QUICK GUIDE FOR PROCESSING HEALTH AND PERSONAL INFORMATION

WHEN USING WELFARE TECHNOLOGY

National Welfare Technology Program

KS NORMEN Direktoratet for e-helse Helsedirektoratet

Version 2 - December 2019

INTRODUCTION

Target group

This guide is for those of you who work with welfare technology in the municipal health and care service, and who have gained experience and basic knowledge in this area. It is recommended that you have familiarized yourself with Roadmap for service innovation and that one has read Quick guide to welfare technology .

The purpose of the guide

In order to be able to provide sound health and care services, it is crucial that correct and up-to-date information about patients and service recipients is available in the right place at the right time. Healthcare professionals must have confidence that the information is correct and complete, and the health and care service depends on the trust of the population for patients, users and relatives to dare to share sensitive and personal information with the services.

To ensure this, the data controller (municipality) must ensure that the information is safeguarded, used and **treated in a safe manner.** Furthermore, it must be ensured that relevant and necessary information is available to those who are to have access to it, and that the information is correct. It must be ensured that the information does not go astray and that unauthorized persons do not gain access to it.

Without satisfactory processing of relevant and necessary information, it is not possible to provide good quality health and care services.

This guide addresses issues and topics within the use of welfare technology in the provision of health and care services, especially with regard to **processing of health and personal data.**

Work with privacy and **information security** must be anchored at a sufficiently high level in the organization. Everyone is responsible for participating in training and change processes in the company.

With the introduction of welfare technology, many municipalities face challenges that affect the processing of health and personal data. Although processing and health and personal information is not new within the health and care service, the challenges may be experienced as greater and different than before. There are several reasons for this:

- The use of welfare technology generates a lot of information about patients and users, and it must be considered whether the storage of the information is relevant and necessary for the provision of services. This places demands on knowledge of the duty to document, including the duty of confidentiality and exceptions from this.

- There are many actors involved in the processing of the information, and information is shared with various actors such as alarm centers / response centers, technical units and communication and equipment suppliers. m.fl. This requires knowledge of roles and responsibilities in the processing of information, including requirements for confidentiality, the need for data processor agreements, etc.

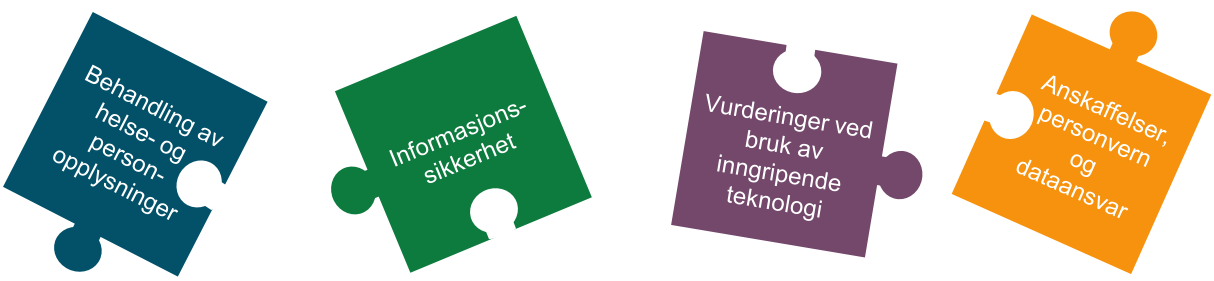
- New personal data law, which makes the EU Privacy Regulation (GDPR) to Norwegian law, has given an increased focus on privacy and the rules for processing health and personal data. It has also led to some new requirements. The regulation requires i.a. that a privacy impact assessment (DPIA) is carried out when introducing technology that involves the processing of health and personal data. A written overview (protocol) of the processing of the information must also be kept.

