POWER OF ATTORNEY FOR BETTER DATA PROTECTION

Final report from the sandbox project with Ahus

Datatilsynet

Contents

Summary

Akershus University Hospital (Ahus) provides digital follow-up at home (DHO) to around 6,000 patients. Most people are able to use the service unaided, but some, for various reasons, need help from others to use it. This can be provided by next of kin, assistants or other helpers. Ahus lacks a solution that gives helpers independent access, and has identified an unfortunate practice that has developed where helpers use the patient's login information.

This means that Ahus does not know who is logging in, nor does it have an overview of who has seen or done what. The patients themselves can also lose track. Sharing login information also entails a risk of misuse of other solutions the patient uses.

Ahus is looking for a solution that allows patients to give their helpers power of attorney to perform certain tasks for them. The solution will enable helpers to log in as themselves. This will improve data protection and benefit more patients and patient groups who struggle to use digital tools without assistance.

Through the Norwegian Data Protection Authority's regulatory sandbox, we have assessed whether Ahus can use a national supplier of power of attorney solutions for the healthcare sector, rather than developing its own solution or purchasing it from a private provider. *Norsk helsenett* (NHN), owned by the Norwegian Ministry of Health and Care Services, has a power of attorney solution in place for its users.

The sandbox project has looked at what data protection assessments Ahus must make to ensure data protection for patients who could use the power of attorney solution in connection with follow-up at home.

What is the sandbox?

In the sandbox, participants work together with the Data Protection Authority to address privacy and data protection issues. The goal is ensuring that their service or product meets legal requirements and provides sound data protection. The Data Protection Authority provides advice to participants, but the conclusions are not official or administrative decisions or approvals. Participants are thus free to choose whether they want to follow the advice.

The sandbox is useful for looking at issues that have not yet been referred to in case law to any degree. We hope this report can help others with similar challenges.

The following is a summary of the project's discussions and findings:

1. Who is **the data controller** for the processing of personal data in NHN's power of attorney solution?
    - Ahus determines the purpose of the data processing and how the power of attorney solution will be adapted. It is therefore natural that Ahus is the data controller.
2. Which **legal basis** could be used for allowing patients to use the power of attorney solution?
    - The Norwegian Patient and User Rights Act regulates who can consent to health care and when children can consent. In the first instance, the power of attorney solution will be used by people with the capacity to consent.
    - In line with this, consent may be a relevant legal basis, cf. Article 6(1)(a), cf. Article 9(2)(a) of the GDPR.
    - However, consent is not valid if there are negative consequences of not consenting, or if consent is in other ways given under pressure. The patient must be able to choose freely. The question is how freely a person perceives their consent to be if the alternative is not being able to live at home.
    - As long as the patient has the capacity to consent and can choose who is granted power of attorney, the requirement for consent being freely given may be met. Consent could therefore be a legal basis for using the digital power of attorney solution.
3. How can such a solution ensure **availability, confidentiality and integrity** in line with the data protection regulations?
    - Any solution in which personal data are processed must comply with requirements for technical and organisational measures that ensure confidentiality, integrity and availability.
    - Since the DHO service uses the NHN network, and some of the data shared via the service must be documented in medical records, the security system must satisfy the security requirements for a treatment-oriented health registry.
    - In this report, we review the security requirements that we believe are most relevant to this particular power of attorney solution: access management and solutions that ensure traceability.

Data controllership

The term ‘data controller’ corresponds to the Norwegian term ‘dataansvarlig’ used in Norwegian health law. (In Norwegian, the term ‘dataansvar’ is used instead of ‘behandlingsansvar’, as ‘behandling’ can refer to both medical treatment and processing in the context of data).

About the project

With increasing pressure on the health sector, it is a political goal that patients are able to live at home and receive health follow-up digitally (Report No 9 to the Storting (2023-2024)).

An increasing number of older people and patients with more complex medical conditions than before give rise to new challenges. The healthcare sector is therefore seeking digital solutions to ease the pressure. By using technology, patients can send measurement data and other health updates digitally from home, avoiding unnecessary visits to hospitals or municipal health services. Digital sharing of health data between patients and healthcare professionals, or between different care sector services, can provide major benefits, but also places high demands on security and data protection.

