software and other suppliers

The **review** part should include:
• Plan for the performance of security audits and a procedure for the follow-up of the results of such security audits. Security audits must be carried out regularly.
• Plans for the management’s review and a procedure for the follow-up of action plans approved by the management. The management’s review must be carried out at least once a year and cover areas such as non-conformities and any corrections in the management system
• Procedures for non-conformity management in the event of breaches of procedures, among other things

Documents specified in the management system must be kept up to date on an ongoing basis and archived from the date on which the document is superseded by a new current version. The purpose of the archiving is partly to facilitate the tracing and correction of breaches over time.

The following must be archived for at least five years from the date on which the document was withdrawn from use:

• All documents in the management, execution and review parts referred to above
• Results of security audits
• Results of risk assessments
• Results of breach management
• Results of the management’s review
• Overview of allocated authorisations and access to personal health data and personal data (authorisation log)
• Agreements with partners, processors and suppliers

The following must be safeguarded until there is no longer considered to be any need for them given the nature of the health and social care services:

• Logs of importance as regards security, including registration of authorised use and attempted unauthorised use of the information systems

Documentation concerning measures relating to information security must be secured in a corresponding way to personal health data and personal data when awareness of the measures by unauthorised parties would entail a risk.

### 2.4 Information security goals

Key information security goals for the health and social care sector are that personal health data and personal data must:

• Be available to the right personnel at the right time and in accordance with established principles for access control pursuant to Chapter Feil! Fant ikke referansekilden.
• Be processed in accordance with the rules concerning the confidentiality and be protected so that unauthorised parties do not gain access to the data. “Unauthorised parties” also includes personnel who do not have an official need.
• Be complete, updated and accurate and a result of legitimate registrations and controlled activities.
• Be limited so that only personal health data and personal data which is necessary is processed.

The organisation’s management must determine an acceptable level of risk based on the above information security goals and the requirements set out in Chapter 3.

The options for achieving the information security goals must be documented. Among other things, it is the organisation’s responsibility to decide whether the work should be carried out internally within the organisation or whether the organisation should outsource some, or all of the work to external contractual parties.

Based on this, the organisation must identify appropriate technical and organisational measures. The measures must be implemented on the basis of a risk assessment regarding for the data subject’s data privacy. This assessment must take into account the nature, scope and purpose of the processing and the context in which it is carried out. The implementation of measures to protect personal data must be considered for the various processing activities.

2.5 Information security instructions

The senior management must ensure that the organisation prepares and administers information security instructions which summarise the key requirements regarding data protection and information security within the organisation. This assessment must take into account the nature, scope and purpose of the information processing and the context in which it is carried out.

The instructions must bind the employee to follow the requirements and must be updated in the event of changes in requirements and measures.

2.6 Data protection officer

The organisation’s senior management must ensure that a data protection officer is appointed within all public and private sector organisations as and when necessary on the basis of the scope of information processing. The data protection officer may be an employee or an external party who performs tasks based on a service agreement.

The data protection officer must be appointed on the basis of personal qualifications, specialist expertise relating to data protection legislation and the ability to perform the tasks involved. The data protection officer must not have any conflicts of interest with respect to any other roles that the person performs within the organisation and must not receive instructions regarding how the tasks are to be performed. The data protection officer must not reach decisions concerning the processing of personal data or the method to be used for such processing.

The data protection officer must be given sufficient resources and access to appropriate expertise in order to perform his or her tasks. The data protection officer must report directly to the organisation’s senior management.
The processor must also appoint a data protection officer in accordance with the rules stipulated above.

The data protection officer must assist the work of the controller, processor and the employees relating to data protection and information security in order to maintain an acceptable level of risk.

2.7 The management’s review

The organisation’s senior management must evaluate the organisation’s activities and ensure that information security is safeguarded through at least an annual review. The obligation includes a review of breaches, including incidents, so that similar circumstances can be avoided.

The management’s review must be viewed in the context of financial and organisation planning, as the decisions taken can have financial consequences.

The purpose of the review is to determine the status of the security level and assess whether this level is in accordance with the organisation’s information security goals. On the basis of risk and relevance, the following points should be covered:

- The purposes of the processing of personal health data and personal data and a record of the processing of such data
- Responsibility and organisation with regard to data protection and information security
- Results of security audits
- Results of risk assessments and data protection impact assessments as and where necessary
- Results of breach management. The organisation’s management must regularly follow up to ensure that measures based on the breaches are identified, planned and implemented
- Follow-up of suppliers in relation to the technical solutions that are used
- Monitoring and follow-up of established agreements (see Chapter 5.7)
- Level of acceptable risk
- Where appropriate, decide on the updating of information security goals

If the review indicates that the actual situation does not comply with the established acceptable level of risk, action plans must be established in order to achieve the established acceptable level of risk. The responsibility must be delegated as necessary.
3 Risk management

It is the responsibility of the management to ensure that risk management and control are effective. This entails establishing an overview of data types which are processed within the organisation, the risks that this entails for both the organisation and the data subjects, and the countermeasures that should be implemented.

Both the controller and the processor must implement proportionate technical and organisational measures. This includes safeguarding confidentiality, integrity, availability and robustness in the information systems. Consideration must be given to technological developments, implementation costs and the nature, scope and purpose of the information processing and the context in which it is carried out.

In the case of small organisations, this means that the work relating to risk management must take account of numerous factors, including the size and organisational structure of the organisation. For example, if the organisation performs ICT tasks as an operator, the organisation's own risk assessment will be more comprehensive than if a supplier or vendor was responsible for these tasks. The controller's organisation is however always responsible for the risk management.

In order to prevent unintentional or unlawful destruction, loss, alteration or the unauthorised disclosure of or access to personal data, the following minimum general requirements must be used as a basis for the establishment of security measures:

Confidentiality
Confidentiality must ensure that the duty of confidentiality is fulfilled and otherwise ensure that unauthorised persons do not gain access to data. Among other things, this means that:

- Persons outside the organisation must not be able to gain unauthorised access to personal health data and personal data.
- Persons within the organisation must be given access in accordance with established principles for access control in accordance with the requirements of Chapter Feil! Fant ikke referansekilden..
- The names of persons who have had access must be recorded in logs in personal health data and personal data filing systems (including electronic patient records (EPR)) and data processing systems.

Integrity
- The names of persons who entered records, changes, corrections and deletions must be recorded in personal health data and personal data filing systems for health purposes (including electronic patient records (EPR)) and data processing systems. This will ensure that there is an audit trail to the origin.
- Security measures must be implemented to ensure that persons or technology, either within or outside the organisation, must not be able to change personal health data and personal data without authorisation.
- Personal health data and personal data must be accurate and be linked to the appropriate identified person.
- Personal health data and personal data must be entered in accordance with the relevant coding system.
- Personal health data and personal data must be complete and updated in relation to the processing of the data.

**Availability**

- Within the framework of the duty of confidentiality, personal health data and personal data must be accessible when there is an official need to access such data.
- Self-authorisation may be established as an option for authorised users to give themselves access without following established principles for gaining access to personal health data and personal data in accordance with Chapter Feil! Fant ikke referansekilden. In such cases, specific procedures must be prepared. The reason for self-authorisation must be documented.
- The misuse of self-authorisation must be followed up as a breach.
- See Chapter 5.9 concerning the classification of the criticality of the information system and the determination of an acceptable level of risk for availability for each relevant classification.

**Robustness**

- Appropriate technical and organisational measures must be implemented to facilitate the prevention, detection, scalability, handling and restoration of personal data security and information security in general.

On the basis of these general requirements and the organisation's information security goals (see Chapter 2.4), the organisation must establish an acceptable level risk which is to apply within the organisation.

### 3.1 Record of the processing of personal health data and personal data

An overall updated overview of all processing of personal health data and personal data within the organisation is an important governing document for information security, as well as a practical tool in the execution work. The overview will also contribute to the general level of internal control within the organisation. This will help to document the compliance with applicable legislation. The overview could for example be prepared as a database with an overview of the processing of personal health data and personal data that are carried out within the organisation at any time. This could encompass IT systems, projects (research projects, etc.), medical equipment and manual filing systems, etc.