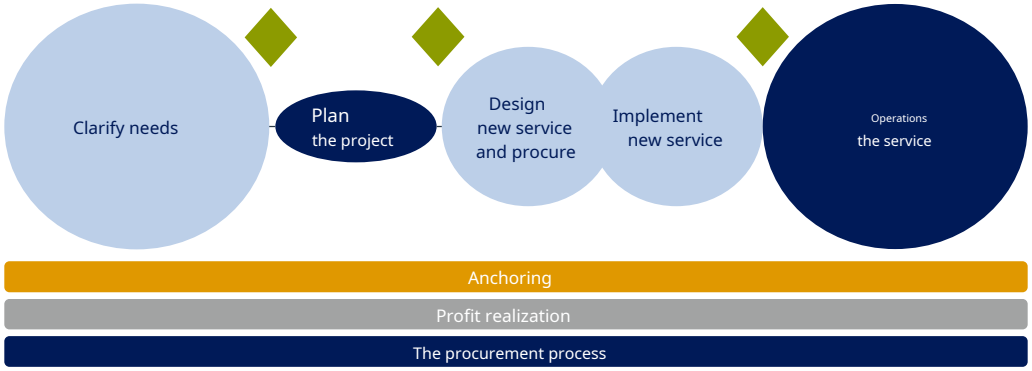
- Several welfare technology solutions provide the opportunity for control or monitoring of the user. This requires knowledge of the regulations regarding the use of intrusive technology.

Each chapter has suggestions for assessments and tools - in the same sense as tools in «Roadmap for service innovation».

The guide has been developed by a working group with members from the Norwegian Directorate of Health, the Norwegian Directorate for e-Health, Normen and PA Consulting

The Quick Guide is an aid to using welfare technology in a correct, safe and secure way.





IMPORTANT TASKS IN THE VARIOUS PROJECT PHASES DESCRIBED IN THE QUICK GUIDE TO WELFARE TECHNOLOGY

The "Quick Guide to Welfare Technology" describes five phases for the introduction of welfare technology (illustrated in the figure at the top of the page). This chapter describes activities and assessments related to the processing of health and personal data in each of these phases.

Clarify needs

In the needs phase, it is important to clarify roles and responsibilities, for example:

- Is there the right competence in the project? If not, you must obtain it, either from the municipality's own resources or from outside.
- Make an overview of the service's processing of information. What information should be processed, and who should process the information?

Plan the project

When planning the project and establishing a project and steering group, it is important to involve the right resources in privacy and information security, such as:

- Privacy Officer
- Legal expertise
- IT and security
- Cooperation with the county governor
- Existing networks, such as other municipalities in the National Welfare Technology Program

Design new service

During the design phase, the new service is designed with routines and guidelines. Here it is important to think about the following related to the processing of health and personal data:

- Make a risk assessment before new solutions are
- used. Carry out a privacy impact assessment
- Implement measures as identified in risk assessment and privacy impact assessment
- Describe any need for built-in privacy in procurement, configuration / setup and testing of new technical solutions.
- Consider storage time for information
- Make sure you have routines for following up logs

Implement new service

In this phase, the focus is on implementation plans and training of users and personnel. It is about being prepared for the transition to operation, also with regard to privacy and information security:

- Update the information security management system
- Update the overview of personal information Plan and
- carry out training of users and personnel
- Establish access control

Operate the service

When new technology and new services are put into operation, the services must still be followed up and further developed. This applies not least with regard to the processing of health and personal data:

- Implement continuous measures for information security
  - Secure data communication
  - Update the configuration overview
  - Follow up logs
  - Maintain access control
- Carry out non-conformance treatment
- Carry out follow-up by supplier

Tool

- E-Health: Template for data processor agreement
- The norm: Supervisor in information security when using welfare technology
- The standard fact sheet 15: Logging and follow-up of logs
- The Norwegian Data Protection Authority: Risk assessment of information systems
- Difi: Information security and privacy in ICT procurements

PROCESSING OF HEALTH AND PERSONAL INFORMATION

This chapter describes how health and personal data must be processed legally. Examples of personal information are health information in medical records, registers, professional systems, research, etc. See, among other things, "Important about consent" in a later chapter.

Legal treatment

The municipality shall have knowledge of and an overview of which personal data the municipality processes, why they are processed and how.

All processing of health and personal data must have a legal basis. The Personal Data Act sets out various bases for the legal processing of health and personal data.