Akershus University Hospital (Ahus) provides digital follow-up at home (DHO) to around 6,000 patients. They recognise that some patients and certain patient groups need help from next of kin, assistants or others, hereinafter referred to as helpers, to use the service.

They therefore seek to offer a solution whereby patients can give their helpers power of attorney to perform certain tasks on their behalf in the hospital's digital system. In such a power of attorney solution, it must be possible to limit the helper's access to precisely what they need to perform specific tasks, and the solution must clearly show who has done and read what.

In this project, we have investigated how patients can share health data using such a power of attorney solution in a way that safeguards data protection.

What is power of attorney?

Power of attorney is a legal arrangement where a person (the principal) grants another individual (the agent) permission to act on their behalf, while still acting in their own name.

A power of attorney can be time-limited, task-based or linked to specific roles, and they must always be given on a voluntary and informed basis.

An agent cannot have access to more than the patient themselves.

About Akershus University Hospital (Ahus)

Akershus University Hospital (Ahus) is the hospital for approximately 594,000 inhabitants in Follo, Romerike, the Kongsvinger region and the northern regions of Oslo. The hospital employs around 12,000 people and is owned by South-Eastern Norway Regional Health Authority. The most important tasks are patient treatment, research, teaching and patient education.

Ahus currently has around 6,000 patients receiving digital follow-up at home. Like other hospitals, they expect more people to receive this type of follow-up in the years ahead.

About the hospital's digital follow-up at home (DHO) service

Digital follow-up at home (DHO) means that you can receive treatment at home without having to go to the hospital. Communication between doctor and patient takes place online. Several different companies provide such services with functionality that makes it possible to send information between the hospital and patients living at home.

The DHO service is like a toolbox, allowing the different hospital departments to use the tools they need to provide their patient group the best digital follow-up at home. The department that follows up patients with epilepsy, for example, will need different functionality than the department that follows up patients with diabetes.

Ahus uses a service provided by Dignio Connected Care. This service collects the same information that the hospital would receive if the patient had been admitted. The stay-at-home patient can share how they are feeling, how the treatment is working and describe their quality of life (PROM form). They can also send messages to the hospital. If the patient has a device that measures heart rate or other vital data, this is also sent to the hospital. As a security measure, the service requires the patient to log in with the BankID authentication system.

The challenge with the current DHO system

Many patients are able to use the hospital's DHO independently, but some patient groups need help from others to use the service. Patients need help for different reasons, and what they need help with also varies:

- Some patients have motor challenges that make it difficult for them to navigate the digital service. Others face challenges due to limited digital skills. These patients will need a helper who can do all the tasks in the service for them.
- Other patients are able to do some tasks themselves, but need help with specific tasks.
- Some want to keep parts of their communication with the hospital private, while they appreciate help with tasks they consider less sensitive.

Ahus has seen a practice where helpers sometimes log in with the patient's BankID. Ahus does not encourage this practice, but is aware that it is done due to a lack of better alternatives. They also know that some people use an analogue version, where relevant instructions and health data are available on paper in a binder at the patient's home.

A lack of secure and efficient solutions for helpers can compromise patient privacy in several ways:

- Generally speaking, it is risky to hand over login information for services that require a high level of security. A BankID provides access to more than just DHO – you can also access the Helsenorge service, the Norwegian Tax Administration and your bank.

- Helpers can gain access to more information than necessary. When they have the same access to the patient's health data as the patient themselves, whether in a physical folder or in a DHO system, they can see health data they do not need in order to provide assistance.

- Multiple users sharing the same login information makes it more difficult to ensure that the information is accurate, confidential and protected against misuse. Under the General Data

Protection Regulation (GDPR), the data controller has a duty to ensure the ongoing confidentiality, integrity and availability of personal data.

- The confidentiality of personal data is challenged when there are no security measures in place to protect the data from unauthorised disclosure and access. This also makes it difficult for Ahus to trace who has done what with the patient's personal and health data.

- Logging is possible on paper in a binder, but manual processing can create a risk of patients losing control over their own data and the integrity and accuracy of the data. For a vulnerable patient, it can be challenging to identify misuse with such practices.