Organisations that process health data must have an overview of the processing activities. In the General Data Protection Regulation, this overview is referred to as “Record of processing activities”.

The record must as a minimum contain the following data:

- Name and contact details of the controller and any joint controller
- Processor and processor agreements
- Name and contact details of the data protection officer
Purposes of the processing
- Basis for the processing
- Categories of data subjects (e.g. patients - child and adult, client, user of service, employee, health personnel, information system user)
- Categories of personal data (e.g. employee data, health data)
- The extent to which it processes personal data from special categories
- Recipients of personal data (e.g. NAV, HELFO, the prescription register, insurance companies, etc.)
- Any transfer to other countries and confirmation that the recipient is complying with regulatory requirements
- Planned storage time
- Description of technical and organisational security measures; see the management system
- Whether a data protection impact assessment has been prepared

The record must be in writing, and it may be electronic.

3.2 Overview of ICT equipment

The organisation must have an overview of all ICT equipment. This overview must include desktop and portable computers, mobile phones and other communication equipment, servers, network equipment (routers, switches, firewalls, etc.), printers, storage networks, apps, IP phones, etc.

The following measures should be implemented in large organisations:
- Prepare an overview of hardware and software which are maintained using automatic tools
- The inventory system for software should trace the version of the underlying operating system and the programs that are installed on it.

3.3 Risk assessment

Risk assessments are an important part of the management, execution and review of the information security work.

Before the processing of personal health data and personal data is initiated, a risk assessment must be carried out in order to map risk areas and determine the probability and consequences of incidents. A new risk assessment must be carried out in the event of changes that are of importance for information security. The organisation’s management must also regularly carry out risk assessments as part of its work to monitor information security.

The controller and processor must implement appropriate technical and organisational measures to achieve a level of security which is proportionate to the risk. In connection with the assessment of measures, consideration must be given to the nature of the information processing and the context in which it is carried out, scope, purpose, technological developments and the cost of implementing the measures.
The purpose of the risk assessment is to determine whether the controller and the processor have implemented sufficient measures to ensure that an appropriate level of security is achieved, or whether additional measures must be implemented.

A key aspect of the task is to identify the data which must be protected and to map out the environment in which the data exists. With regard to this, the record of the processing of personal health data and personal data will act as a starting point; see section 4.1. The risk assessment must also identify the need for risk mitigation measures by comparing the identified risk with the established acceptable level of risk. The acceptable level of risk is based on the information security goals.

The term “risk” encompasses two parameters: the probability that something will happen and the consequences the incident could have. When we refer to security risk regarding information systems, incidents which are assessed in this way will be linked to the three aspects that are normally associated with information security. These are confidentiality, integrity and availability.

The risk assessment is based on the acceptable level of risk and consists of the following stages:

1. Preparations regarding planning and organisation
2. Mapping and assessment of personal data processing
3. Identification of incidents
4. Impact assessments
5. Probability assessments
6. Risk calculation and assessment
7. Measures that are implemented

Risk assessments should as a minimum be carried out before:

- the processing of personal health data and personal data is initiated
- new information processing systems or registers which contain personal health data and personal data are established
- organisational changes are implemented that could have an impact on the data processing
- technical changes are made to equipment and/or software that could have an impact on the data processing
- other changes of importance to the information security are implemented
- access to health data between organisations is implemented

The risk assessment must be documented. The conclusions from the assessment must be compared with the established acceptable level of risk. If the risk is higher than the established acceptable level of risk, measures (new/amended) must be implemented to attain an acceptable level of risk. If technical measures for achieving an acceptable level of risk are not implemented immediately, administrative measures, e.g. in the form of procedures, may be implemented as a transitional measure.

The organisation’s management must also regularly carry out risk assessments in order to map risk areas and determine the probability and consequences of incidents.
3.4 Data protection impact assessment

If it is likely that a certain type of processing of personal health data and personal data will entail a high risk to privacy and data protection, the controller must assess the impact that the planned processing will have. An assessment of the data protection consequences must be carried out before the processing of personal data commences. If a new system is to be developed, the assessment must be carried out at a sufficiently early time in the development process and always as part of the establishment of requirements.

A data protection impact assessment must be carried out when a high risk regarding privacy and data protection will result:

- from the use of new technology
- from the nature, scope and purpose of the processing and the context in which it is carried out
- [Reference to impending list from the Norwegian Data Protection Authority]

A data protection impact assessment must specifically be carried out when the processing:

- involves a large-scale processing of health data in or of personal data concerning convictions and criminal offences
- involves a systematic and comprehensive assessment of personal aspects linked to individuals based on automated processing (profiling), which forms the basis for decisions which have legal effect or a significant impact on the data subject.

If the processing of personal health data and personal data is regulated by law and an assessment of the data protection impact has already been carried out as part of a general impact assessment in connection with the adoption of the regulations concerned, the requirement for a data protection impact assessment may be waived.

Data protection impact assessments must at least include:

- a systematic description of the processing activities
- a description of the purpose of the processing
- an assessment of whether the processing activities are necessary and proportionate to the purpose
- an assessment of the privacy and data protection risks for the data subject
- the planned risk mitigation measures regarding privacy and data protection.

In the case of a number of similar processing activities which entail similar levels of risk, such activities may be assessed jointly.

If necessary, e.g. if the risk situation changes, a review should be carried out to determine whether the processing is being carried out in accordance with the original data protection impact assessment.

If the organisation has a data protection officer, the officer must be consulted in connection with the preparation of the assessment.

Measures that reduce the risk for data protection must be planned. If the processing of personal health data and personal data will entail a high level of risk that cannot be mitigated through reasonable means, the controller must consult the Norwegian Data Protection Authority before the processing commences.
3.4.1 Additional assessment criteria

The following nine criteria may be used to determine whether processing will require a data protection impact assessment. If the controller’s response to two or more of the questions concerning the planned processing of personal health data and personal data is affirmative, a data protection impact assessment must be carried out:

1. Is the processing an evaluation or a scoring?
2. Does it cover automated decisions?
3. Does it entail systematic monitoring?
4. Does it involve special categories of personal data?
5. Does it involve the processing of personal data on a large scale?
6. Will two or more data sets be merged?
7. Does the processing cover personal data concerning data subjects with special needs for protection?
8. Does it use new technology or is existing technology used for new purposes?
9. Will the context of the processing limit the opportunity for the data subjects to exercise their rights?

If a processing activity fulfils fewer than two criteria, a data protection impact assessment may not be necessary.

3.5 Advance discussions with the Norwegian Data Protection Authority

The controller must consult with the Norwegian Data Protection Authority if:

- the data protection impact assessment indicates that the processing of personal health data and personal data will entail a high level of risk, even after the planned measures have been carried out
- the data protection impact assessment indicates that the processing of personal health data and personal data will entail a high level of risk irrespective of any measures that are carried out.

The controller must present the following to the Norwegian Data Protection Authority:

- The delegation of responsibility between the controller, joint controllers and processors, where relevant
- The purposes of the planned processing and the way in which it will be carried out
- The measures and guarantees that have been established to protect the data subjects’ personal data
- Contact details for the data protection officer, where relevant
- The data protection impact assessment
- Any other information which the Norwegian Data Protection Authority requests

If the Norwegian Data Protection Authority considers that the processing will be in breach of data protection legislation, the authority may provide the controller with written advice. This particularly applies if the controller has not adequately identified or mitigated the risks.
4 Data protection and patient rights

In version 5.3 of the Code, certain articles from the Regulation have been incorporated; see the preface. The provisions of the Regulation concerning the rights of data subjects and the associated patient rights have not been incorporated in this version. This work will continue in future versions of the Code. As a result, this chapter is not exhaustive as regards data protection and patient rights in general but refers to selected topics.

4.1 Duty of confidentiality

To safeguard the confidentiality of personal health data and personal data, the organisation’s manager must ensure that all personnel who are given access are subject to a duty of confidentiality and aware of the content and scope of the duty of confidentiality as regards all personal health data and personal data and other information of importance for information security. The confidentiality statement must at least:

- Describe the consequences of a breach of the duty of confidentiality.
- Describe the consequences of acquiring or attempting to acquire data for which one has no official need (unlawful access).
- Describe the consequences of altering/attempting to alter data that one does not have authorisation to alter.