The basis for processing must be identified before the processing of health and personal data begins, or in the event of changes in the processing. The treatment basis must cover all the treatments performed; collection, registration, storage, deletion, delivery, etc.

When processing information that is relevant and necessary for the provision of sound health and care services to the individual, it is *"Necessary for the fulfillment of a legal obligation"* which is the relevant basis for treatment.

If welfare technology is used in arenas other than the health and care service, any sector legislation must be considered.

Built-in privacy

New solutions that are developed in the health and care sector must have built-in privacy. This means that privacy considerations must be taken into account in all stages of the development and implementation of new solutions. The data controller must ensure built-in privacy.

Read more on the Data Inspectorate's pages, and set requirements for built-in privacy in products and solutions.

Other obligations when processing personal data

When a data processor is to handle personal data on behalf of the data controller, one must be created data processor agreement.

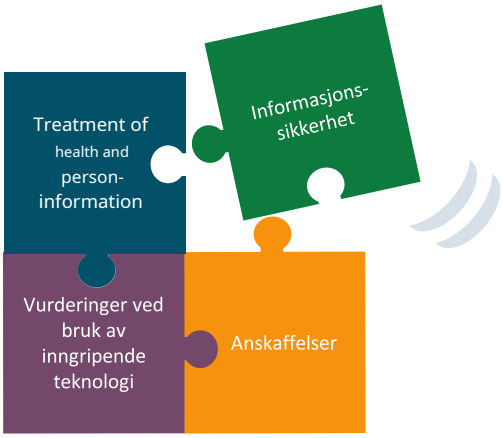
The company must have a written overview of the processing of personal data - «Protocol of processing activities». If the company is to conduct research, either alone or in collaboration with others, it is important to familiarize yourself with the regulations on how health and personal data are to be processed for this purpose. These rules are different from the regulations on the processing of information when providing health and care services. It is important to have established a legal basis for using personal data for research purposes; this can e.g. be consent or decision on dispensation from the duty of confidentiality.

Assessments

- Does the municipality know which personal data is processed, as well as how and why it is processed? Has
- a written overview of the processing of personal data been created?
- Is there a legal basis for the processing of personal data
- Does the municipality have routines for detecting and dealing with deviations?

Tool

- Fact sheet of the standard 8: Deviation treatment
- Norms fact sheet 13: Protocol on processing of health and personal data in the company
- The norm's guide for research
- The norm's guide for privacy in small health businesses
- The Data Inspectorate: Built-in privacy



INFORMATION SECURITY

The Personal Data Act states that the data controller must have "appropriate organizational and technical security measures" to prevent breaches of security. Violations are defined as unintentional or unlawful destruction, loss, alteration, unlawful disclosure of or access to personal information.

The choice of suitable security measures shall be made on the basis of the scope and category of information, patient safety, current risk picture, etc. The measures must be selected based on
risk assessments, and be proportionate based on identified risk.

Risk assessment

When new solutions are developed and put into operation, it is important to get an overview of the risk picture and the need for measures. The municipality must therefore carry out risk assessments to map the probability of, and possible consequences of, undesirable events.

The risk assessment forms the basis for further assessments, measures and decisions on:

- Whether a welfare technology solution should be used
- How personal data is to be processed
- What measures are to be implemented

Risk assessment of welfare technology must be made on the basis of several aspects. Here are some examples:

Availability

- Assessment of technical solution and availability of health and personal information
- Assessment of coverage of wireless networks
- Assessment of vulnerability to destructive software

Integrity

- Access control to prevent unintentional change of health and personal information
- Adequate training to prevent user errors
- Other risks of incorrect health and personal information (for example due to equipment and software defects)

Confidentiality

- Personal information lost
- Remote access solution for supplier
- Use of tablets (eg exposure of information via Internet-based medical devices) distance follow-up)