- The current practice can also challenge the requirement for personal data to be accurate and up to date. Information stored in a binder or written down on a sheet of paper can quickly become outdated without being replaced by new and correct information. It can also go astray. Some information is disclosed orally and is not documented. This can lead to errors in treatment, which can negatively affect the patient's health. When information is recorded on paper and stored with the patient, it is far more difficult to maintain control and adequate personal data protection than in a centralised information system, where all information is processed according to defined security measures.

Ahus shares these challenges with other organisations that provide digital follow-up at home. The challenges are also relevant in other areas where people need help using digital services. As more and more contact with important public and private services goes digital, secure and user-friendly solutions must be in place. Everyone must be able to receive help – without compromising their privacy.

Goals for the sandbox project

The aim of the project is to explore how a power of attorney solution can provide better data protection for patients receiving digital follow-up at home.

To address the challenge, we looked at the following questions:

- Is there an existing power of attorney solution that Ahus can use instead of developing its own?
- Is the hospital's DHO considered a patient record system?
- Who is the data controller for the processing of personal data in a power of attorney solution operated by *Norsk Helsenett* (NHN)?
- Which legal basis could be used for allowing patients to use the power of attorney solution?
- What data protection requirements must be met to ensure the availability, confidentiality and integrity of such a service?

Data controllership

The term 'data controller' corresponds to the Norwegian term 'dataansvarlig' used in Norwegian health law. (In Norwegian, the term 'dataansvar' is used instead of 'behandlingsansvar', as 'behandling' can refer to both medical treatment and processing in the context of data).

Delimitation

We have limited the scope of this project to patients with the capacity to consent. Initially, Ahus plans to roll out the power of attorney solution for this group. In the long term, however, a power of attorney solution can also be adapted to people without the capacity to consent, but this will require thorough assessments, as it will raise legal and practical issues about who has legal capacity to act on behalf of the patient. Which diagnoses the patient receiving follow-up at home has may also be relevant for such assessments. When the patient is a child, age will be relevant, but diagnoses and maturity could also play a role.

In this project, we have also assumed that the people acting as agents are assistants, next of kin and other helpers without healthcare expertise.

§ Capacity to consent under the health regulations

The Norwegian Patient and User Rights Act sets out rules on the capacity to consent and healthcare for patients without capacity to consent. In principle, healthcare can only be provided with the patient's consent, cf. section 4-1 of the Patient and User Rights Act. Who has capacity to consent is regulated by section 4-3.

In principle, children can consent to healthcare from the age of 16, which is often referred to as the 'age of majority' under health law. Children between the ages of 12 and 16 may also have independent capacity to consent in cases concerning matters their parents should not know about. In such cases, the parents or those with parental responsibility will not have capacity to consent on behalf of the child. Otherwise, parents or those with parental responsibility will have capacity to consent for children under the age of 16.

Section 4-4 of the Patient and User Rights Act contains special rules for consent on behalf of children.

The capacity to consent for persons over the age of 16 may also lapse for health reasons, cf. section 4-3 second paragraph. This is assessed by healthcare professionals.

Can Ahus use an existing power of attorney solution?

In the short term, it would be easiest to develop a new solution for Ahus in cooperation with their service provider. At the same time, Ahus recognises the benefits of integration with a national solution for the healthcare sector. A common solution for all DHO services will probably make it easier for the user to understand what they are giving power of attorney for, and to manage the power of attorneys that have been given.

Considering the transfer value of a tested solution for other services and health trusts, as well as the value of having one such solution in the health sector rather than several, a technical adaptation to an existing power of attorney solution will potentially strengthen data protection for the user. It could also improve security if the solution is operated by a public-sector organisation with extensive experience in the field and a robust test environment. A common solution will also counteract inconsistencies between solutions.

Part of this sandbox project has therefore been to gain insight into which power of attorney solutions could be relevant for Ahus. In a meeting with the Norwegian Digitalisation Agency, *Norsk helsenett* (NHN), Ahus and the Data Protection Authority, we explored the possibilities and limitations of existing and planned power of attorney solutions. The purpose was also to gain insight into, and provide input to, the Norwegian Digitalisation Agency's ongoing work to develop a new power of attorney solution for the public sector.

Helsenorge is a public website for information about and access to most health services in Norway. The content is provided by various organisations and services in the health sector, and the state-owned NHN is responsible for the operation and development of the website.

