Svar på høringsnotat:

Tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser
Etablering av virksomhetsovergripende behandlingsrettede helseregistre

Innholdsfortegnelse

Oslo universitetssykehus - Ullevål

2009

1. Innledning

Det er positivt at det nå foreslås endringer i lov for å gi bedre mulighet for tilgang til journalopplysninger på tvers av juridiske enheter. Hensikten og behovet begrunnes i å kunne gi pasientbehandlere den tilgangen på informasjon de trenger for å kunne utøve ansvarlig og effektiv pasientbehandling.

I dag kan pasienten behandles for samme sykdom av flere sykehus, avhengig av hvem som har ledig kapasitet i øyeblikket. Det kan også være pasientforløp der pasienten er definert innom flere foretak grunnet den økende spesialisering av sykehusene. Således er foretaket som autonom enhet i forhold til alle behandlingsforløp en historisk situasjon, og i fremtiden vil økende spesialisering medføre at stadig flere pasientforløp krysser grensene mellom foretakene og ulike nivåer av behandlingsapparatet. Samtidig er avhengigheten og forventningen til effektiv tilgang til eksisterende opplysninger, uavhengig av hvor de er, langt større enn virkeligheten kan levere.

Det økende kravet til tilgjengelighet til journalopplysninger på tvers av foretakene utfordrer samtidig taushetsplikten, siden sensitive personopplysninger potensielt eksponeres for en større mengde mennesker, hvorav kun et mindretall faktisk kan sies å ha autorisasjon for å se slike opplysninger i kraft av å være behandler for den aktuelle pasient. Samtidig vil det også være mange pasienter som fremdeles behandles kun av et foretak, og hvor eksponering for det større antall mennesker ikke kan sies å være berettiget.

Videre utvikling av håndtering av deling av journalopplysninger må således forventes å ivareta alle perspektiver av behovene og detaljert samhandling mellom foretak der det er nødvendig, uten at opplysningene blir eksponert for uvedkommende. Høringsnotatet som kommenteres, synes i for stor grad å forutsette at en generell åpning for tilgang til journalopplysninger på tvers av juridiske foretak, forholdsvis raskt og uten store økonomiske ressurser, vil kunne avdekke manglende tilgjengelighet, samtidig som taushetsplikten ikke påvirkes.

Videre synes det som om manglende løsninger har gitt en stor utålmodighet og at foreslått løsning forventes å være svaret på alle behov for deling av journalopplysninger.

2. Ulike behov for tilgang og deling – bør løses på ulike måter

Det synes å være stor tiltro til at denne lovendring vil medføre at disse utfordringer løses, men så langt er det ingenting som tyder på at en lovendring alene vil løse alle samhandlingsutfordringer gjennom å gi en så vid tilgang til pasientinformasjon på tvers av foretak.

Det er også viktig å være bevisst at det fremdeles er vesentlig handlingsrom innenfor dagens lovverk og fortolkning. Å benytte dette handlingsrom krever imidlertid ressurser som ikke har vært tilgjengelig.

En studie av Anders Grimsmo, bestilt av Shdir vinteren 2007, indikerer også at det er mer å hente på å etablere gode kommunikasjonsløsninger mellom helsearbeiderne, enn at de deler felles journal. Grunnen til dette synes å være at man i første tilfellet deler *kunnskap*, mens i andre tilfellet kun deler *informasjon*.

For å komme videre i arbeidet med å utvikle gode samhandlingsløsninger, tror Oslo universitetssykehus - Ullevål det er viktig å gjennomføre et virksomhetsarkitekturarbeid, der en identifiserer og beskriver de viktigste samhandlingsscenariene. Scenariene kan delvis fremskaffes gjennom å basere seg på arbeidet i NIKT's Nasjonal Systemarkitektur, samt ulike prosjekter rundt standardiserte behandlingslinjer. I tillegg vil det sannsynligvis være behov for enkelte arbeidsmøter der informasjonen fra disse prosjektene analyseres og videre bearbeides med samhandling som formål.

Eksempler på aktuelle scenarier kan være:

- Akutte pasienter som får del-behandling ved regionssykehus (PCI/Hjerteinfarkt, hjerneslag)
- Pasientoppfølging på ulike sykehus, avhengig av kapasitet og kompetanse (Kreft)
- Oppfølging av inneliggende pasient ved et foretak av leger fra annet foretak (Funksjonsfordeling)
- Planlagt pasientforløp mellom ulike foretak (strålebehandling)
- "Second opinion"/bakvakt fra spesialist ved annet foretak
- Prehospitale tjenester og behandlingsforløp, inkludert forberedelse inn mot ulike akuttmottak.