Any breach of the duty of confidentiality and/or unlawful access must at least result in a warning being issued to the person who committed the breach, and the breach must be dealt with in accordance with the applicable breach procedure. In the event of serious or repeated breaches of the duty of confidentiality, the consequences for the employment must be assessed.

All breaches of the duty of confidentiality and/or unlawful access are prohibited, and consideration must be given to notifying the supervisory authorities and the police.

4.2 Rights of data subjects

Procedures must be established, and measures must be implemented to ensure that:

- Patients/health care users are informed of the organisation’s processing of personal health data and personal data and their rights regarding access, correction, erasure and blocking of data that is registered about them.
- The written consent of patients/health care users is obtained in all cases where this is necessary, including when access to the relevant processing of personal health data and personal data concerned is neither stipulated by law nor has any other valid basis.
- Patients/health care users are secured access to their own personal health data and personal data.
- Patients’/health care users’ rights regarding the correction/deletion of personal health data and personal data are safeguarded.
• Patients’ rights regarding the blocking of all or certain data in their own medical records must be safeguarded

If a data subject submits a request electronically, the information must be provided electronically where possible, unless the data subject requests otherwise.

In the case of access to health data across organisations, the controller must inform the patient/health care user that health data has been accessed across the organisations. The information must be adapted to meet the needs and circumstances of the patient/health care user and may be omitted if it is clearly inadvisable. Among other things, the information must state:

• the organisations that are being given access
• the personal health data and personal data that the access concerns
• that the patient/health care user may object to access being given.

4.2.1 Access to personal data and logs

Patients and health care users have a right to access their own data in personal health data and personal data filing systems (including electronic patient records (EPR)/data processing systems) and a right to a clear and brief explanation of technical expressions or the like. Patients and health care users may be denied access to data in the record under special rules.

Procedures must be established to ensure that the rights of data subjects regarding access to logs are safeguarded. The procedures must at least ensure that the data subject receives data concerning:

• The name and organisational affiliation of the person who processed the health data
• The processing of the personal health data and personal data that has been carried out
• When the processing of the personal health data and personal data was carried out.

When health data is exchanged between organisations, the data subject must also receive data concerning:

• the name and organisational affiliation of the person who retrieved the health data
• why the health data was retrieved
• the periods of time during which the person has retrieved the health data.

4.3 Disclosure of personal health data and personal data

4.3.1 To parties other than the organisation’s and the administrative agency’s own employees
When it is necessary in order to provide appropriate health and social care services, personal health data and personal data may be transferred, disclosed or given to health personnel other than the organisation’s own employees. This must take place in accordance with statutory provisions concerning duty of confidentiality. Requests for the transfer or disclosure of personal health data and personal data must be processed in accordance with procedures which fulfil the requirements relating to confidentiality, integrity and availability. Health records must always state when personal health data and personal data has been disclosed to employees other than the organisation’s own employees.

The disclosure of personal health data and personal data by one administrative agency to another may only take place when this is necessary in order to provide a care service or to prevent a material risk of loss of life and health or in accordance with any other basis in law. This must take place in accordance with statutory provisions concerning duty of confidentiality. Requests for the transfer or disclosure of personal health data and personal data must be processed in accordance with procedures which fulfil the requirements relating to confidentiality, integrity and availability.

Personal health data and personal data may be disclosed from one organisation to another (both within the health and care sector) if one of the following conditions is met:

- the data subject consents to the disclosure
- it is stipulated in law that such disclosure is permitted
- disclosure is necessary in order to protect a person’s vital interests and the data subject is unable to give his or her consent
- it exclusively concerns the disclosure of data which the data subject themselves has voluntarily made publicly known

A patient or health care user may object to health data in a health- and personal data filing systems (electronic patient record (EPR), joint personal health data and personal data filing system or national personal health data and personal data filing systems being made available to health personnel and health data being registered or otherwise processed in the Kjernejournal (Summary Care Record).

### 4.3.2 To the organisation’s management and to administrative systems

When it is necessary in order to provide health and social care services or for internal control and quality control of the service, the party that provides health and social care services may disclose the data to the organisation’s management. The disclosure of data must be limited to data that is necessary and relevant for the purpose. Insofar as is possible, the health data must be processed without the name and national ID number of the data subject being disclosed. However, if it is necessary to disclose directly identifiable personal data, the patient/health care user may object to the disclosure.

Health personnel must be obliged to disclose a patient’s national ID number and data concerning diagnoses, medical needs, services, admission and discharge dates and relevant administrative data to the organisation’s internal patient administration systems (see Section 26 of the Health Personnel Act (helsepersonelloven)).
4.3.3 For educational and quality assurance purposes

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

The disclosure of data must be limited to data that is necessary and relevant for the purpose. The patient’s record must state the data has that been disclosed and who it has been disclosed to.
5 Information security

This chapter describes the key security measures which must be carried out by organisations that process personal health data and personal data. This covers both the controller and the processor. All security measures must be appropriate and be chosen on the basis of risk assessments. It may therefore be necessary to carry out more comprehensive measures than what is described here.

5.1 Employees, competence and attitude-forming campaigns

5.1.1 Terms and conditions

In connection with appointments, conditions must be established individually for employees concerning the manner in which personal data must be processed within the organisation and the general requirements that apply. These conditions may be included in the employment agreement between the employer and the employee or agreed in writing in some other appropriate manner.

Such conditions must at least include:

- Security instructions
- Confidentiality declaration
- The sanctions open to the organisation in the event of a breach

5.1.2 Training and competence

The organisation must implement measures that ensure that:

- anyone who is given access to and/or operates data systems and associated information possesses sufficient knowledge to use the systems both to perform their role and to safeguard information security.
- anyone who has access to personal health data and personal data processes such data in accordance with applicable regulations, the Code and the organisation’s routines

Training must take place continually and be adapted to the various roles and user groups concerned. Specific training measures must be assessed for new employees and in the event of changes to data systems or the processing of personal health data and personal data.

5.1.3 Termination of employment
When an employee’s employment is terminated, it must be ensured that the former employee returns to their employer all media (including digital, paper, etc.) which may contain personal data to which the person concerned has gained access in their capacity as an employee within the healthcare sector.

The duty of confidentiality must also apply after the employment has ended.

### 5.2 Access control

This affects how one administers:

- Authorisation, which is the allocation of rights to read, register, correct, erase and/or block personal health data and personal data.
- Authentication, which protects the identification of authorised users.
- Disclosure of personal health data and personal data concerning specific patients/health care users for authorised personnel.
- Disclosure of personal health data and personal data to personnel other than the organisation’s own personnel.
- Regulations concerning the private use of the organisation’s data systems.
- Review measures.

Within the framework of the duty of confidentiality, the controller must ensure that relevant and necessary health data is available to health personnel and other collaborating personnel as and when necessary in order to provide, administer or quality-assure health and social care services to an individual.

The controller must determine the manner in which the data is made available. The data must be made available in a manner which safeguards information security.

Access control must be established for all personal health data and personal data filing systems for therapeutic purposes (including electronic patient records (EPR)) and data processing systems.

The disclosure of personal health data and personal data to health personnel other than the organisation’s own personnel is regulated in Chapter 4.3.

Only authorised personnel may gain access to personal health data and personal data.

Access to personal health data and personal data filing systems for therapeutic purposes (including electronic patient records/data processing systems) must be granted following a specific decision based on the completed or planned implementation of measures for the medical treatment of the patient. Access must be controlled to ensure compliance with the confidentiality rules and so that no access to personal health data and personal data is given to anyone other than those with an official need to gain such access.

In the case of the exchange of health data across organisations, both the organisations involved must have technical and organisational solutions which delimit access to health data which at least ensure that:

- health data is not made available if the patient/health care user has objected or objects to it
• access is only given to health data which is relevant and necessary in order to provide, administer or quality-assurance health and social care services to the patient/health care user
• the health personnel are authorised to gain such access and have authenticated themselves using a secure authentication solution.

5.2.1 Authorisation

The controller is responsible for ensuring that authorisations are assigned, administered and monitored.

