FULLMAKT TIL BEDRE PERSONVERN

Sluttrapport fra sandkasseprosjektet med Ahus

Datatilsynet

Innhold

Merk

Teknologien og jussen er stadig i utvikling, og det vil kunne ha skjedd justeringer og presiseringer etter at denne rapporten ble skrevet.

Sammendrag

Akershus Universitetssykehus (Ahus) gir digital hjemmeoppfølging (DHO) til rundt 6000 pasienter. De fleste klarer fint å bruke tjenesten på egenhånd, mens enkelte av ulike grunner trenger hjelp fra andre for å bruke den. Det kan være fra pårørende, assistenter eller andre hjelpere. Ahus mangler en løsning som gir hjelperne egen tilgang, og ser at det har utviklet seg en uheldig praksis der hjelperne bruker pasientens påloggingsinformasjon.

Dette gjør at Ahus ikke vet hvem som logger seg inn, og heller ikke har oversikt over hvem som har sett eller gjort hva. Pasientene kan også miste oversikten selv. Å dele påloggingsinformasjon innebærer i tillegg en risiko for misbruk av andre løsninger pasienten bruker.

Ahus ønsker en løsning der pasientene gir hjelperne fullmakt til å utføre visse oppgaver for dem. Løsningen skal gjøre det mulig for hjelperne å logge seg på som seg selv. Dette vil gi bedre personvern og være til hjelp for flere pasienter og pasientgrupper som sliter med å bruke digitale verktøy uten hjelp.

I Datatilsynets regulatoriske sandkasse har vi vurdert om Ahus kan bruke en nasjonal leverandør av fullmaktsløsninger for helsesektoren, i stedet for å utvikle en egen løsning eller kjøpe det fra en privat aktør. Norsk helsenett (NHN), eid av Helse- og omsorgsdepartementet, har en fullmaktsløsning for sine brukere.

I sandkasseprosjektet har vi sett på hvilke personvernvurderinger Ahus må gjøre for å sikre pasientenes personvern om de bruker denne fullmaktsløsningen i hjemmeoppfølgingen.

Hva er sandkassa?

I sandkassa jobber deltakere sammen med Datatilsynet for å løse spørsmål om personvern. Målet er at tjenesten eller produktet deres følger loven og gir godt personvern. Datatilsynet gir råd til deltakerne, men konklusjonene er ikke offisielle avgjørelser, vedtak eller godkjenninger. Deltakerne velger selv om de vil følge rådene.

Sandkassa er nyttig for å se på spørsmål der jussen har få praktiske eksempler å vise til. Vi håper rapporten kan hjelpe andre med liknende utfordringer.

Her er en oppsummering av prosjektets diskusjoner og funn:

1. Hvem har **dataansvaret** for behandling av personopplysninger i NHNs fullmaktsløsning?
    - Ahus bestemmer formålet med behandlingen av opplysningene og tilpasningen til fullmaktsløsningen. Det er derfor naturlig at Ahus er dataansvarlig.
2. Hva kan være det **rettslige grunnlaget** for å la pasienter bruke fullmaktsløsningen?
    - Pasient- og brukerrettighetsloven regulerer hvem som kan samtykke til helsehjelp og når barn kan samtykke. Det er i første omgang personer med samtykkekompetanse som vil bruke fullmaktsløsningen.
    - I tråd med dette kan samtykke kan være et aktuelt rettslig grunnlag, jf. artikkel 6 nr. 1 bokstav a, jf. artikkel 9 nr. 2 bokstav a.
    - Et samtykke er imidlertid ikke gyldig hvis det oppstår negative konsekvenser ved ikke å samtykke, eller om samtykket på andre måter blir gitt under press. Pasienten må kunne velge fritt. Spørsmålet er hvor fritt det oppleves å samtykke, dersom alternativet er å ikke kunne bli boende hjemme?
    - All den tid pasienten har samtykkekompetanse og selv kan velge hvem som får fullmakter, vil kravet til frivillighet kunne være oppfylt. Samtykke kan derfor være et rettslig grunnlag for å bruke den digitale fullmaktsløsningen.
3. Hvordan kan en slik løsning sikre **tilgjengelighet, konfidensialitet og integritet** i tråd med personvernregelverket?
    - Enhver løsning som det behandles personopplysninger i må følge krav om tekniske og organisatoriske tiltak som sikrer konfidensialitet, integritet og tilgjengelighet.
    - Siden DHO-tjenesten bruker Norsk helsenett, og noen av opplysningene som deles over tjenesten er journalpliktige, må sikkerheten tilfredsstille kravene til sikkerhet for et behandlingsrettet helseregister.
    - I denne rapporten går vi igjennom sikkerhetskravene vi mener er mest relevante for denne fullmaktsløsningen: tilgangsstyring og løsninger som sikrer sporbarhet.

Dataansvar

I helseretten brukes begrepet "dataansvar" i stedet for "behandlingsansvar" for å markere at ansvaret skiller seg fra det medisinske behandlingsansvaret.

Om prosjektet

Med økende press på helsesektoren er det et politisk satt mål, at pasienter skal kunne bo hjemme og få helseoppfølging digitalt (Meld. St. 9 (2023 – 2024).

Flere eldre og pasienter med mer sammensatte sykdomsbilder enn tidligere gir nye utfordringer. Derfor ser aktører i helsesektoren på digitale løsninger for å lette presset. Ved å bruke teknologi kan pasienter sende måledata og andre oppdateringer på helsesituasjonen digitalt hjemmefra, og unngå unødvendige besøk på sykehus eller kommunehelsetjeneste. Digital deling av helseopplysninger mellom pasient og helsepersonell, eller mellom ulike aktører i omsorgssektoren, kan gi store gevinster, men stiller også høye krav til sikkerhet og personvern.