Using Helsenorge, citizens can:

- gain access to what health data is registered about them
- see their patient records
- use various digital services such as booking a doctor’s appointment and communicating with their GP

Users with the capacity to consent can also give power of attorney to others to use the service on their behalf, whether it concerns a selection or all of the aforementioned areas of use that they themselves have consented to in the Helsenorge service. The user chooses who to give power of attorney to and what they want it to cover, and Helsenorge, in turn, performs a lookup in the National Population Register to authenticate the agents. The agent cannot gain access to more information than the principal has consented to in Helsenorge.

Helsenorge users must use an authentication solution with a high level of security to gain access. They can choose between BankID, Buypass or Commfides.

Norsk helsenett (NHN) – external power of attorney

NHN has developed an external power of attorney solution that will be put into production in the near future. Pharmacies will be the first enterprises to use the solution. Pharmacies are connected to the specialised industry solution EIK, which facilitates work processes and digital interaction between the pharmacies. EIK acts as a central link between various pharmacy systems and national systems

such as *Reseptformidleren*, the Norwegian Labour and Welfare Administration (NAV), Helfo, the health personnel register, the personal data register (PREG), etc.[1] This allows NHN to integrate its power of attorneys with EIK, which in turn communicates with all associated pharmacy systems.

The solution allows a private individual to use the Helsenorge service to give power of attorney to another private individual to collect medication from a pharmacy. For users, this works in the same way as giving power of attorney to read or manage services on Helsenorge on their behalf.

NHN explains that the system has been developed in a way that will allow other sectors to use the service, such as for digital follow-up at home.

The South-Eastern Norway Regional Health Authority currently has a framework agreement for digital follow-up at home with six different providers. It is therefore natural for health trusts to use solutions provided by these different data suppliers for the duration of the framework agreement. Unlike pharmacies, whose specialised systems are integrated with a common component such as EIK, there is no common component for the various systems used for DHO in the health trusts. This will require data suppliers to structure data and facilitate technical interaction with the NHN network.

NHN explains that it is possible to create an external power of attorney for each of the six solutions for DHO, but that an assessment must be made of whether this is desirable with respect to user-friendliness and simple administration for users.

A potential user scenario for a patient living at home

Ahus and NHN have now begun work on exploring how their DHO can be integrated with NHN's power of attorney solution. The concept for the solution could resemble the following for a patient who wants to give power of attorney to a next of kin or assistant to represent them in the hospital's DHO solution:

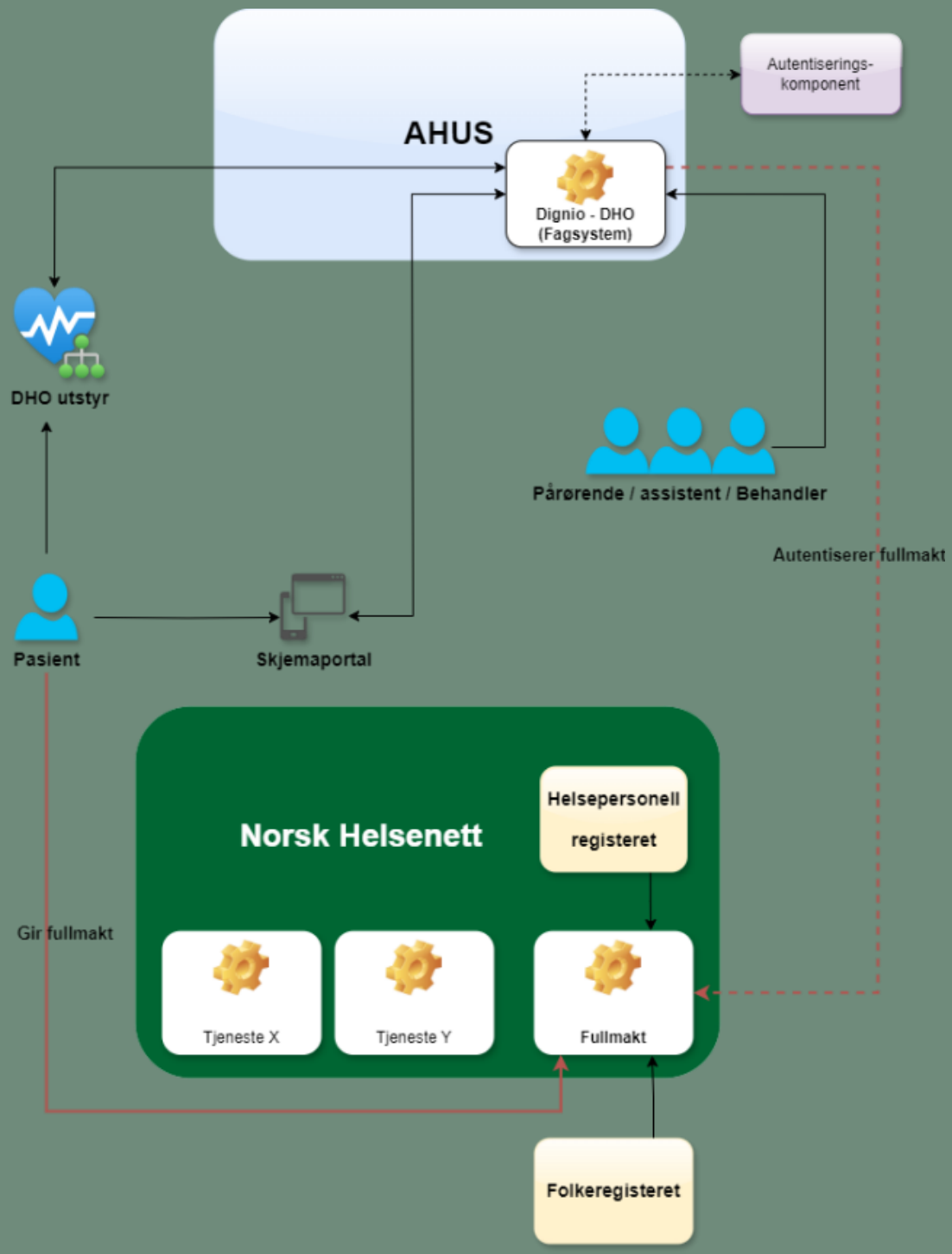
1. The patient logs into Helsenorge using BankID or another authentication solution with a high level of security.
2. The patient finds the name of an assistant, next of kin or other helper.
3. The patient decides what access they should have, and then gives power of attorney to represent them in the hospital's digital follow-up at home (DHO) service.
4. Next of kin or assistants log into the hospital's DHO using BankID or another authentication solution.
5. Next of kin or assistants can access the power of attorney area that the patient has given them access to. This is done through a lookup in Helsenorge where the relation between patient and health personnel and power of attorney are registered.

In the hospital's DHO, the content and tasks to which the various roles are given access are granulated and graded in the form of different power of attorney areas. These will also be shown in Helsenorge, allowing the patient to choose which power of attorney area they want to give the agent access to.

[1] What is EIK?

General illustration

Interactions between actors and systems in a potential solution could be illustrated as follows:



Is the hospital's DHO a patient record system?

For this project, it is important to clarify whether a potential power of attorney solution will process information that must be documented in medical records. Health legislation, including the Patient Records Act, regulates what information must be documented. A requirement to document information in medical records also has an impact on which security requirements are made when developing a power of attorney solution.

Ahus's DHO service is used in patient treatment and patient administration, and contains certain information that must be documented in medical records. This is documented in the patient's records in the hospital's record-keeping system (DIPS), which is outside the hospital's DHO. The information registered is considered necessary and relevant for the hospital to provide proper treatment of the patient. It can include being aware of measurement data outside the patient's normal value or a notification stating that the patient is no longer experiencing an effect from a treatment. If, on the other hand, measurement data shows normal values, or a patient asks to change an appointment, healthcare professionals may consider it unnecessary to document the information, and it remains in the hospital's DHO.

Currently, healthcare professionals at the hospital assess whether parts of the information submitted by the patient must be documented in their medical records, and enter these manually in DIPS. In future solutions, this can be done automatically by transferring the data without the involvement or control of healthcare professionals. Both of these ways of transferring data mean that the information must be handled in line with the same data security requirements as in a patient record system, right from the initial registration.

Patients or their agents should be able to use the service without having to think about whether what they communicate must be documented in the patient records. Whether or not the information communicated must be documented must be assessed by healthcare professionals or well-tested automated solutions.