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

The controller must delegate authority to assign authorisation to the individual unit’s responsible manager. As part of this, the responsible manager must, within their area of responsibility, assess and approve each individual employee’s need to gain access to personal health data and personal data. Assigned authorisation must ensure that an individual employee is able to gain access to personal health data and personal data as and when necessary in accordance with the employee’s responsibilities and duties, insofar as the statutory duty of confidentiality does not prevent such access.

If roles are used within an organisation, authorisation must be granted for each role, irrespective of the employee’s other roles.

Procedures must be established for the allocation and administration of access rights.

• Authorisation to read, register, correct, erase and/or block personal health data and personal data must be given to those with an official need to gain such access. The authorisation must be assigned in accordance with appropriate procedures. The statutory duty of confidentiality must be assessed and complied with. Technical measures must also be implemented in order to fulfil requirements regarding confidentiality by actively preventing unauthorised persons from gaining access to data and in order to ensure that assigned authorisations are documented. The time of use of authorisations must be recorded in the personal health data and personal data filing system for therapeutic purposes (including electronic patient records) or data processing system.

• Only technical personnel with a specific need for access may be authorised for large quantities of personal health data and personal data. Measures must be implemented to ensure that possible cases of misuse can be detected.

• Authorisation for other services must be given on the basis of official need, e.g. authorisation to use e-mail, the internet, etc.

The following measures must be implemented to prevent unauthorised persons from gaining access to personal health data and personal data:

• Technical and organisational measures must be implemented so that persons are unable to gain access to personal health data and personal data for which they do not have authorisation.

• If provision is made for self-authorisation, technical measures must be established in such a way that health personnel may gain access to personal health data and personal data as and when necessary. Such access must be justified and registered in personal
health data and personal data filing systems for therapeutic purposes (including electronic patient records).

- The misuse of self-authorisation must be followed up as a breach.
- Technical measures must be implemented to ensure that persons within or outside the organisation are unable to alter data without it being registered in personal health data and personal data filing systems for therapeutic purposes (including electronic patient records) and data processing systems who made the alteration and what was altered.
- Systems that administer authorisation must distinguish between rights to read, register, correct, erase and/or block personal health data and personal data. All allocations of authorisation must be registered in a register of authorisations.

5.2.1.1 Authorisation register

The controller must ensure that an authorisation register is established. The register must at least contain the following:

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

5.2.1.2 Kjernejournal (the Summary Care Record)

The controller for Kjernejournal may delegate authority to assign authorisation to an individual organisation which is to use summary care records. Access must then be obtained via an authorisation solution within the organisation. For Kjernejournal, the authorisation must be time-limited. Each organisation is responsible for ensuring that an authorisation register is established in accordance with what is described above. The guidelines for authorisation and access control regarding Kjernejournal are described in more detail in the specific guidelines for the national summary care record.

5.2.1.3 Access across organisations

In connection with access across organisations, the authorisation of health personnel regarding access to health data in other organisations must:

- describe the rights and obligations that follow from the authorisation
- be in accordance with rules concerning duty of confidentiality
- be documented in the organisation’s authorisation register
- be time-limited
- always be assessed and, where appropriate, amended in the event of changes in areas of responsibility or employment.
In connection with access to health data across organisations, patients/health care users may request that access to their own health data be blocked to health personnel from organisations other than that in which the data was registered. ‘Blocking’ means a technical solution where record data is rendered inaccessible to individuals, groups of health personnel or health personnel in organisations other than that in which the record notes were registered.

5.2.2 Authentication

Authentication must safeguard at least the following:

- In connection with access to personal health data and personal data filing systems for therapeutic purposes (including electronic patient records (EPR)) and data processing systems, different employment relationships must be identified. Satisfactory authentication must be used in accordance with a risk assessment.
- Several people must not use the same authentication criteria.
- The assigning of authentication criteria (such as user name and password) must be carried out in an appropriate safe manner.
- A secure authentication solution must be used in connection with access to health data across organisations.
- Access from home offices and/or mobile equipment must be secured through authentication which does not entail an increase in risk over and above that which applies to stationary equipment. A risk assessment must demonstrate that the authentication solution provides an adequate level of security. This also applies to regional offices which communicate with the aid of lines over which one has no physical control.

If roles are used, different roles must be identified and, where necessary, assigned different authentication criteria.

5.2.3 Control of access rights

Access control, including assigned authorisations, must be reviewed and monitored by the individual manager:

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

The organisation’s management must ensure that checks are regularly carried out to determine who has gained electronic access to health data in a personal health data and personal data filing system for therapeutic purposes (including electronic patient records (EPR)) or a data processing system. See Chapter 5.4.4. Logging.

The organisation’s management must be informed if checks result in a suspicion that unauthorised access has taken place. The incident must otherwise be dealt with in
accordance with established procedures for breach management, particularly with the aim of clarifying whether existing access control is satisfactory.

The Norwegian Data Protection Authority must be informed if the controls indicate that unauthorised access has taken place. The organisation’s management must also consider whether the patient/health care user should be informed.

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

- who within his or her own organisation has electronically retrieved health data from another organisation
- why this was done
- the period during which the health data was retrieved

If the controls indicate that an unauthorised person has retrieved health data, the organisation from which the data has been obtained must notify the patient/health care user the data concerns. The breach must be dealt with in accordance with established procedures for non-conformity management.

### 5.3 Physical security and the handling of equipment

#### 5.3.1 Keys/access cards

Procedures must be established for the administration of keys/access cards in the access control system.

#### 5.3.2 User equipment (computers and printers - desktop)

Security measures must prevent unauthorised persons from gaining access to personal health data and personal data - either through access-regulated control of premises with equipment or through the equipment being protected from misuse and screens, printouts, etc. by protecting it from unauthorised access.

#### 5.3.3 Operating equipment (servers and network equipment)

Security measures must ensure that only authorised personnel can gain access to such equipment.

All storage media, i.e. disks, memory sticks, CDs, etc. must be labelled, and all personal health data and personal data must be erased when the storage medium is taken out of use. Archiving obligations regarding the data must be fulfilled under all circumstances.

#### 5.3.4 Mobile equipment and home offices

As it is not possible to secure premises for this type of equipment, it is necessary to secure the equipment. Risk assessments must be carried out concerning the solutions that are
used. Administrative procedures must be established regarding the use of mobile equipment and home offices.

Security measures must prevent unauthorised persons from gaining access to personal health data and personal data through:

- Technical measures being implemented so that data can only be communicated using pre-defined equipment. Authentication must not entail an increase in risks beyond what applies to desktop equipment. A risk assessment must demonstrate that the authentication solution provides an adequate level of security.
- Personal health data and personal data must only be stored locally where such storage is necessary on the basis of official need and must always be stored encrypted.
- All communication, whether wireless or wired, must be secured through encryption in accordance with the "NSM Cryptographic Requirements Version 3.1".

5.3.5 Encryption

Technical measures must be implemented so that all communication of personal health data and personal data outside the control of the organisation is encrypted.

5.3.6 Medical equipment

Storage devices for electromedical equipment that processes personal health data and personal data must be located in a locked room or a manned area.

Medical equipment which processes personal health data and personal data must be included in the organisation’s work relating to information security, e.g. in risk assessments, access control and procedures regarding use, in the same way as other information systems.

5.4 Secure IT operation

5.4.1 Configuration control

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

- The configuration must ensure that the equipment and software only perform the functions that are specific to the intended purpose.

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

- Risk assessment which demonstrates that an acceptable level of risk is achieved
- Test which ensures that the expected functions are provided
- Implementation which provides protection against unforeseen events
- New configuration is documented

• Configuration changes have been approved by the organisation’s manager or the person designated by the management

Configuration checks must be regulated through an agreement concerning:
• Use by the processor.
• Use of remote access for maintenance and updates.

5.4.2 Change management

All changes within the organisation, information systems and systems which impact on information security must be anchored at the relevant managerial level.