Akershus Universitetssykehus (Ahus) tilbyr Digital hjemmeoppfølging (DHO) til rundt 6000 pasienter. De ser at noen pasienter og enkelte pasientgrupper trenger hjelp fra pårørende, assistenter eller andre, heretter kalt hjelpere, med å bruke tjenesten.

De ønsker derfor å tilby en løsning, der pasienter kan gi hjelperne fullmakt til å utføre visse oppgaver på deres vegne i sykehusets digitale system. En fullmaktsløsning skal kunne avgrense tilgangen hjelperne får til akkurat det de trenger for å utføre spesifikke oppgaver, og vil gjøre tydelig hvem som har gjort og lest hva.

I dette prosjektet har vi undersøkt hvordan pasienter kan dele helseopplysninger ved hjelp av en slik fullmaktsløsning på en personvernvennlig måte.

Hva er fullmakt?

Fullmakt er en juridisk rettighet der en person (fullmaktsgiver) gir en annen person (fullmektig) tillatelse til å handle på deres vegne, men ved å samtidig opptre som seg selv.

Fullmakter kan være tidsbegrensede, oppgavebaserte eller tilknyttet spesifikke roller, og de må alltid gis frivillig og informert.

En fullmektig kan ikke få tilgang til mer enn pasienten selv.

Om Akershus Universitetssykehus (Ahus)

Akershus universitetssykehus (Ahus) er sykehuset for cirka 594 000 innbyggere i Follo, Romerike, kongsvingerregionen og de nordlige bydelene i Oslo. Sykehuset har omtrent 12 000 ansatte og eies av Helse Sør-Øst. De viktigste oppgavene er pasientbehandling, forskning, undervisning og opplæring av pasienter.

Ahus har i dag rundt 6000 pasienter som mottar digital hjemmeoppfølging. I likhet med andre sykehus, forventer de at flere vil få denne typen oppfølging de kommende årene.

Om sykehusets digitale hjemmeoppfølgningstjeneste (DHO)

Digital hjemmeoppfølging (DHO) betyr at du kan få behandling hjemme uten å måtte dra til sykehuset. Kommunikasjonen mellom lege og pasient skjer over nettet. Flere ulike selskaper tilbyr slike tjenester med funksjonalitet som gjør det mulig å sende informasjon mellom sykehuset og pasienter som bor hjemme.

DHO-tjenesten er som en verktøykasse, og lar de ulike avdelingene på sykehuset bruke de verktøyene de trenger for å tilby pasientgruppen sin den beste digitale hjemmeoppfølgingen. For eksempel vil avdelingen som følger opp pasienter med epilepsi ha behov for annen funksjonalitet enn avdelingen som følger opp pasienter med diabetes.

Ahus bruker en tjeneste fra Dignio Connected Care. Denne samler inn de samme opplysningene som sykehuset ville fått om pasienten var innlagt. Den hjemmeværende pasienten kan dele hvordan de føler seg, hvordan behandlingen virker, og hvordan livskvaliteten er (PROM-skjema). De kan også sende meldinger til sykehuset. Hvis pasienten har en maskin som måler puls eller andre vitale data, sendes disse til sykehuset også. Som et sikkerhetstiltak krever tjenesten at pasienten logger seg på med BankID.

Utfordringen med dagens DHO

Mange pasienter klarer fint å bruke sykehusets DHO på egenhånd. Men noen pasientgrupper trenger hjelp av andre for å bruke tjenesten. Det er ulike grunner til at pasienter trenger hjelp, og det varierer hva de trenger hjelp med:

- En del pasienter har motoriske utfordringer, som gjør det vanskelig å manøvrere seg rundt i tjenesten. Andre er hindret av svake digitale ferdigheter. Disse pasientene vil ha behov for at en hjelper gjør alle oppgavene i tjenesten for dem.
- Andre pasienter kan gjøre noe selv, men trenger hjelp til å løse enkelte oppgaver.
- Noen ønsker å holde deler av kommunikasjonen med sykehuset privat, mens de setter pris på hjelp til oppgaver de selv opplever som mindre sensitive.

Ahus ser at det hender hjelpere logger inn med pasientens BankID. Ahus oppfordrer ikke til slik praksis, men er klar over at det skjer i mangel av gode alternativer. De vet også at noen bruker en analog variant, der relevante instrukser og helseopplysninger er tilgjengelig i en papirperm hjemme hos pasienten.

Når det ikke finnes trygge og gode løsninger for hjelpere, kan det gå ut over pasientens personvern på flere måter:

- Rent overordnet er det risikabelt å gi fra seg påloggingsinformasjon til tjenester som krever høyt sikkerhetsnivå. En BankID gir tilgang til mer enn bare DHO – for eksempel Helsenorge, banken og Skatteetaten.

- Hjelpere kan få innsyn i mer enn nødvendig. Når de får samme tilgang til pasientens helseopplysninger som pasienten selv, enten den ligger i en fysisk perm eller i et DHO-system, kan de se helseopplysninger de ikke trenger for å hjelpe.

- At flere brukere deler samme innloggingsinformasjon gjør det vanskeligere å sikre at informasjonen er riktig, konfidensiell og beskytta mot misbruk. Etter Personvernforordningen har den dataansvarlige plikt til å sikre vedvarende konfidensialitet, integritet og tilgjengelighet av personopplysninger.

- Personopplysningenes konfidensialitet utfordres når det mangler sikkerhetstiltak som beskytter opplysningene mot uautorisert utlevering og tilgang. Dette gjør at det også er vanskelig for Ahus å spore hvem som har gjort hva med pasientens person- og helseopplysninger.