Privacy Impact Assessment

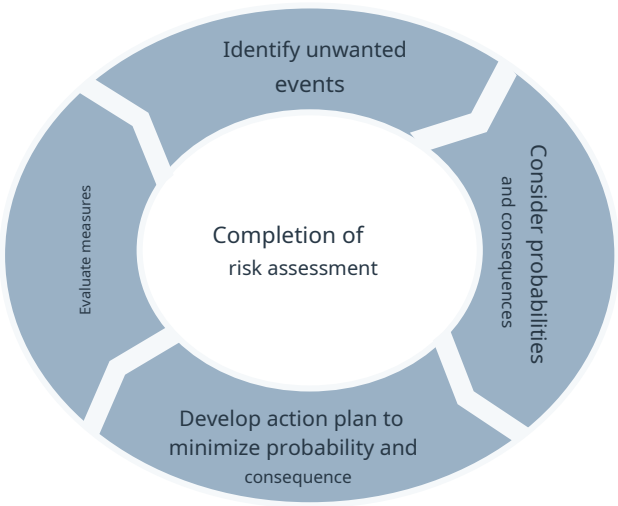
If it is probable that the processing of personal data entails a high risk for the data subjects, the municipality shall carry out a privacy impact assessment, also called DPIA. More about this in a separate chapter.

Deviation treatment

Carrying out a risk assessment and establishing measures will never be able to prevent all undesirable events. Adverse events occur and fractures are detected. When this happens, the company must systematically register, handle and follow up the discrepancy.

Tool

- The norm's guide in information security when using welfare technology
- The norm's guide in privacy and information security - medical equipment
- Standard Fact Sheet 7 - Risk Assessment
- Standard Fact Sheet 13 - Protocol
- The Data Inspectorate's guidance in information security



PROCUREMENT, PRIVACY AND DATA RESPONSIBILITY

Dialogue with suppliers

Prior to the requirements specification being sent out, there should be a dialogue with the supplier as part of the preparatory work to specify requirements and measures related to information security.

Requirements for suppliers when purchasing equipment or services

Suppliers of technology to the municipality are not independently responsible for the technology meeting the requirements of the legislation. The municipality must therefore set requirements for the supplier regarding compliance with regulations in requirements specifications, agreements, etc. and ensure that the solution is documented. The norm is a good tool here.

The municipality must also make demands on the supplier **built-in privacy.** This means that privacy and information security must be taken into account in all phases of the development of welfare technology. Predefined default settings should be set to the most privacy-friendly level.

When it comes to purchasing services, the requirements will vary with the scope of the services. More comprehensive requirements will be set for the purchase of an entire value chain compared to the purchase of service equipment.

Risk assessment at acquisition

A complete risk assessment of the specific offer must be carried out. The risk assessment shall provide answers to which measures may need to be implemented, and whether the identified risk can be sufficiently reduced with these measures so that it falls within the company's acceptable risk.

Data controller and data processor

Data controller (in the Privacy Ordinance this is called *treatment manager)* is the one who decides the purpose of the processing of the information - and which aids are to be used. Aids here means system, method of storage and transmission, etc. Data controller for processing information in the municipal health and care service is the municipality.

The data processor (supplier, response center or others) is the person who processes personal data on behalf of the data controller. This relationship must be regulated in a data processor agreement.

When the municipality uses a supplier for an assignment, this supplier will not necessarily be a data processor. It is only when the supplier has to treat health and personal information on behalf of the municipality that there is a data processor relationship. If the supplier e.g. only access to information but not to process it, a confidentiality statement will suffice.

Assessments

- Should a dialogue be held prior to procurement?
- What are the requirements for built-in privacy?
- Should a data processor agreement be established?

Tool

- Template for data processor agreement (directorate for e-health)
- The norm's guide in information security when using welfare technology
- The norm guides in the use of cloud services for the processing of health and personal data
- Normen's Fact Sheet 6b - Safety audit - checklist to meet the requirements of the Norm
- Standard fact sheet 10 - Use of data processor
- The standard fact sheet 38 - Safety requirements for systems
- The standard fact sheet 46 - Data responsibility and agreements in connection with service outsourcing
- The Data Inspectorate's guide on data controller and data processor
- The Data Inspectorate's guide for data processor agreements
- The Data Inspectorate's principles for embedded privacy
- Quick procurement guide (coming)

ASSESSMENTS WHEN USING INTERVENTION TECHNOLOGY

The municipality is largely free in terms of how it is to fulfill the "provide for" responsibility in the Health and Care Services Act § 3-1 first paragraph, as long as the services offered fulfill the patient's or service recipient's right to necessary and justifiable services. It is basically up to the municipality to assess whether a service offer should include welfare technology. However, the recipient of the services has the right to participate in the design of the service offer.