The organisation must prepare procedures for change management which must cover the following topics:
• Identification of material changes
• Planning and testing of changes
• Assessment of potential consequences, e.g. by carrying out a risk assessment
• Approval procedure for changes
• Communication of plan to relevant persons/roles
• Back-up procedure if the change has to be terminated, fails or undesirable events occur
• Change log with relevant information

5.4.3 Back-up

The organisation’s management must also ensure that back-up copies are made of personal health data and personal data as well as other information that is necessary for the restoration of normal use.
• Back-up copies must be stored in a locked and fire-proof facility and kept separate from the operating equipment.
• Regular tests must be carried out to ensure that the back-up copies are correct and can be restored.

5.4.4 Logging

It must be possible to analyse logs using analysis tools with the aim of detecting breaches.
• Procedures must be established to analyse the logs so that incidents are discovered before they have serious consequences, ideally within one week.
• Procedures must be established so that logs can be compared with the authorisation log as and when necessary.
• If breaches are discovered, personnel-related action must be taken.
• If personnel-related action does not have the necessary effect over time, i.e. repeated access is made by a number of unauthorised persons, the necessary technical measures must be implemented.
• The logs and authorisation register must be protected against alteration and erasure by unauthorised personnel.

In order to discover either actual or attempted breaches of the regulations, at least the following must be logged:

• Authorised use of the information systems must be registered.
• Security barriers must log security-related events, e.g. attempted unauthorised use of the information system.
• Network operating systems must log all cases of attempted unauthorised use.
• All information systems must log all cases of attempted unauthorised use.
• The use of self-authorisation for personal health data and personal datafiling systems for therapeutic purposes must be logged.
• Logs must be protected against alteration and erasure by unauthorised personnel.

At least the following must be recorded in the logs:

• unique identifier for the authorised user
• the role of the authorised user at the time of access
• organisational affiliation
• organisational affiliation of the authorised person
• type of data to which access has been gained
• who disclosed health data that is linked to the name or national ID number of the patient or health care user
• basis for the access
• time and duration of access.

When health data is exchanged across organisations, the following must also be logged by the organisations concerned:

• the name and organisational affiliation of the person who retrieved the health data
• why the health data was retrieved
• the periods of time during which the person has retrieved the health data.

It must be possible to analyse all logs using suitable tools and, when necessary, to compare the logs with the authorisation log.

5.4.5 Management and handling of technical vulnerabilities

The management and handling of technical vulnerabilities must follow the procedures for change management (see chapter 5.4.2). The organisation must have procedures for obtaining information concerning technical vulnerabilities in equipment and software.

The basis for management and handling must be as follows:

• Overview of ICT equipment
• Software: software, supplier, version numbers, which version is installed where, and who is responsible for the software.
Procedures and operational measures must be established which address:

- Responsibility for: monitoring, risk assessment, correction and coordination
- How the organisation should respond to and report vulnerabilities
- Prioritisation and establishment of time line for correction
- All corrections should be tested before they are implemented

5.4.6 Security audit of information systems

The organisation’s management must follow up to ensure that security is being safeguarded through regular and at least annual security audits. An approved plan for security audits must be established.

The security audit must at least include assessments of:

- Delegation of responsibility and organisation of the security work
- Quality of security goals and security strategy
- Compliance with procedures concerning the use of information systems and personal health data and personal data
- Results of training
- Administration of the use of personal health data and personal data
- Access to personal health data and personal data and measures to prevent unauthorised access
- Testing, analysis and assessment of the effectiveness of the technical and organisational security measures
- Safeguarding of information security amongst communication partners, processors and suppliers

The results and conclusions of security audits must be documented. If a security audit identifies that information systems are being or have been used in a manner that was not anticipated, this must be treated as a non-conformity.

5.5 Communication security

5.5.1 Management of network security

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

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

5.5.2 Safeguarding of network services

In the case of connections to networks which are located outside the organisation, technical measures must be established which ensure that:
• Only explicitly permitted traffic may pass through; all other traffic must be stopped
• At least two independent technical measures must be implemented so that persons outside the organisation cannot gain unauthorised access to and/or alter or erase personal health data and personal data.
• Traffic cannot pass directly from the outside in; all such external traffic must be initiated from the organisation’s systems.
• Logging must be initiated to ensure that rules are not broken; in the event of breaches, the channel must be closed until a new secure solution is in place.

5.5.3 Message exchange

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

The sender is responsible for:

• His own connection security which prevents unauthorised access and penetration.
• The service must not allow software that contains a virus, etc. to pass through.
• Secure transmission encryption end-to-end.
• Correct addressing.
• When necessary, the message or e-mail must be signed in such a way that the organisation cannot deny that it sent it.
• Breach reporting in connection with erroneous sending.
• Message or e-mail delivered in the agreed format.

The recipient is responsible for:

• His own connection security which prevents unauthorised access and penetration.
• Ensure secure transmission encryption end-to-end.
• When necessary, receipt must be logged so that the recipient cannot deny having received the message or e-mail.
• Breach reporting in connection with errors, i.e. receipt of message or e-mail which is not addressed to the organisation.
• Message or e-mail received in the agreed format.

The communication mediator is responsible for:

• Ensuring that the message or e-mail is delivered to the addressee only.
• Message or e-mail must not be altered or destroyed during transport from the sender to the recipient.
• Only the sender and the recipient must be able to read the message or e-mail.
• Message or e-mail must be delivered by the agreed deadlines following dispatch.
• Breach reporting in connection with all the above points.

5.5.4 E-mail, text and social media
The organisation must implement measures to prevent health data from being disclosed with the aid of e-mail, text or other unencrypted channels.

- Through technical and organisational measures, the organisation must ensure that e-mails do not contain identifiable personal health data and personal data.
- Logging must be initiated in order to check that rules are not being breached. Breaches of rules must be handled as a non-conformity and personnel-related consequences must be considered.

### 5.5.5 Internet connection

The organisation must implement the following measures:

- Technical measures which ensure that the internet service is logically separated from areas where personal health data and personal data are processed.
- Logging is initiated in order to check that rules are not being breached. Breaches of rules must be handled as a non-conformity and personnel-related consequences must be considered.

### 5.6 Digital communication with patients/health care users

In the case of digital communication with patients, organisations must be responsible for ensuring that:

- Consent is obtained from the patient/health care user to mediate personal health data and personal data electronically. Consent must be obtained in accordance with the relevant rules regarding consent. In accordance with this Code, the consent of the patient/health care user is the only basis for data communication with patients/users. The consent may be withdrawn at any time.
- If the patient/health care user has provided digital contact details, this may be deemed to constitute consent for the organisation to send appointment reminders by SMS. Moreover, the organisation must ensure that sufficient measures are implemented to ensure that messages are sent to the correct recipient in a SMS solution for reminders concerning appointments and other administrative information. Provision must be made to enable patients/health care users to notify the organisation if they do not wish to receive such messages. The overall information given in the message must be assessed on the basis of whether or not the overall content could result in a breach of the duty of confidentiality.
- Sufficient measures must be implemented to ensure that messages are sent to the correct recipient. The overall information given in the message must be assessed on the basis of whether or not the overall content could result in a breach of the duty of confidentiality.
- The patient/health care user must be uniquely identified.
- Technical measures must be implemented so that all communication is encrypted.
- Communication must not take place simultaneously with parties other than the specified patient/health care user.
- Personal health data and personal data must not be made available in such a way that the patient/health care user is dependent on storing the data on his or her own equipment in order to familiarise him-/herself with the information.
5.7 Suppliers and agreements

This section only refers to the contractual relationships that concern information security. It should be noted that the requirements in section 5.7 (with the exception of 5.7.2 Processor) will be extensively revised in the next version of the Code and should therefore be interpreted as indicative requirements.

A list is presented below of examples of communication parties where identifiable personal health data and personal data is exchanged and/or parties who have/are given access to equipment and/or software via which such information is processed. Written agreements must be established with such parties, unless stipulated otherwise. The agreements must include obligations which require the parties to fulfil the requirements and measures that follow from the Code for information security in force at any one time, as well as regulations concerning sanctions in the event of a breach of the Code and the agreement in general.