- Loggføring er mulig i en perm, men denne manuelle behandlingen kan skape risiko for at pasienter mister kontrollen over egne opplysninger, opplysningenes integritet og riktighet. For en sårbar pasient, kan det være krevende å avdekke misbruk under en slik praksis.

- Dagens praksis kan også utfordre krav om at personopplysninger skal være riktige og oppdaterte. Opplysninger som ligger i en perm eller noteres på et ark kan fort bli utdatert uten at det erstattes av nye og riktige opplysninger. De kan også komme på avveie. Enkelte opplysninger overleveres muntlig og blir ikke dokumentert. Dette kan føre til feil i behandlingen, noe som kan påvirke pasientens helse negativt. Når informasjonen er papirbasert og plassert hos pasienten, er det langt vanskeligere å opprettholde kontroll og tilstrekkelig personvernsikkerhet enn i et sentralisert informasjonssystem, der all informasjon blir behandlet etter definerte sikkerhetstiltak.

Dette er utfordringer Ahus deler med andre aktører som tilbyr digital hjemmeoppfølging. Utfordringen er også aktuell på andre områder der innbyggere trenger hjelp til å bruke digitale tjenester. Når stadig mer kontakt med viktige offentlige og private aktører skjer digitalt, må det finnes sikre og brukervennlige løsninger. Alle må ha mulighet til å få hjelp – uten at det går ut over personvernet.

Mål for sandkasseprosjektet

Målet med prosjektet er å utforske hvordan en fullmaktsløsning kan gi bedre personvern for pasienter som får digital hjemmeoppfølging.

For å finne ut av dette har vi sett nærmere på følgende spørsmål:

- Finnes det allerede en fullmaktsløsning Ahus kan bruke, i stedet for å utvikle sin egen?
- Regnes sykehusets DHO som et pasientjournalsystem?
- Hvem har dataansvaret for behandling av personopplysninger i en fullmaktsløsning som driftes av Norsk Helsenett (NHN)?
- Hva kan være det rettslige grunnlaget for at en pasient tar i bruk en slik løsning?
- Hvilke krav til personvern må oppfylles for å sikre tilgjengelighet, konfidensialitet og integritet i en slik tjeneste?

Dataansvar

I helseretten brukes begrepet "dataansvar" i stedet for "behandlingsansvar" for å markere at ansvaret skiller seg fra det medisinske behandlingsansvaret.

Avgrensning

I dette prosjektet har vi avgrenset oss til pasienter med samtykkekompetanse. Det er disse Ahus ser for seg å rulle ut fullmaktsløsningen for i første omgang. På sikt kan en eventuell fullmaktsløsning også tilpasses til personer uten samtykkekompetanse, men det vil kreve grundige vurderinger. En slik bruk av løsningen vil reise rettslige og praktiske spørsmål om hvem som har rettslig handleevne for pasienten. Hvilke diagnoser pasienten på hjemmeoppfølging har, kan også være relevant for slike vurderinger. Når pasienten er et barn vil alder være relevant, men diagnoser og modenhet kan også spille inn.

Vi har i dette prosjektet også tatt utgangspunkt i at det er assistenter, pårørende og andre hjelpere uten helsefaglig kompetanse som opptrer som fullmektige.

§ Samtykkekompetanse etter helseregelverket

Pasient og brukerrettighetsloven har regler om samtykkekompetanse og helsehjelp til pasienter uten samtykkekompetanse. Utgangspunktet er at helsehjelp bare kan gis med pasientens samtykke, jf. pasient og brukerrettighetsloven § 4-1. Hvem som har samtykkekompetanse reguleres av § 4-3.

Barn kan i utgangspunktet samtykke til helsehjelp fra de er 16 år, dette kalles gjerne den helserettslige «myndighetsalderen». Barn mellom 12 og 16 år kan også ha selvstendig samtykkekompetanse dersom det gjelder forhold som foreldrene ikke bør få vite om. Da vil foreldre eller de med foreldreansvaret ikke ha samtykkekompetanse på vegne av barnet. Ellers vil foreldre eller de med foreldreansvaret ha samtykkekompetanse for barn under 16 år.

Pasient- og brukerrettighetsloven § 4-4 inneholder særskilte regler for samtykke på vegne av barn.

Samtykkekompetansen for personer over 16 år kan videre bortfalle av helsemessige årsaker, jf. § 4-3 andre ledd. Det er helsepersonellet som vurdere dette.

Kan Ahus bruke en eksisterende fullmaktsløsning?

På kort sikt ville det enkleste være å utvikle en egen løsning i samarbeid med deres tjenesteleverandør. Samtidig ser Ahus fordelene ved å knytte seg til en nasjonal løsning for helsesektoren. En felles løsning for alle DHO-tjenestene vil trolig gjøre det enklere for brukeren å forstå hva man gir fullmakt til, samt enklere å administrere de fullmakter som er gitt.

Med tanke på overføringsverdien en allerede utprøvd løsning vil ha for andre tjenester og helseforetak, samt verdien av å ha en slik løsning i helsesektoren framfor flere, vil en teknisk tilpasning til en eksisterende fullmaktsløsning potensielt styrke personvernet for brukerne. Det kan dessuten gi økt sikkerhet om løsningen driftes av en offentlig aktør med lang erfaring på området, og som har et solid testmiljø. En felles løsning vil også motvirke inkonsistens mellom løsninger.

En del av dette sandkasseprosjektet har derfor vært å få et innblikk i hvilke fullmaktsløsninger som kunne være aktuelle for Ahus. I et møte med Digitaliseringsdirektoratet, Norsk helsenett (NHN), Ahus og Datatilsynet utforsket vi sammen muligheter og begrensninger i eksisterende og planlagte fullmaktsløsninger. Formålet var også å få innsyn i, og gi innspill til, Digitaliseringsdirektoratets pågående arbeid med å utvikle en ny fullmaktsløsning for offentlig sektor.