Ahus's DHO service uses the NHN network as a communication channel. This means that it is integrated with the Helsenettet network provided by NHN in order to send health data securely. Before using NHN, users must agree to and comply with the Norwegian Code of Conduct for Information Security and Data Protection in the Health and Care Sector (the Code of Conduct). The Code of Conduct sets data security and data protection requirements in line with relevant regulations and is adapted to the healthcare sector.

Given the nature of the information and the fact that Ahus already uses the NHN network, we have together concluded that the power of attorney solution must satisfy the same security requirements as a patient record system.

Who is the data controller?

The data controller is the person who determines the purpose of the processing of personal data and the means to be used, cf. Article 4(7) of the General Data Protection Regulation (GDPR). The data controller is responsible for, and must be able to demonstrate compliance with, the GDPR, cf. the accountability principle in Article 5(2) of the GDPR. For example, the data controller is responsible for assessing what is considered to be appropriate technical and organisational measures for the power of attorney solution in accordance with Articles 24, 25 and 32 of the GDPR.

In this project, it is Ahus that wants integration with a power of attorney solution. The purpose is to ensure that their patients can send accurate and up-to-date health data to the hospital and to relevant parts of the municipal health service. This will enable patients to live at home for longer, while receiving the healthcare they need in an efficient and effective manner. The patient will, for example, avoid having to travel to the hospital for a check-up if there is no need to do so. Similarly, the patient may be called in for a check-up sooner if the information reported so indicates.

Ahus determines the purpose of the data processing and how the power of attorney solution will be adapted, and will therefore also be the data controller.

What are the relevant legal bases?

In this project, we have assessed what the legal basis might be for a patient to use a power of attorney solution that gives the agent access to the patient's health data in the hospital's DHO service.

The GDPR requires that all processing of personal data has a legal basis in one of the six alternatives listed in Article 6(1) (a) to (f).

Additional conditions must be met to process special categories of data, including data concerning health, cf. Article 9. In order to process health data, one of the exemptions set out in Article 9(2) must be met.

Communication between the patient and the hospital is considered part of the healthcare Ahus provides. The establishment of the solution itself is assumed to be covered by the general rules that apply to the processing of personal data in the health sector.

In the assessment of the legal basis for using the solution for the individual patient, consent may be a relevant legal basis, cf. Article 6(1)(a), cf. Article 9(2)(a).

For consent to be valid, it must be freely given, specific, informed and unambiguous, given through clear affirmative action, documentable and as easy to withdraw as to give, cf. Article 4(11) and Article 7 GDPR. As the solution will process health data, the consent must also be 'explicit', cf. Article 9(2)(a).

The patient, who will also be the principal, must receive information about how data is processed, why it is processed, who has access, the possibilities for rectifying and deleting health data, and how they can restrict and withdraw their power of attorney. As such, Ahus must create a solution that provides clear information and descriptions that are easy to understand and adapted to the individual patient.

The requirement of freely given consent

One challenge when using consent, which must be given particular attention in this case, is the requirement for consent being freely given.

We assume that some patients want to stay at home for as long as possible. A prerequisite for living at home is being able to report health data to the municipality and/or hospital. If they are unable to do this themselves, they must consent to giving power of attorney to assistants, next of kin or other helpers to carry out the tasks.

However, consent is not valid as a legal basis under the GDPR if there is pressure to consent or if there are negative consequences of not consenting. The individual must be able to make a free choice. This can put pressure on giving consent freely if the alternative to consenting to the use of the power of attorney solution is, for example, living in a healthcare institution.

At the same time, it is up to the patient to choose who will represent them. In many cases, it is the patient themselves who hires assistants, and they can choose who they want to act as their next of kin and other helpers. This reduces the risk of the patient giving power of attorney to a person they do not want to give it to. The solution must also be tailored so that the power of attorney given to a person and their right to access information is not too broad. Assuming that the solution is only to be used by patients with the capacity to consent and that the patient can choose who is given power of attorney to report information to the health services, as well as what the agents will have access to,

it is the Data Protection Authority's opinion that the requirement for freely given consent will generally be met.

Based on the above assumptions, we believe that consent in this context is a relevant legal basis for use of the digital power of attorney solution.