- Suppliers of communication services, e.g. the Norwegian Health Net (Norsk Helsenett).
  - For organisations within the sector which have undertaken through an affiliation agreement with Norsk Helsenett to comply with the requirements set out in this document, no specific agreement concerning information security will be necessary for communication via the health net.
- Processors who process personal health data and personal data on behalf of the organisation.
- Suppliers of equipment and/or software which require access for maintenance, troubleshooting, updating, via an online connection and/or physical attendance.
- Security providers.
- Supplier that the requirements under section 5.6 are met, no specific agreement is required with each individual patient/health care user.
- Students and research fellows who are not subject to the controller’s instruction authority

5.7.1 Suppliers of communication services

The supplier must have an independent responsibility for ensuring:

- that all affiliated organisations satisfy the requirements in this document, or for implementing technical measures which prevent affiliated organisations which do not satisfy the requirements from exposing personal health data and personal data held by other affiliated organisations to risk;
- that only organisations and/or services that have an agreement with the provider can gain access to the provider’s communication network;
- that communication packages, i.e. messages, e-mail, online communication, etc. are only transferred to a specified authenticated addressee;
- sufficient capacity and alternative communication paths are available so that the communication packages are available to the recipient as and when necessary (messages are delivered with stipulated deadlines, online communication takes place without interruption, etc.);
- that technical measures are established which ensure that communication packages are not altered, damaged, erased and/or disappear during transmission;
- that technical and organisational measures are established which prevent other parties from carrying out attacks via the provider’s communication network.
5.7.2 Processor

The processor has an independent responsibility for information security and for addressing data protection concerning data subjects.

The processor must only process personal health data and personal data in accordance with instructions from the controller the way in which the processor may process data on behalf of the controller must be regulated in an agreement.

5.7.2.1 Choice of processor

The controller may only use processors who provide adequate guarantees that it will implement appropriate technical and organisational measures which ensure that the processing fulfils the requirements of the Personal Data Act.

“Adequate guarantees” means that the processor fulfils the requirements set out in applicable laws and regulations, Chapters 3 and 4 of the Code and the requirements of the Code that are relevant to the contractual relationship concerned.

The processor must not engage subcontractors without the prior specific or general permission of the controller. If general, written permission is obtained, the processor must notify the controller of any plans to substitute subcontractors. The controller may object to such substitutions.

Specific conditions apply to processor agreements outside the EU/EEA. More information on this can be obtained from the Norwegian Data Protection Authority.

5.7.2.2 The processor’s subcontractors

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

Subcontractors have an independent responsibility regarding information security and for addressing data protection concerning data subjects. Subcontractors are subject to the same obligations as the processor under the processor agreement. This must be regulated in an agreement between the Processor and the Subcontractor.

5.7.2.3 Scope of processor agreements

Processor agreements can be either an independent agreement between the parties concerned or an integrated part of other contracts. The processor agreement must be written and may exist in digital form.

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

The agreement must state that the processor undertakes to fulfil the requirements of the Code.

The processor agreement must specify:

- The processor’s obligations
- The purpose of the processing of the personal health data and personal data
The processor agreement must regulate:

- Specific security measures
- On his own initiative, the processor must implement all measures that are necessary to ensure a high level of information security, including following the requirements of the Code.
- The processor must only be able to transfer personal data to another country in accordance with instructions from the controller.
- The processor must only authorise persons who are covered by a duty of confidentiality regarding the processing of personal health data and personal data.
- Requirements concerning the use of subcontractors (other processors).
- The controller must be granted right of access to ensure that applicable requirements are being complied with.

- The processor agreement must ensure stipulate that the processor is obliged to assist with/in:
  - technical and organisational measures to fulfil the rights of data subjects
  - relevant technical and organisational measures to ensure a high level of information security
  - reporting data protection breaches to the Norwegian Data Protection Authority
  - notifying data subjects of data protection breaches
  - documentation of completed relevant data protection impact assessments or the preparation of data protection impact assessments
  - advance discussions with the Norwegian Data Protection Authority
  - deleting or returning personal data in accordance with instructions
  - making available of all information which demonstrates that the obligations under the processor agreement have been fulfilled
  - contributing to security audits
  - assisting with regard to inspections
  - amendment of instructions from the controller which are in breach of the legislation

A processor which is also a supplier of a system or service which requires a data protection impact assessment must present such an assessment or assist in the preparation of such an assessment.

### 5.7.2.4 Processor’s overview of processing activities

The processor must maintain an overview of all categories of processing activities that are carried out on behalf of a controller. The overview must include:

- Name and contact details of the processor
- Name of the controller on behalf of which the processor is acting
- The controller’s data protection officer
- The categories of processing carried out on behalf of each controller
- Transfer of personal data to other countries
• Description of technical and organisational security measures
The overview must be written and may be digital.

5.7.2.5 The processor’s other obligations

If the processor processes personal health data and personal data from a number of organisations, the processor must ensure the following with the aid of technical measures which cannot be overridden by users:

• that partitions are established between the organisations in accordance with a risk assessment.
• that only the processor, those who work under the instruction authority of the processor and the organisations themselves have access to the organisation’s data.

The processor must notify the controller without delay of non-conformities relating to data protection security.

5.7.3 Suppliers

In order to safeguard the confidentiality, integrity and availability of personal health data and personal data, the organisation must ensure that:

• the supplier’s personnel have signed a confidentiality declaration which entails an absolute duty of confidentiality with regard to all personal health data and personal data;
• the supplier complies with the Code with regard to the controller’s obligations regarding security audits and non-conformity management;
• the supplier’s equipment that is used for an online connection via a communication network or supplied equipped which is connected to the organisation’s equipment has no malware which contains viruses, etc. and that the equipment is protected against access by unauthorised parties;
• the supplier may only gain access with the special permission of the organisation in each individual case, and to the devices for which there is a need;
• all access must be monitored by the organisation’s personnel;
• availability of personal health data and personal data must insofar as is possible be maintained when the supplier performs work on the organisation’s equipment/software, so that the organisation is able to continue performing its tasks.

5.7.4 Security providers

The controller must establish the necessary security measures. A possible alternative to the inhouse establishment of security measures is to outsource security tasks to a supplier where the delegation of tasks between the organisation and the supplier collectively satisfy the requirements of the Code. A security provider may for example perform the tasks in Chapter 5.7.2 or other parts of the Code.
An agreement must be established with the security provider concerning the performance of specific security tasks which regulates the following:

- The security tasks that are covered and the delegation of responsibility for these tasks.
- Description of the supplier’s solution in the form of a configuration chart.
- Documented risk assessment which demonstrates that the organisation’s level of risk is acceptable, and that the security level stipulated in the Code has been established.

The security provider must comply with the requirements of Chapter 5.7.2.

### 5.7.5 Collaboration between organisations concerning personal health data and personal data filing systems for therapeutic purposes

Two or more organisations may collaborate concerning a joint personal health data and personal data filing system which replaces the organisations' internal records. The organisations must then enter into a written agreement concerning:

- the scope of the collaboration;
- the way in which the rights of patients and health care users are addressed;
- the way in which the health data is to be processed and protected, including in connection with changes or termination of the collaboration;
- the data processing responsibility.

The organisation(s) that have actual control over and responsibility for the processing are the controller(s). If all the organisations are controllers, a representative may be appointed to act as a contact person for enquiries from patients and/or health care users.

When a municipality and one or more private service providers which provides services on behalf of the municipality begins using a joint personal health data and personal data filing system in order to fulfil the recordkeeping obligation, the municipality must be the controller, because the authority determines the purpose and use of the joint personal health data and personal data filing system.

Collaboration concerning a joint personal health data and personal data filing system opens up the possibility of using a personal health data and personal data filing system for therapeutic purposes when two or more organisations work together to provide health and/or care services, corresponding to the previous cross-organisational health record in a formalised working partnership. The Regulation on cross-organisational health records in a formalised working partnership (*Forskrift om virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap*) has now been repealed, but organisations which have entered into an agreement in accordance with this Regulation may continue their partnerships.
5.7.6 Access to health data across organisations

Access to health data may be established across organisations. ‘Access’ means that health personnel within an organisation are given access to directly electronically retrieve health data concerning patients/users registered via another organisation.

The rules concerning access across organisations that are referred to here do not apply to access to health data across organisations which collaborate concerning a common personal health data and personal data filing system for therapeutic purposes; see Chapter 5.7.5.