Med utgangspunkt i slike scenarier, vil en kunne gjøre en vurdering av hvordan ulike teknologiske løsninger har styrker og svakheter i forhold til de gitte scenariene, og hva som skal til for at behovene for samhandling dekkes. Videre vil dette kunne danne grunnlaget for å identifisere hva som faktisk er lovmessige hindringer og hva som er ressursmessige eller tekniske hindringer og utfordringer (forankring, prioritering, økonomi, kompetanse, tid med mer).

Det er overveiende sannsynlig at de ulike scenariene vil ha forskjellige prefererte tekniske løsninger. Således kan en videre drøfte om det er mulig å implementere en løsning for å dekke alle behov, eller det må etableres komplementære løsninger for å dekke de ulike behovene.

Den endring som foreslås i høringsutkastet går meget langt i det å tilsidesette store pasientgruppers behov for konfidensialitet. Dette kan i verste fall undergrave den tilliten som er nødvendig i helsevesenet for å gi god behandling. Det må sørges for at taushetsplikt og personvern blir ivaretatt på en slik måte at pasienten er vernet mot at opplysninger blir spredt til uvedkommende. Manglende tillit kan medføre at :

- Pasienter ikke vil gi fra seg nødvendig informasjon
- Helsepersonell dokumenterer sparsomt
- Noen pasientgrupper ikke tør oppsøke helsetjenesten

Tilgang til nødvendige, oppdaterte og korrekte pasientdata er av avgjørende betydning for utfallet av kliniske beslutningsprosesser. Samtidig har pasienten også en forventing om og tillitt til at opplysninger ikke skal være tilgjengelig for uvedkommende. Dette innebærer at selv om noen pasientgrupper har behov for at det gis en utvidet mulighet for tilgang til opplysninger, så må man ikke gå for langt i denne retning når det gjelder pasienter som ikke har dette behovet.

3. Områder som bør videre bearbeides

3.1. Databehandlingsansvar kontra bruk av opplysninger

I kommentar til hjemling av ny hlsrgl § 6 a anføres det at begrensningen i nåværende hlsrgl 6 om hvem som kan være databehandlingsansvarlig for behandlingsrettede helseregistre ikke vil komme til anvendelse for virksomhetsovergripende registre. At registrene er virksomhets-overgripende nevnes i denne sammenheng som et argument i seg selv for at andre enn de som selv tar i bruk registeret kan være databehandlingsansvarlig.

Iflg Hlsrgl § 2 nr 7 er et behandlingsrettet helseregister et journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har fore-byggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger, Nærmere regler om pasientjournalen, som utgjør innholdet i behandlingsrettede helseregistre, er fastsatt i helsepersonelloven. Virksomheter hvor det ytes helsehjelp er pålagt å opprette pasientjournalsystem, jfr forskrift om pasientjournal § 4. Det er derfor et ganske detaljert regelverk som angir formål og nærmere regler for behandlingsrettede helseregistre. Å yte helsetjenester er uløselig knyttet til det å kunne samle inn, tolke og lagre opplysninger om pasienten.

Databehandlingsansvarlig er iflg hlsrgl § 2-8 den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes. Den som er databehandlings-ansvarlig, er også den som er strafferettslig og sivilrettslig ansvarlig for brudd på loven. Prinsipielt bør databehandlingsansvaret påhvile den som er ansvarlig for virksomheten. Kun utøvende helsetjeneste bør derav være databehandlingsansvarlig.

3.2. Ansvar for kontroll med formål og registrertes rettigheter

Databehandlingsansvarlig er ansvarlig for både at bruken av opplysninger er innenfor formålet til registeret/behandlingen, samt at den registrertes rettigheter ivaretas. Åpning for direkte tilgang til journalopplysninger i annet foretak, åpner opp for en del spørsmål som må avklares nærmere:

1. *Kontroll med formål* – Hvem er ansvarlig for at innsamlede opplysninger kun benyttes til formål eksisterende hjemmelsgrunnlag gir grunnlag for? Normalt er dette data-behandlingsansvarlig, og formål journal gir rammer for hva opplysningene kan brukes til og av hvem, uten at nytt hjemmelsgrunnlag må innhentes. Eksempelvis vil bruk av opplysninger til forskning, kreve samtykke fra den registrerte og intern kvalitets-sikring basert på HPL § 26 begrenser bruken innen databehandlingsansvarlig som foretak. En teknisk tilgang til journalopplysninger i et annet foretak, gir ingen kontroll med at opplysningene kun brukes i samsvar med databehandlingens formål, og ikke også brukes til andre formål som forskning. Innhenting og bruk av journal-opplysninger til forskning i annet foretak, innebærer en utlevering som skal ha et hjemmelsgrunnlag. Ansvarsforholdet ved potensiell bruk/misbruk av opplysninger hentet fra annet foretak til andre formål enn helsehjelp må avklares nærmere.