Helsenorge er et offentlig nettsted for informasjon om – og tilgang til – de fleste helsetjenester i Norge. Innholdet blir levert av ulike aktører i helsesektoren, og det er statseide Norsk helsenett (NHN) som har ansvar for drift og utvikling av nettstedet.

Ved hjelp av Helsenorge kan innbyggere:

- få innsyn i hvilke helseopplysninger som er registrert om dem,
- se sin pasientjournal, og
- bruke ulike digitale tjenester som å bestille legetime og kommunisere med fastlegen

Brukere med samtykkekompetanse kan også gi andre fullmakt til å bruke tjenesten på deres vegne, enten det gjelder et utvalg, eller alle de nevnte bruksområdene som de selv har samtykket til hos Helsenorge. Brukeren velger hvem og hva hen vil gi fullmakt til å gjøre, og Helsenorge gjør på sin side oppslag mot folkeregisteret for å autentisere de fullmektige. Fullmektige kan ikke få tilgang til mer informasjon enn det fullmaktsgiveren selv har samtykket til hos Helsenorge.

Brukere av Helsenorge må bruke en autentiseringsløsning med høyt sikkerhetsnivå for å få tilgang. De kan velge mellom BankID, Buypass eller Commfides.

Norsk helsenett – ekstern fullmakt

NHN har utviklet en løsning kalt ekstern fullmakt som skal settes i produksjon i nær fremtid. De første som skal benytte seg av løsningen er apotekene. Apotekene er knyttet til den spesialiserte bransjeløsningen EIK som tilrettelegger arbeidsprosesser og digital samhandling mellom apotekene. EIK fungerer som et sentralt bindeledd mellom ulike apoteksystemer og myndighetssystemer som reseptformidleren, NAV, Helfo, helsepersonellregisteret, personregisteret m.m[1]. Dette åpner for at

[1] Hva er Eik?

NHN kan knytte sine fullmakter til EIK, som igjen kommuniserer ut mot samtlige tilknyttede apoteksystemer.

Løsningen kan gjøre at en privatperson kan gi fullmakt – via Helsenorge – til en annen privatperson for å hente ut legemidler hos et apotek. For brukere fungerer dette på samme måte som å gi fullmakt til å lese eller administrere tjenester på Helsenorge på vegne av seg selv.

NHN forklarer at systemet er utviklet med tanke på at andre sektorer også skal kunne benytte tjenesten, som for eksempel digital hjemmeoppfølging.

Helse Sør-Øst har i dag en rammeavtale for digital hjemmeoppfølging med seks ulike leverandører. Derfor er det naturlig at helseforetakene benytter løsninger fra disse ulike aktørene i den tiden rammeavtalen gjelder. I motsetning til apotekene som har sine fagsystemer knyttet opp mot en felleskomponent som EIK, er det ikke noen felleskomponent for de forskjellige systemene som benyttes for DHO i helseforetakene. Dette vil kreve at leverandørene strukturerer data og tilrettelegger teknisk samhandling med Norsk helsenett (NHN).

NHN forklarer at det er mulig å lage en ekstern fullmakt for hver av de seks løsningene for DHO, men at det må utredes om hvorvidt dette er ønskelig med tanke på brukervennlighet og enkel administrasjon for brukerne.

Et tenkt brukerscenario for en hjemmeboende pasient

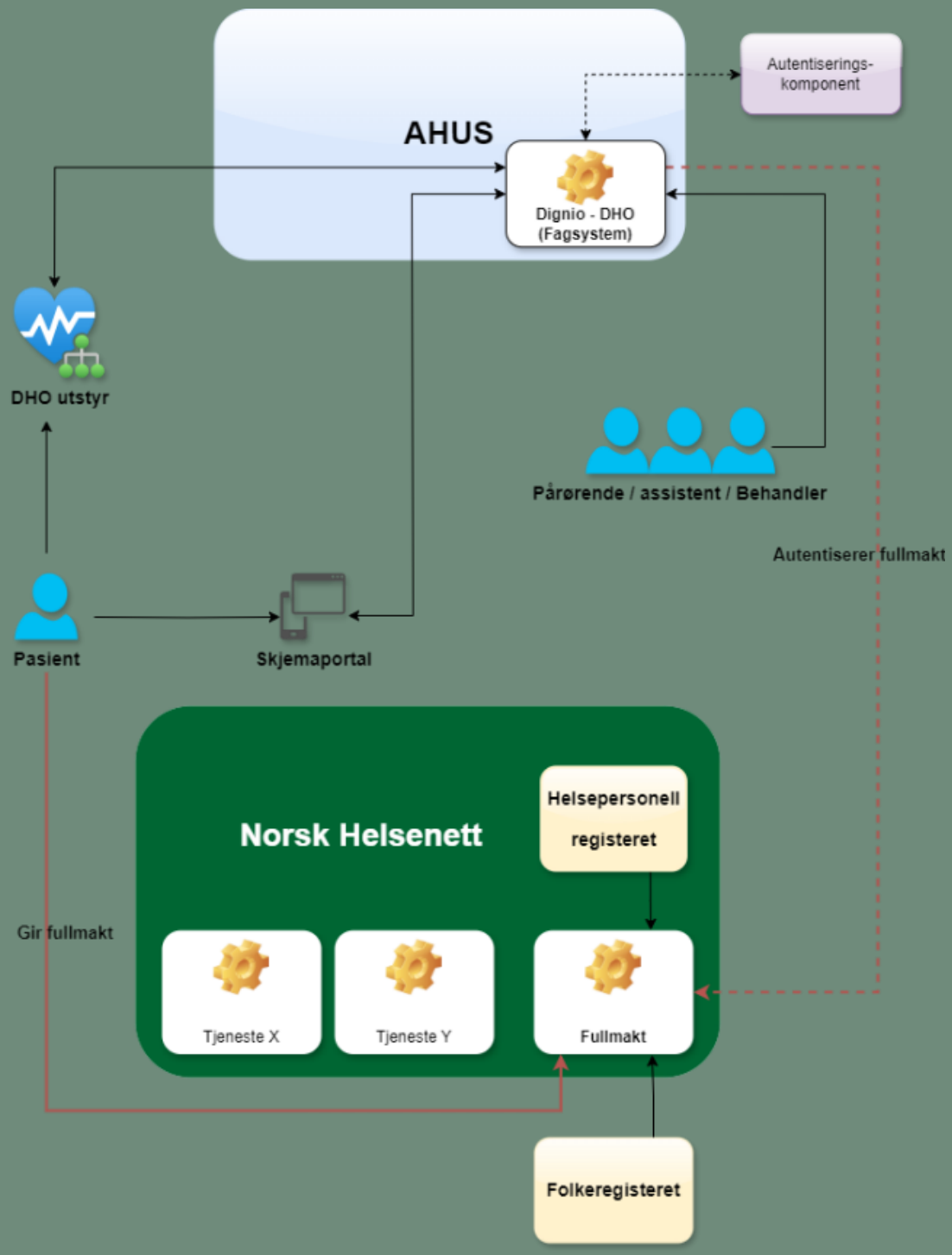
Ahus og NHN har nå startet arbeidet med å utforske hvordan deres DHO kan knytte seg til NHNs fullmaktsløsning, og konseptet for løsningen kan se omtrent ut som følger for en pasient som ønsker å gi en pårørende eller assistent fullmakt til å representere dem i sykehusets DHO-løsning:

1. Pasient logger seg inn på Helsenorge med BankID eller annen autentiseringsløsning med høyt sikkerhetsnivå.
2. Pasienten finner navnet på assistent, pårørende eller annen hjelper.
3. Pasienten bestemmer hvilken tilgang vedkommende skal ha – og gir deretter fullmakt til å representere seg i sykehusets Digitale hjemmeoppfølgingstjeneste (DHO).
4. Pårørende eller assistent logger seg inn med BankID eller annen autentiseringsløsning på sykehusets DHO.
5. Pårørende eller assistent får tilgang til fullmaktsområdet som pasienten har gitt dem tilgang til. Dette foregår gjennom et oppslag mot Helsenorge der behandlerrelasjon og fullmakt er registrert.

I sykehusets DHO granuleres og graderes hvilket innhold og oppgaver de ulike rollene skal ha tilgang til i form av ulike fullmaktsområder. Disse vil også fremkomme i Helsenorge, slik at pasienten kan velge hvilket fullmaktsområde hen ønsker å gi fullmektig tilgang til.

Overordnet illustrasjon

Interaksjoner mellom aktører og systemer i en tenkt løsning kan se slik ut:



Er sykehusets DHO et pasientjournalsystem?

For dette prosjektet er det viktig å avklare hvorvidt en eventuell fullmaktsløsning vil behandle journalpliktige opplysninger. Helselovgivningen, blant annet pasientjournalloven, regulerer hva som er journalpliktig. Og en eventuell journalplikt har konsekvenser for hvilke krav som stilles til sikkerhet i utviklingen av en fullmaktsløsning.

DHO-tjenesten til Ahus benyttes i pasientbehandling og pasientadministrasjon, og inneholder visse journalpliktige opplysninger. Disse dokumenteres i pasientens journal i sykehusets journalsystem (DIPS) som ligger utenfor sykehusets DHO. Dette er opplysninger som vurderes som nødvendige og relevante for at sykehuset skal yte en forsvarlig behandling av pasienten. Dette kan inkludere å vite om måledata utenfor pasientens normalverdi eller en melding om at pasienten ikke lenger opplever effekt av behandlingen. Om måledata derimot viser normale verdier, eller en pasient ber om å få endre en time, er dette informasjon som helsepersonell kan anse som unødvendig å dokumentere, og forblir i sykehusets DHO.

I dag er det slik at helsepersonell ved sykehuset vurderer om deler av opplysningene som pasienten har sendt inn er journalpliktige, og fører disse manuelt inn i DIPS. Dette kan i framtidige løsninger skje automatisk ved at opplysningene overføres uten innblanding eller kontroll av helsepersonell. Begge disse måtene å overføre opplysninger på betyr at opplysningene allerede ved førstegangs registrering må ivaretas i tråd med de samme kravene til informasjonssikkerhet som i et journalsystem.

Pasienter eller deres fullmektig skal kunne bruke tjenesten uten å tenke på om det de formidler er journalpliktig. Hvor vidt opplysningene som formidles er journalpliktige eller ikke må vurderes av helsepersonell eller godt utprøvde automatiserte løsninger.

DHO-tjenesten til Ahus bruker Norsk helsenett (NHN) som kommunikasjonskanal. Det betyr at den er koblet på Helsenettet – et nettverk levert av Norsk Helsenett (NHN) – for å kunne sende helseopplysninger på en sikker måte. Før man kan benytte NHN, må man gjennom avtale forplikte seg til å følge Norm for informasjonssikkerhet (Normen) og personvern i helsesektoren (Normen). Normen stiller krav til informasjonssikkerhet og personvern i tråd med relevant regelverk og er tilpasset helseaktører.

Gitt opplysningenes karakter og at Ahus allerede bruker Norsk helsenett har vi sammen kommet frem til at fullmaktsløsningen må tilfredsstille samme krav til sikkerhet som et pasientjournalsystem.

Hvem har dataansvar?

Dataansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningen artikkel 4 nr. 7. Det er den dataansvarlige som er ansvarlig for, og som skal kunne påvise, at personvernforordningen overholdes, jf. ansvarsprinsippet i personvernforordningen artikkel 5 nr. 2. Den dataansvarlige er for eksempel ansvarlig for at det gjøres vurderinger av hva som anses som egnede tekniske og organisatoriske tiltak ved fullmaktsløsningen i henhold til personvernforordningen artikkel 24, 25 og 32.

I dette prosjektet er det Ahus som ønsker å knytte seg til en fullmaktsløsning. Formålet er å sikre at deres pasienter kan oversende korrekte og oppdaterte helseopplysninger til sykehuset og til relevante deler av kommunehelsetjenesten. Dette skal gjøre at pasienter skal kunne bo lengre hjemme, samtidig som de skal få den helsehjelpen de har behov for på en effektiv og god måte. Pasienten skal for eksempel slippe å reise til sykehuset for kontroll dersom det ikke er behov for dette. På samme måte vil pasienten kunne kalles inn til en tidligere kontroll, dersom opplysningene som rapporteres tilsier det.

Ahus bestemmer formålet med behandlingen av opplysningene og tilpasningen av fullmaktsløsningen, og vil dermed også være dataansvarlig.

Hva er relevante rettslige grunnlag?

I dette prosjektet har vi vurdert hva et rettslig grunnlag kan være for at en pasient kan ta i bruk en fullmaktsløsning som gir fullmektig tilgang til pasientens helseopplysninger i sykehusets DHO-tjeneste.

Personvernforordningen (GDPR) krever at all behandling av personopplysninger har hjemmel i ett av de seks rettslige grunnlagene oppstilt i artikkel 6 nr. 1 bokstav a til f.

Behandling av opplysninger av særlige kategorier, herunder helseopplysninger, jf. artikkel 9 forutsetter ytterligere vilkår for å behandle slike opplysninger. Behandling av helseopplysninger medfører at det må foreligge et unntak i artikkel 9 nr. 2 for å kunne foreta behandlingen.

Kommunikasjonen mellom pasienten og sykehuset regnes som et ledd i helsehjelpen Ahus gir. Etableringen av selve løsningen antas å være dekket av de generelle reglene som gjelder for behandling av personopplysninger i helsesektoren.

I vurderingen av rettslig grunnlag for å bruke løsningen overfor den enkelte pasient, kan samtykke være et aktuelt rettslig grunnlag, jf. artikkel 6 nr. 1 bokstav a, jf. artikkel 9 nr. 2 bokstav a.

For at et samtykke skal være gyldig, må det være frivillig, spesifikt, informert, utvetydig, gitt gjennom en aktiv handling, dokumenterbart og mulig å trekke tilbake like lett som det ble gitt, jf. artikkel 4 nr. 11 og artikkel 7. Ettersom løsningen skal behandle helseopplysninger, må samtykket i tillegg være «uttrykkelig» jf. artikkel 9 nr. 2 bokstav a.

Pasienten, som også vil være fullmaktsgiver, må få informasjon om hvordan opplysninger behandles, hvorfor de behandles, hvem som har tilgang, om mulighetene for å rette og slette helsedata, og om hvordan de kan begrense, og trekke fullmakten tilbake. Dette krever at Ahus lager en løsning med tydelig informasjon og med lett forståelige beskrivelser tilpasset den enkelte pasienten.

Kravet til frivillighet

En utfordring ved bruk av samtykke, som særlig må vurderes i dette tilfellet, er kravet til frivillighet.

Vi antar at noen pasienter ønsker å bo hjemme så lenge som mulig. En forutsetning for å bo hjemme er å kunne rapportere helseopplysninger til kommune og/eller sykehus. Klarer de ikke dette selv, må de samtykke til at assistenter, pårørende eller andre hjelpere får fullmakt til å utføre oppgavene.

Et samtykke er imidlertid ikke gyldig som rettslig grunnlag etter personvernforordningen hvis det foreligger press for å samtykke eller dersom det oppstår negative konsekvenser dersom man ikke samtykker. Den enkelte må være i stand til å foreta et fritt valg. Det kan sette frivilligheten under press hvis alternativet til å samtykke til å ta i bruk fullmaktsløsningen for eksempel er å bo på en helseinstitusjon.

Samtidig er det opp til pasienten selv å velge hvem som skal representere dem. I mange tilfeller er det pasienten selv som ansetter assistenter, og de kan selv velge hvem de ønsker at skal opptre som pårørende og andre hjelpere. Dette reduserer risikoen for at pasienten gir fullmakt til en person hen ikke ønsker å gi den til. Løsningen skal dessuten skreddersys slik at den som får fullmakt ikke får for vide fullmakter eller innsynsrettigheter. Med forutsetning om at løsningen kun skal brukes av pasienter med samtykkekompetanse og pasienten selv kan velge hvem det er som kan få fullmakt til å rapportere i helsetjenesten, samt hva fullmektig får tilgang til, er Datatilsynets vurdering at kravet til frivillighet som hovedregel vil være oppfylt.

På bakgrunn av forutsetningene ovenfor mener vi at samtykke i denne sammenhengen er et relevant rettslig grunnlag for bruk av den digitale fullmaktsløsningen.

Hva hvis pasienten ikke har samtykkekompetanse?
I de tilfellene der pasienten ikke har samtykkekompetanse, kan det være utfordrende å ta i bruk fullmaktsløsningen. Ahus må i slike tilfeller vurdere verge og andre rettslige grunnlag. Både personvernforordningen artikkel 6 nr. 3 og artikkel 9 nr. 2 krever i noen tilfeller et supplerende rettsgrunnlag i nasjonal lovgivning. Dette innebærer at den dataansvarlige må kunne påvise et rettslig grunnlag for den aktuelle behandlingen av personopplysninger både i personvernforordningen artikkel 6 og 9, og i nasjonal rett.