The Regulation on access to health data across organisations (*Forskrift om tilgang til helseopplysninger mellom virksomheter*) stipulates that the organisations must enter into an agreement concerning access to health data across organisations.

The agreement must be written and stipulate at least the following:

- the scope of the agreement
- the need and risk assessments that form the basis for the agreement
- the personal health data and personal data filing systems for therapeutic purposes, parts of data filing systems or types of data that the agreement covers
- routines and delegation of tasks in order to fulfil the requirements of the Regulation.

Before access is given to health data across organisations, both the organisations concerned must carry out a risk assessment to ensure that the patient's/health care user's data protection rights are addressed. The risk assessments must at least cover the risk of breaches of the duty of confidentiality and weakened information security.

5.8 Handling of information security breaches

5.8.1 Breach management

The organisation’s management, or the body that the management authorises, must process breaches with the aim of restoring normal status, eliminating the cause of the breach and preventing reoccurrence.

The processing of breaches must be initiated in the event of a security breach and/or when the processing of personal health data and personal data has been carried out in breach of applicable regulations, guidelines or procedures. Breach processing may also be initiated in the event of the absence of procedures or if procedures are inappropriate.

- Every employee is responsible for reporting any breach that are discovered using a set form to their immediate superior or another designated person/body.
- For each reported breach, the factual sequence of events must be collated, and an assessment must be carried out as a basis for the implementation of corrective measures.
- Measures and possible alternative measures must be proposed with a description of a plan for implementation for restoring normal status and preventing reoccurrence.
- Measures and a plan at a feasible level must be adopted. The measures must prevent or reduce the probability of reoccurrence.
• Measures must be implemented in accordance with the plan, with reporting to the organisation’s management or the body authorised by the management.
• A status report must be submitted to the organisation’s management or the body authorised by the management, which documents the results of the breach processing.
• In the event of repeated breaches, a new risk assessment must be carried out.

Systems for breach management must be able to handle messages concerning breaches even if they had neither actual nor potential adverse consequences for an identified patient.

In the event of a breach of data protection which has consequences for the data subject, the controller must report the breach to the Norwegian Data Protection Authority within 72 hours after becoming aware of it. If the breach is reported later, the reason for the delay must be stated. Breaches which have not had any consequences for the data subject need not be reported.

The notification to the Norwegian Data Protection Authority must state:

• a description of the data protection breach, including the
  o categories of data subjects affected
  o approximate number of data subjects affected
  o types of personal data that the breach concerned
• name and contact details for the data protection officer or other contact person from whom more information can be obtained
• description of the likely consequences of the breach
• description of the measures that the controller has implemented or is proposing to implement in order to manage and reduce any adverse effects of the breach.

Notifications to the Norwegian Data Protection Authority may be given in stages if it is not possible to provide all information at the same time.

5.8.2 Notification of data subjects

Data subjects must be notified if the breach has resulted in the erasure, alteration or unauthorised disclosure/access to personal health data and personal data.

The notification must include:

• Description of the breach in clear language
• The contact details of the data protection officer or another role who is able to provide more information
• Description of the consequences of the breach.
• Description of completed or planned measures to manage and reduce the adverse effects.

It will not be necessary to notify the data subject if:

• Technical and organisational security measures have been implemented regarding the personal data that was affected by the breach, e.g. measures which render the data unreadable.
• Retrospective measures have been implemented which mean that it is unlikely that the breach has resulted in unintended or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data.
• If giving notification would entail a disproportionate effort (e.g. because the breach involves a large number of individuals), the general public may be informed so that the data subject is still notified in an effective manner.

5.9 ICT readiness

The lack of availability of personal health data and personal data can have adverse implications for both the organisation and the organisation’s users. The organisation must therefore ensure that essential personal health data and personal data will continue to be available in the event of the shutdown of all or part of an electronic information system.

In order to establish the measures necessary to safeguard availability in the event of a shutdown, the organisation must review each information system with regard to criticality. Criticality must be assessed for both the organisation itself and its users. The systems and associated personal health data and personal data which the organisation uses must be classified:

• Systems where the non-availability of a service could be critical, e.g.
  o life-threatening for a patient
  o critical for the organisation’s operation
• Systems where the non-availability of a service could have severe consequences, e.g. it could result in:
  o the incorrect treatment of a patient
  o considerable additional work for personnel
  o loss of efficiency
  o lost revenues for the organisation
• Systems where the non-availability of a service could weaken the patient’s trust.
• Systems where protracted non-availability could be accepted.
• Low priority systems.

A review must also be carried out to determine which other systems the classified systems are dependent on. These must have the same classification and acceptable level of risk as the critical systems.

For each classification, the management must determine an acceptable level of risk for availability, in the form of at least a maximum period of non-availability.

The organisation must establish emergency procedures based on the classification of the information systems:

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

These procedures must be tested at least annually.

In accordance with the classification referred to above, the organisation must consider establishing an alternative solution which will ensure the continuity of the information systems in the event of an operational shutdown.
6 Appendices

6.1 Definitions

Words and expressions that are defined below are written in italics in the Code. No rights or obligations must be deduced from the definitions alone. They must be considered in the context in which they are used in the Code.

"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 all operations.

"Warning" means, for the purposes of this Code, a written reprimand from the organisation to an employee who has breached procedures, etc. It must be clearly stated that the notification is a warning and a statement must be given of the reason for the warning and the possible consequences of further breaches of procedures, etc.

"Acceptable risk" means, for the purposes of this Code, the level of risk that the sector can accept as regards the occurrence of incidents which could result in a breach of confidentiality, availability or integrity of personal health data and personal data. The magnitude of risk will depend on the probability of an incident occurring and the consequences of such an incident. The Code describes what constitutes an acceptable level of risk in the sector. Each individual organisation must perform a specific assessment of how it will achieve an acceptable level of risk.

"Anonymised" means, for the purposes of this Code, personal health data and personal 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 and personal 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.

"Authorise/authorised/authorisation" means, for the purposes of this Code, that a person in a certain role may be given or has been given specific rights to read, register, correct, erase and/or block personal health data and personal data. Authorisation may only be given if it is necessary for the work of the person concerned, where it is justified on the basis of an official need and in accordance with provisions concerning duty of confidentiality.

"Breach" means, for the purposes of this Code, any processing of personal health data and personal data that is not in accordance with applicable regulations, guidelines and/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.
“Processing” means, for the purposes of this Code, any operation or series of operations which is or are performed on personal data, whether automated or not, e.g. collection, registration, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure through transfer, distribution or any other form of disclosure, compilation or coordination, limitation, erasure or destruction.

“Nature of the processing” means, for the purposes of this Code, the organisation’s specific types of processing activities.

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

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

“Biometric data” means, for the purposes of this Code, personal data that originates from specific technical processing linked to a natural person’s physical, physiological or behavioural characteristics, which enables or verifies a unique identification of the said natural person, e.g. facial images or fingerprint data.

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

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

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

“Electronic patient record” means, for the purposes of this Code, an electronically managed collection or collation of recorded/registered information concerning a patient in connection with the provision of health and social care services; see also Section 40 first paragraph of the Health Personnel Act and Section 3(a) of the Regulation on health records.
This includes both somatic and psychiatric records, etc., either separately or collectively. See also “personal health data and personal data filing system for therapeutic purposes”.

“Electronic patient record system (EPR system)” means, for the purposes of this Code, an electronic system which has the functionality necessary to record, retrieve, communicate, correct and erase data in an electronic patient record system (EPR). This includes radiology systems, systems for somatic and psychiatric records, patient administration systems and other systems containing health data.

“Data processing system” means, for the purposes of this Code, an application or IT system which processes personal health data and personal data. The term “system solution” is also used to refer to a data processing system. Examples of data processing systems are care systems, health centre systems and child service systems. Data in different data processing systems can comprise electronic patient records (EPR) and other service documentation.

“Joint personal health data and personal data record system” means, for the purposes of this Code, a collaboration between two or more organisations concerning a personal health data and personal data filing system for processing purposes that is intended to replace the organisations’ internal records; see Section 9 of the Patient Records Act.