What if the patient does not have the capacity to consent?
In cases where the patient does not have the capacity to consent, it can be challenging to use the power of attorney solution. In such cases, Ahus must consider guardianship and other legal bases. Both Article 6(3) and Article 9(2) of the GDPR require in some cases a supplementary legal basis in national legislation. This means that the data controller must be able to demonstrate a legal basis for the relevant processing of personal data in Articles 6 and 9 of the GDPR *and* in national legislation.

For people without the capacity to consent, a guardianship solution will generally also be established, and it must be considered whether this includes safeguarding patient rights.

Ensuring availability, confidentiality and integrity

In the solution, Ahus will have to meet requirements for technical and organisational measures to ensure confidentiality, integrity and availability.

Article 32 of the GDPR sets out requirements for the assessments and technical measures that must be implemented to fulfil the requirement for security of processing. Due to the scope of the project, not all assessments and measures are covered. As the purpose of the service is to make personal and health data available, we have chosen to emphasise access control and ensuring traceability as the most important measures.

§ Security of processing, cf. Article 32

Article 32 of the GDPR sets out requirements for the security of the processing of personal data. The controller must establish 'appropriate technical and organisational measures'. In order to clarify what appropriate technical and organisational measures could be, this must be seen in the context of 'the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons'. It is up to the controller to make this assessment, but Article 32 provides examples of measures that may be appropriate to ensure a 'level of security appropriate to the risk'.

See also the Code of Conduct for additional requirements.

Access control

Access control entails a duty to ensure that personal data are only accessible on the basis of a legitimate need. Efficient and proper access control will help ensure that confidentiality is maintained, because the data is only available to those who have been granted access. It will ensure integrity because the user only has access to make the changes required to complete the task, and it will ensure availability because the user only has access to the data necessary to perform the task.

To do so, access must be authenticated in a secure way. It also requires such access to be granted, managed, controlled and removed.

The requirement for access control is not explicitly stated in the GDPR, but it is a natural consequence of the requirement for the data controller to implement 'appropriate technical and organisational measures' under Article 32, cf. the principle of integrity and confidentiality in Article 5(f). Good access control is, for example, absolutely necessary in order to comply with confidentiality requirements and section 21 of the Health Personnel Act, cf. sections 15 et seq. of the Patient Records Act and section 13 of the Patient Records Regulations.

In the adaptation of NHN's power of attorney solution, Ahus will assess which roles should have access to structured and unstructured data in the hospital's DHO. Unstructured data, such as how the patient feels from day to day, information about sexuality, substance abuse, mental health etc., requires a different level of confidentiality than structured data, such as measurement data showing the patient's pulse rate. This will reflect the power of attorney areas patients give access to, so that it is clear who is given access to the respective areas.

Access control in a potential solution will require coordination and collaboration between the health trusts, the DHO providers and NHN. When access must be granulated across several levels, all stakeholders must be involved. First and foremost, the data controllers (health trusts) must decide which access levels to use for their DHO solution. DHO providers must then customise their systems based on this specification. Finally, NHN must implement the different access levels in its service.

Given that the granularity levels reflecting which data the different agents will have access to have not yet been defined, it is not clear what will be considered sufficient information for patients to make an informed choice about the level of power of attorney.

A new solution where assistants, next of kin and other helpers log in as themselves and not as the patient will increase the patient's control over their own data, as well as the data controller's ability to control access to health and personal data.

Requirements for data protection by design

Article 25 of the GDPR sets out requirements for privacy by design, which must be considered when developing a new power of attorney solution. Privacy by design and privacy by default entail that the controller must implement appropriate technical and organisational measures designed to effectively implement the principles for the protection of personal data. This is to integrate the necessary safeguards into the processing to fulfil the requirements of the GDPR and protect the rights of data subjects.

Read more in our guide on data protection by design and data protection by default.

Ensuring traceability

Traceability can be achieved by the system logging which users or identities perform various actions in the solution. These actions could be reading, registration, modification or erasure of data, depending on which power of attorneys a user has in the system. For logging to be an effective measure to ensure confidentiality, log control must also be established. Logging of actions is the tool, and a prerequisite for being able to implement the controlling measure, namely systematic log control.