For personer uten samtykkekompetanse vil det som hovedregel også være etablert en vergeløsning, og man må vurdere om dette inkluderer ivaretakelse av pasientrettigheter.

Å sikre tilgjengelighet, konfidensialitet og integritet

I løsningen vil Ahus måtte imøtekomme krav til tekniske og organisatoriske tiltak for å sikre konfidensialitet, integritet og tilgjengelighet.

Personvernforordningen artikkel 32 setter krav til hvilke vurderinger og tekniske tiltak som må iverksettes for å oppfylle kravet om sikkerhet ved behandlingen. Av hensyn til prosjektets omfang er ikke alle vurderinger og tiltak dekket. Da tjenesten har som formål å tilgjengeliggjøre person- og helseopplysninger har vi valgt å trekke frem tilgangsstyring og sikring av sporbarhet som de viktigste tiltakene.

§ Sikkerhet ved behandlingen, jf. artikkel 32

Personvernforordningen artikkel 32 stiller krav til sikkerheten ved behandlingen av personopplysninger. Den behandlingsansvarlige skal fastsette «egnede tekniske og organisatoriske tiltak». For å avklare hva som er egnede tekniske og organisatoriske tiltak må dette ses i sammenheng med «den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Det er opp til den behandlingsansvarlige å gjøre denne vurderingen, men artikkel 32 kommer med eksempler på tiltak som kan være egnet for å oppnå et «sikkerhetsnivå som er egnet med hensyn til risikoen».

Se også Normen for utfyllende krav.

Tilgangsstyring

Tilgangsstyring innebærer plikt til å sikre at personopplysninger bare er tilgengelig etter tjenstlig behov. En god og riktig tilgangsstyring vil bidra til å sikre at konfidensialitet opprettholdes, fordi opplysningene kun er tilgjengelige for de som har blitt gitt tilgang. Den vil sikre integritet fordi brukeren kun har tilgang til å gjøre de endringene som kreves for å gjennomføre oppgaven, og den vil sikre tilgjengelighet fordi brukeren kun får tilgang til de opplysningene som er nødvendige for å gjennomføre oppgaven.

Dette krever at tilganger blir autentisert på en trygg måte. Det krever også at tilganger tildeles, administreres, kontrolleres og fjernes.

Kravet til tilgangsstyring fremkommer ikke eksplisitt av personvernforordningen, men det er en naturlig konsekvens av kravet til at den dataansvarlige skal gjennomføre «egnede tekniske og organisatoriske tiltak» etter personvernforordningen artikkel 32, jf. prinsippet om integritet og konfidensialitet artikkel 5 bokstav f. God tilgangsstyring er for eksempel helt nødvendig for å ivareta krav til taushetsplikt og etter helsepersonelloven § 21, jf. pasientjournalloven §§ 15 flg. og pasientjournalforskriften § 13.

I tilpasningen til NHNs fullmaktsløsning vil Ahus vurdere hvilke roller som skal ha tilgang til strukturerte og ustrukturerte data i sykehusets DHO. Ustrukturerte data – som for eksempel hvordan pasienten føler seg fra dag til dag, opplysninger om seksualitet, rus, mental helse og lignende – krever et annet nivå av konfidensialitet enn strukturerte data som for eksempel måledata om pasientens puls. Dette vil reflektere fullmaktsområdene som pasientene gir tilgang til, slik at det kommer tydelig frem hvem som får tilgang til de respektive områdene.

Tilgangsstyringen i en tenkt løsning vil kreve koordinering og samarbeid mellom helseforetakene, DHO-leverandørene og NHN. Når tilganger skal granuleres over flere nivåer må alle aktørene involveres. Først og fremst må dataansvarlige (helseforetakene) bestemme hvilke tilgangsnivåer som skal benyttes for deres DHO-løsning. Deretter må DHO-leverandørene tilpasse sine systemer basert på dette ønsket. Til slutt må NHN implementere de forskjellige tilgangsnivåene i sin tjeneste.

Gitt at granuleringsnivåene som reflekterer hvilke data de ulike fullmektigene får tilgang til ikke enda er definert, er det ikke klart hva som vil være tilstrekkelig informasjon for at pasientene skal kunne ta et informert valg av fullmaktsnivå.

En ny løsning der assistenter, pårørende og andre hjelpere logger på som seg selv og ikke som pasienten, vil øke pasientens kontroll med egne opplysninger, samt dataansvarliges mulighet til å kontrollere tilgang til helse og personopplysninger.

Krav om innebygd personvern

Ved utvikling av en ny fullmaktsløsning er det krav i personvernforordningen om innebygd personvern, jf. Personvernforordningen artikkel 25. Innebygd personvern og personvern som standard beskriver at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger. Dette for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i forordningen og verne de registrertes rettigheter.

Se gjerne mer i vår veiledning om innebygd personvern og personvern som standard.

Sikring av sporbarhet

Sporbarhet kan oppnås ved at systemet logger hvilke brukere eller identiteter som utfører ulike handlinger i løsningen. Disse handlingene kan for eksempel være lesing, registrering, endring eller sletting – avhengig av hvilke autorisasjoner brukerne har i systemet. For at logging skal være et effektivt tiltak for å sikre konfidensialitet må det også etableres loggkontroll. Logging av handlinger er verktøyet, og en forutsetning for å kunne gjennomføre det kontrollerende tiltaket, nemlig systematisk loggkontroll.