“Administrative agency/public administration” means, for the purposes of this Code, any central or local government body. A private legal person must be considered an administrative agency in cases where such a person makes individual decisions or issues regulations; see paragraph1 of the Public Administration Act.

“Genetic data” means, for the purposes of this Code, personal data concerning a natural person’s inherited or acquired genetic characteristics which provide unique information concerning the physiology or health of the natural person concerned, often generated through the analysis of a biological sample taken from the natural person concerned.

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

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

“The Norwegian health net” means, for the purposes of this Code, the network that is provided by Norsk Helsenett SF.

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

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

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

"Indirectly identifiable personal health data and personal data" means, for the purposes of this Code, personal health data and personal data from which names, dates of birth and national identity numbers and other information which may serve to identify an individual has been removed, such that the data can no longer be linked to a specific individual, and where the identity of an individual only can be traced by combining the data with the specific information that has been removed (see paragraph 2(b) of the Personal health data and personal data Filing System Act). To be considered indirectly identifiable personal health data and personal data, the data must have been processed to appear anonymous in the absence of any serial number.

"Integrity" means, for the purposes of this Code, that personal health data and personal data must be secured against unintended or unauthorised amendment or deletion and that such data must be correct, up to date, relevant and adequate for the purposes of providing medical care.

"Internal 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 according to the requirements specified in, or pursuant to, existing legislation.

"Categories of processing", see “nature of the processing”.

"Categories of data subjects" means, for the purposes of this Code, that persons are categorised into groups and sub-groups. For examples, persons according to: patient, health care user, employment, cause of death, disability, nationality, year, place of birth or upbringing, etc.

"Kjernejournal/Core record" means, for the purposes of this Code, the Norwegian National summary care record. This is an electronic centralised multi-organisation personal health data and personal data filing system for processing purposes in which a limited set of relevant personal health data and personal data necessary for the provision of proper health care is collated in a filing system/register; see paragraph 13 of the Patient Records Act and the Regulation concerning the Summary Care Records (Forskrift om nasjonal Kjernejournal).

"Re-identification key" means, for the purposes of this Code, a unique personal code which allows the re-identification of an individual from a file containing indirectly identifiable personal health data and personal data concerning health.

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

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

"Configuration" means, for the purposes of this Code, the information system’s design, including both technical equipment and software.
"Configuration change" means, for the purposes of this Code, a change in the construction of the information system as a result of the installation, upgrading or removal of equipment or software.

"Storage device" means, for the purposes of this Code, a device for storing personal health data and personal data electronically.

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

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

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

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

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

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

"Patient data", see personal health data and personal data.

"Personal qualified certificate" means, for the purposes of this Code, two-factor authentication where one factor is dynamic, based on qualified certificates and which in all respects satisfy the requirements for security level 4 in the “Framework for Authentication and Non-repudiation in Electronic Communication in and with the Public Sector”.

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

"Personal data security" means, for the purposes of this Code, technical and organisational measures which have been implemented in order to safeguard the data protection rights of individuals.
"Data protection impact assessment" means, for the purposes of this Code, a systematic process which identifies and evaluates potential data protection consequences from the perspective of all stakeholders in a project, initiative, proposed system or process.

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

"Report on processing activities" means an overview of processing activities in accordance with the provisions of Article 30 of the General Data Protection Regulation.

"Pseudonymisation" means, for the purposes of this Code, the processing of personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, provided that the mentioned additional data is stored separately and covered by technical and organisational measures, which ensure that the personal data cannot be traced to an identified or identifiable natural person.

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

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

"Consent" from the data subject means, for the purposes of this Code, any freely given, specific, informed and unambiguous indication of the data subject's wishes where the person concerned gives their consent through a statement or clear confirmation of the processing of his/hers personal data for given purposes.

"(The) sector" means, for the purposes of this Code, the healthcare services or one or more parts thereof.

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

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

"Secure authentication system" means, for the purposes of this Code, an authentication system which, for example, is based on the use of personal qualified certificates or any other authentication system that through a risk assessment has been shown to provide adequate security.
"Confidentiality" means, for the purposes of this Code, a statutory or agreed obligation to prevent others from accessing or gaining knowledge of personal health data and personal data, see paragraph 21 of the Health Personnel Act, paragraph 17 of the Personal health and personal dataFiling System Act, paragraph 15 of the Patient Records Act, paragraph 12-1 of the Healthcare Services Act, paragraph 6-1 of the Specialist Health Service Act and Section 13 to 13(e) of the Public Administration Act, in addition to other information pertinent to information security. The duty of confidentiality includes both a passive obligation to remain silent and an obligation to actively prevent unauthorised persons from gaining knowledge of confidential data.

"Technical measures" means, for the purposes of this Code, measures of a technical character that may not be influenced or circumvented by employees, and that are not restricted by actions that individuals are assumed to perform. Examples of such measures include authentication via a personal qualified certificate or the configuration of a firewall such that it only permits specific data traffic or a message service that is designed in such a way that all messages are automatically encrypted.

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

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

"Service documentation" means, for the purposes of this Code, documentation for planning, mapping, follow-up and information exchange concerning a service recipient’s application, practical and medical problems, needs, resources, medical assistance, assistive aids, etc. Together with the electronic patient record (EPR), the service documentation constitutes the documentation required by the Health Personnel Act, etc.

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

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

"Unlawful access" means, for the purposes of this Code, a violation of the prohibition on reading, searching or otherwise acquiring, using or possessing personal health data and personal data without any basis in the provision of medical assistance to the patient, the administration of such assistance or specific authorisation in legislation or regulations. See
paragraph 18 of the Personal health data and personal data Filing System Act, paragraph 16 of the Patient Records Act and paragraph 21(a) of the Health Personnel Act.

"Subcontractor" means, for the purposes of this Code, an organisation which enters into a contract to fulfil some or all of the obligations in a processor’s agreement.

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

"Multi-organisational patient record" means, for the purposes of this Code, a personal health data and personal data filing system for the purposes of processing wherein healthcare personnel and personnel providing healthcare services pursuant to the Healthcare Service Act, record or register information concerning patients and users; see paragraph 39 and 40 of the Health Personnel Act.

6.2 Supporting documents

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

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

The illustration shown below shows this principle:
6.2.1 Fact sheets

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

6.2.2 Guidelines

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

6.2.3 Templates

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

6.3 References

Specification of requirements for PKI in the public sector: (https://www.regjeringen.no/no/dokumenter/kravbeskrivelse-for-pki-i-offentlig-se/id611085/)

NSM's recommendations regarding cryptosolutions: kortliste-krav-til-krypto


Framework for Authentication and Non-repudiation in Electronic Communication in and with the Public Sector: https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/

Website for the Code of conduct for information security in the healthcare and care services sector: https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

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

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

The Agency for Public Management and eGovernment's website: https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet
Norwegian Data Protection Authority: https://www.datatilsynet.no/


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

European Commission’s Article 29 group: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

6.4 History of the Code

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

The increasing proportion of electronic data processing is opening up new opportunities, but it is also creating challenges relating to information security amongst the organisations involved. Among other things, electronic processing enables data to be made available easier and faster both internally within an organisation and externally outside the organisation. This is an advantage, if the data is only made available to the right people at the right time. However, unintended consequences can arise regarding data confidentiality, and specific measures must be implemented to ensure that unauthorised persons do not gain access to electronically stored data. Mechanisms are needed to enable everyone involved to be confident that every aspect of information security has been satisfactorily addressed by the organisations concerned.

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

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

28 June 2006

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

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

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

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

In June 2009, the Norwegian Parliament (Stortinget) amended the Personal health data and personal data Filing System Act. This facilitated the adoption of regulations concerning:

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

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

2 June 2010

SECOND EDITION, VERSION 2.1

On 29 November 2012, the steering group for the Code decided to amend the requirement for security level 4 in order to permit alternative solutions, on the condition that a risk assessment documents and confirms that any such alternative solution provides an adequate level of security.

THIRD EDITION

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

FOURTH EDITION

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

**FIFTH EDITION**

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

**FIFTH EDITION, VERSION 5.1**

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

**FIFTH EDITION, VERSION 5.2**

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