Today's logging functionality has its challenges. In a physical binder, logging can easily be forgotten or avoided, while in the hospital's DHO, activity is logged in the patient's profile. This practice does not reflect with certainty who is actually given access to health and personal data. It will be challenging for the patient to know what next of kin, assistants and other helpers actually see and write. A digital power of attorney solution will provide new possibilities. In comparison, a patient record system will require logging or tracking of who has had access to health data. The patient will have the right to access information in the log, cf. section 14 of the Patient Records Regulations. The power of attorney solution should be able to provide the same possibilities. By giving the patient access to this log, they will be able to know and control how the chosen power of attorney scheme works.

This type of logging is a crucial technical or organisational measure that safeguards confidentiality, integrity and availability. This is because all types of discrepancies can be traced and necessary corrective action can be taken.

As one of the health trusts in the South-Eastern Norway Regional Health Authority, Ahus is obliged to comply with the Norwegian Code of Conduct for Information Security and Data Protection in the Health and Care Sector (the Code of Conduct). The Code of Conduct is an industry standard, developed and managed by organisations and enterprises in the healthcare sector. Section 5.4.4 of the Code of Conduct provides guidelines for what, as a minimum, should be recorded in access logs in connection with authorised use of treatment-related health registries. This includes:

- The identity of the person who has read, rectified, registered, changed and/or erased health and personal data
- Organisational affiliation (not relevant for private individuals)
- The basis for the access
- The timeframe for the access

A power of attorney solution should be adapted in such a way that the data controller, if necessary, has access to an adequate log of all events that occur in the DHO service. NHN, on its part, will log which persons are given which types of access to the DHO service.

The way forward

In this project, Ahus and the Data Protection Authority have looked at the possibilities and limitations of using a national power of attorney solution. Although coordination with other services and putting technical solutions in place could be more demanding, we agree that relying on a well-established national platform rather than creating an independent solution locally will be both more secure and user-friendly.

What about patients without the capacity to consent?

There are major differences in the abilities and needs of patients living at home when dealing with a DHO service. In this project, Ahus and the Data Protection Authority have taken as their basis patients with the capacity to consent, who can therefore give power of attorney to next of kin or assistants. In the long term, the power of attorney solution can be developed to encompass more patient groups.

This could be people under guardianship, or children, but also patients who cannot access public services for other reasons, such as foreign citizens without an electronic ID or citizens who opt out of digital communication with the public sector.

Ahus, for example, has an increasing number of patients who are minors who need and are entitled to take a more active role in their own health from the age of 12 (section 3-4 of the Patient and User Rights Act). At present, they are not able to communicate with healthcare professionals in the hospital's DHO without their parents/guardians having full access to the information.

It will also be necessary to take a closer look at who can represent children and other patients without the capacity to consent. Currently, only parents with the same registered address as the child have the right to represent them. Ahus has seen that some children cannot receive digital follow-up at home because their caregivers do not meet this legal definition. Some have bonus parents, live with foster parents, others live with next of kin, some have guardians or live in an institution and need help from the staff there at any given time. Ahus has called for updated legal definitions of caregivers that more accurately reflect the realities.

For patients without the capacity to consent, it is feasible that a guardian or other representative might use the power of attorney solution on their behalf – but this will require thorough legal and practical assessments, particularly in relation to who can actually act on behalf of the patient.

Towards a national digital power of attorney solution in the public sector

This project is one example that indicates a more general need. The public sector needs power of attorney solutions that can have different levels and possibilities depending on which tasks the agent is to perform. This is not limited to the healthcare sector. Similar needs exist in other public sectors that want their services to be accessible to everyone, including those needing help to use them.

The Norwegian Digitalisation Agency has been commissioned to assess and develop a digital power of attorney solution for public services. With this project, Ahus and the Data Protection Authority wish to provide insight into the challenges and needs of one part of the healthcare sector, the possibilities and limitations of existing power of attorney solutions, and to highlight some key data protection issues that can be used in the work to ensure that digitalisation benefits all citizens. Everyone has the right to be included, especially when it comes to public services.

Office address:
Trelastgata 3, Oslo

Postal address:
P.O. Box 458 Sentrum,
NO-0105 Oslo

postkasse@datatilsynet.no
Phone: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no