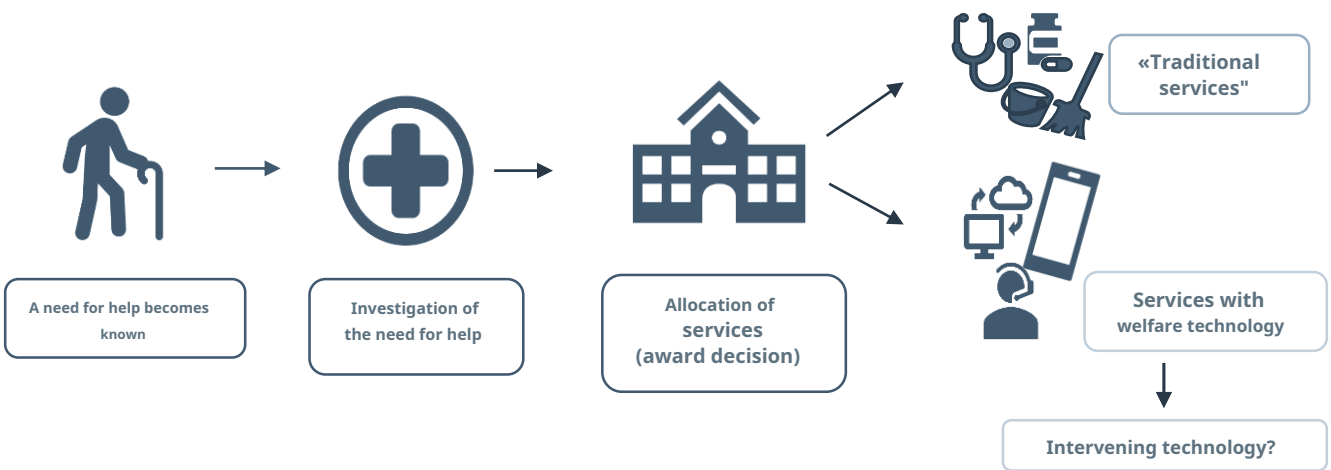
If the municipality comes to the conclusion that it is relevant to offer welfare technology, it must be considered whether the technology is intrusive. Intervening technology is all tracking, alerting, locating and monitoring technology that sends information to a third party about the patient's or user's actions, movements, whereabouts, etc. without the patient or user initiating it.

If the technology *not* is intrusive, ie that it *not* sends information about the patient / user to a third party without the patient / user initiating it themselves, there is no need for any other legal basis than the - usually implicit - consent that forms the basis for the health care / services, alternatively a decision by responsible personnel according to the rules in the Patient and User Rights Act § 4-6 if the patient / user lacks consent competence.

If the technology *is* intervening, it must be considered which legal basis is relevant, and whether a decision must be made (see *Welfare Technology's ABC booklet C, Legislation and ethics).*

Tool

- The Norwegian Directorate of Health's guide for case processing of services in accordance with the Health and Care Services Act
- The ABC of Welfare Technology - Legislation and Ethics



IMPORTANT ABOUT CONSENT

Legal basis for the provision of health and care services

- Consent, most often implicit, is the basis for the provision of health and care services to persons with consent competence.
- If the person is not competent to give consent, the decision is made on the provision of health and care services by the service personnel, based on legal authority and / or illegal law.
- In the event of resistance, mental retardation or the use of intrusive technology, decisions must be considered.

Legal basis for treatment of health and personal information

- The duty to document and the duty to e.g. Ensuring sound services is the legal basis for processing necessary and relevant information when providing health and care services.
- Processing of information beyond this may require consent.