Dagens loggfunksjonalitet har utfordringer. I den fysiske permen kan loggføring enkelt bli glemt eller unngått, og i sykehusets DHO loggføres aktiviteten på pasientens profil. Praksisen gjenspeiler ikke med sikkerhet hvem som faktisk får tilgang til helse- og personopplysninger. Det vil være utfordrende for pasienten å vite hva pårørende, assistenter og andre hjelpere faktisk ser og skriver. En digital fullmaktsløsning vil gi nye muligheter. Til sammenligning vil et pasientjournalsystem ha krav til logging eller sporing av hvem som har hatt tilgang til helseopplysninger. Pasienten vil ha rett til innsyn i loggen, jf. pasientjournalforskriften § 14. Fullmaktsløsningen bør kunne gi de samme mulighetene. Ved å gi pasienten innsyn i denne loggen, vil vedkommende selv kunne ha kunnskap om og kontroll over hvordan den valgte fullmaktsordningen fungerer.

Denne type logging er et avgjørende teknisk eller organisatorisk tiltak for å sikre at konfidensialitet, integritet og tilgjengelighet ivaretas. Dette er fordi alle typer avvik kan spores og at nødvendig korrigering kan iverksettes.

Som et av helseforetakene i Helse Sør-Øst er Ahus pliktig til å etterleve «Norm for informasjonssikkerhet og personvern i helse- og omsorgsektoren» (Normen). Normen er en bransjenorm, utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren. Normens kapittel 5.4.4 legger føringer for hva som minimum bør registreres i tilgangslogger ved autorisert bruk av behandlingsrettede helseregisteret. Dette inkluderer:

- Identiteten til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger
- Organisatorisk tilhørighet (Ikke relevant for privatpersoner)
- Grunnlaget for tilgjengeliggjøringen
- Tidsperiode for tilgjengeliggjøringen

En fullmaktsløsning bør tilpasses på en slik måte at den dataansvarlige ved behov har tilgang på tilstrekkelig logg på alle hendelser som skjer i DHO-tjenesten. NHN vil på sin side loggføre hvilke personer som får hvilke tilganger til DHO-tjenesten.

Veien videre

I dette prosjektet har Ahus og Datatilsynet sett på muligheter og begrensninger ved å bruke en nasjonal fullmaktsløsning. Selv om det kan være mer krevende å samordne med andre aktører og få på plass tekniske løsninger, er vi enige om at det vil gi bedre sikkerhet og brukervennlighet å lene seg på en veletablert nasjonal aktør, heller enn å lage en egen løsning lokalt.

Hva med pasienter uten samtykkekompetanse?

Det er store forskjeller på hjemmeboende pasienters forutsetninger og behov i møtet med en DHO-tjeneste. Ahus og Datatilsynet har i dette prosjektet tatt utgangspunkt i pasienter som har samtykkekompetanse, og som derfor kan gi fullmakt til pårørende eller assistenter. På sikt kan man utvikle fullmaktsløsningen til også å fungere for flere pasientgrupper.

Dette kan være personer som er satt under vergemål eller barn, men også pasienter som av andre grunner ikke får tilgang til offentlige tjenester, som utenlandske borgere uten elektronisk ID, eller innbyggere som ikke ønsker digital kommunikasjon med det offentlige.

Ahus har for eksempel et økende antall mindreårige pasienter som har behov for, og rett til, å ta en mer aktiv rolle i egen helse fra fylte 12 år (Pasient og brukerrettighetsloven § 3-4). De har per i dag ingen mulighet til å kommunisere med helsepersonell i sykehusets DHO uten at foresatte har fullt innsyn.

Det vil også være et behov for å se nærmere på hvem som kan representere barn og andre pasienter uten samtykkekompetanse. I dag er det kun foreldre med samme registrerte bostedsadresse som barnet som har rett til å representere. Ahus ser at enkelte barn ikke kan få digital hjemmeoppfølging fordi deres omsorgspersoner ikke tilfredsstiller denne juridiske definisjonen. Noen har bonusforeldre, bor med fosterforeldre, andre bor med pårørende, enkelte har verge eller bor på institusjon og trenger hjelp av de som til enhver tid er ansatte der. Ahus etterlyser nye juridiske definisjoner av omsorgspersoner som bedre reflekterer virkeligheten.

For pasienter uten samtykkekompetanse kan vi se for oss at en verge eller annen representant kanskje bruker fullmaktsløsningen på deres vegne – men dette krever grudige rettslige og praktiske vurderinger, særlig rundt hvem som faktisk kan handle på vegne av pasienten.

Mot en nasjonal digital fullmaktsløsning i offentlig sektor

Dette prosjektet er ett eksempel som peker på et større behov. Offentlig sektor trenger fullmaktsløsninger som kan ha ulike nivåer og muligheter avhengig av hvilke oppgaver den med fullmakt skal utføre. Dette er ikke avgrenset til helsesektoren. Tilsvarende behov finnes i andre deler av offentlig sektor som ønsker at deres tjenester skal bli tilgjengelige for alle, inkludert de som trenger hjelp til å bruke dem.

Digitaliseringsdirektoratet har fått i oppdrag å utrede og utvikle en digital fullmaktsløsning for offentlige tjenester. Med dette prosjektet ønsker Ahus og Datatilsynet å bidra med innsikt om utfordringene og behovene fra en del av helsesektoren, om hvilke muligheter og begrensninger som finnes i eksisterende fullmaktsløsninger, og å løfte frem noen sentrale personvernspørsmål som kan benyttes i arbeidet med å sørge for at digitaliseringen kommer alle innbyggere til gode. Alle har rett til å bli inkludert, særlig når det gjelder tjenester fra det offentlige.

Besøksadresse:
Trelastgata 3, Oslo

Postadresse:
Postboks 458 Sentrum,
0105 Oslo

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

datatilsynet.no
personvernbloggen.no