QUESTIONS ASSENTS CURRENTLY INDOOR AREAS HEALTH AND THE CARE SERVICE

1. Provision of health and care services

Health and care services can in principle only be provided when the service recipient agrees to this. For health care, this follows from the Patient and User Rights Act § 4-1, but it also applies within the care services based on illegal law and general legal principles.

The starting point is that this consent is given implicitly:

- A person who through his behavior shows that he or she cooperates in the provision of health and care services is considered to have given his or her consent (*implicit consent).*
- The consent must nevertheless be informed, ie that the person must have received sufficient information about the offer / service to know what he or she "participates in".
- In the case of implicit consent, it is not necessary to have declarations of consent read and signed

For persons who have consent competence, the above applies whether the services are provided with or without welfare technology, including intrusive technology.

If the patient / user is considered to *not* be consent competent, the implied consent must be replaced with *another legal basis.* The following legal provisions may then be relevant:

- the Patient and User Rights Act § 4-6
- the Patient and User Rights Act § 4-6a
- the Patient and User Rights Act, Chapter 4A
- the Health and Care Services Act, Chapter 9

2. Processing of health and personal data

The legal basis for the processing of relevant and necessary health and personal data in the health and care service is the duty to document and the duty to ensure that the services offered and provided are justifiable.

This means:

- As long as the processing of health and personal data is *necessary and relevant for service provision / administration* must consent not used as a legal basis.
- The processing of health and personal data as mentioned under the first bullet point for internal company quality assurance does not require consent either.

If it is to be treated *more / other information* than what is necessary and relevant for the provision and administration of health and care services, a new basis for treatment must be considered. It may be that consent will be the basis, and then it must be obtained.

If the information is to be processed *for other purposes* than the performance and administration of health and care services to the individual or internal quality assurance, the basis for treatment must also be reconsidered. If the basis is to be consent, it must be obtained. This may, for example, apply if the information is to be used for research.

Tool

- The Health Personnel Act - documentation obligation
- The Welfare Technology's ABC - booklet C: Legislation and ethics
- Supervisor for case processing

MORE ABOUT PRIVACY IMPACT ASSESSMENT (DPIA)

The data controller (municipality) has a duty to carry out an assessment of privacy consequences before the processing of health and personal data begins, when it is probable that the processing will entail a high risk for the rights and freedoms of natural persons (in accordance with Article 35 of the Privacy Regulation, GDPR).

The use of welfare technology in health and care is an activity that can entail a high risk for the data subjects' rights and freedoms. One should especially consider whether the activity involves:

- Systematic monitoring
- Innovative use of technological solutions
- Information on vulnerable data subjects
- Registration of sensitive information

INSTRUCTIONS FOR IMPLEMENTING THE PDDPIA

Systematic description of the treatment

Here you go systematically the work and describe including:

- What types information is collected in?
- How to proceed the collection?
- Who is registered, how many and how often?
- What is the purpose of the registration?

The description must be complete, clear and specific.

Must and proportionality

Here you ensure the quality of the processing of health and personal data is necessary, that there is a legal basis and that there is compliance between the legal basis and the purpose of the processing of health and personal data.

As part of this, an assessment must be made of the legal basis / legal basis, and whether the purpose is clearly defined.

Risk for those registered rights names and freedoms

In this phase one must conduct an assessment of privacy implications.

With privacy implications mean the consequences it current processing of health and personal data likely to have for it data subjects 'rights and freedoms under the Privacy Ordinance.

Management validation by DPIA

In this phase, the management or the board has the most important role, but the work must be put together so that the management has a basis for implementing a validation. Management must be aware that their business is treating personal data that may pose a high risk to it data subjects' rights and freedoms.

Present measures that have been chosen to ensure that you adhere to the basic principles of compliance privacy regulations

Present measures that have been chosen to provide adequate information security in according to "best practice" Map the risks based on severity and probability.

Prepare an action plan based on additional measures identified during the previous step: for each measure, determine as a minimum who is responsible for implementation, cost (financial or workload) and estimated time frame.

Tool

- KINS template for implementation of DPIA
- The Norwegian Data Protection Authority's guide for DPIA
- The Data Inspectorate's Checklist for Assessing Privacy Impact (DPIA)