Sikring av rettigheter – Hvordan og av hvem skal den registreres rettigheter sikres? Normalt er det databehandlingsansvarlig som er ansvarlig for at den registreres rettigheter sikres. Igjen kan forskning som et eksempel brukes. Forskning vil typisk kreve et aktivt samtykke fra den inkluderte, om opplysningene skal kunne brukes til forskningsformålet. Dersom foretak som

henter opplysninger fra annet foretak, også bruker disse opplysninger til forskning uten å innhente samtykke, hvilket ansvar for den registreres rettigheter påhviler det den som egentlig har samlet inn opplysningene i pasientens journal? Ansvarsforhold og forpliktelser til å sikre den registrertes rettigheter, eksempelvis rett til å samtykke til nytt/annet bruk enn registerets formål må avklares nærmere.

3.3. Tekniske forutsetninger og derav økonomisk behov

Realisering av foreslått lovendring for å tilgjengeliggjøre journalopplysninger på tvers av juridiske enheter synliggjør i begrenset grad den økonomiske forutsetning som må ligge til grunn for at mulighetene i lovendringsforslaget skal kunne benyttes.

Mulighetsrommet i eksisterende lovverk er langt fra benyttet hva gjelder å dele/kommunisere journalopplysninger på tvers av juridiske enheter/foretak. Begrensede økonomiske ressurser i foretakene må tillegges en stor årsak for dette. I en årrekke er både investeringsbudsjett og menneskelige ressurser beskåret til et minimum, samtidig som forventinger om at IT skal gjøre helsehjelpen mer rasjonell er stadig økende.

I det følgende gjennomgås noen sentrale aspekter som er nødvendige for å benytte de muligheter en ny lovendring vil gi:

3.3.1. Nivå på autentisering

Realisering av foreslått lovforslag vil kreve at autentisering i langt de fleste foretakene må styrkes. Dette er klart et ønske også av andre årsaker, men har likevel ikke kunnet realiseres grunnet begrensede økonomiske ressurser.

Tilgang på tvers av foretak vil med krav i personopplysningslovgivningen og tilhørende sikkerhetsnorm forutsette at autentisering må heves til hva som er refereres til som 2-nivå autentisering. Dette krever en form for sertifikater eller tilsvarende. Selv om dette ikke krever nivå kvalifiserte sertifikater, krever det likevel en stor investering i hele helsenorge for at det kan åpnes for tilgang mellom juridiske enheter.

Dette igjen krever store investeringer som trolig også vil måtte gripe inn i selve sikkerhets-arkitekturen for store deler av foretakene. Dette er en ønsket heving av sikkerheten, men er like fullt en svært ressurskrevende forutsetning for at foreslått lovendring skal kunne effektueres.

3.3.2. Mangler i teknisk tilgangsregulering i journal

For å etablere elektronisk tilgang til opplysninger i journal, gis den enkelte ansatte en teknisk tilgang basert på rolle(dvs type dokumenter som det skal gis tilgang til), geografi(dvs gruppering av relevante avdelinger den enkelte helsearbeider har funksjon innen), og tid(dvs tilgang så lenge pasienten er til behandling). Dette gir en tilsynelatende ryddig og grei begrensning av tilgang, samtidig som tilgangen til journalen faktisk sikres. Dette bildet blir imidlertid forstyrret av at pasienter ikke alltid er planlagt inn, langt fra kan forutsies hvilke avdelinger som er relevante for den enkeltes behandling, hvem som til enhver tid er på vakt, med mer, som gjør at oppsettet med tekniske begrensninger på tilgang kun er et ideelt rammeverk. Videre vil pasienter også kontakte sykehuset for spørsmål etter behandlingen er gitt. Her er det et utall varianter og kombinasjoner som gjør, at for å sikre at legen faktisk alltid får tilgang til journalopplysninger ved behov, har autoriserte brukere også en funksjon som i Doculive (OUS-UUS/OUS-RH/Helse Bergen/StOlav/HelseMidt) heter "aktualisering"

og i DIPS (store deler av Sør-Øst, Vest og Nord) heter "Grønnlys". Denne funksjon sikrer at de som er autorisert, får mulighet til selv å beslutte at de skal åpne en hvilken som helst journal innen egen juridiske enhet. Her har dermed behovet for å sikre tilgjengelighet medført en risiko for taushetsplikten ved uberettiget bruk av teknisk mulighet for oppslag. Denne rettigheter gis til både leger, et større antall sekretærer, for at disse skal kunne gjøre sin funksjon for legen, samt et betydelig antall av pleiepersonell. Dermed har svært mange ansatte teknisk tilgang til store deler av pasientenes journaler. Dette er gjort for å sikre tilgjengelighet når det faktisk er behov, men det gir en teknisk mulighet for svært mange til å slå opp i en hvilken som helst journal. For å gjøre oppslag med denne funksjonen, må det angis en årsak som dokumenteres i en logg, og journalen vil åpnes som forespurt ut fra den enkelte helsearbeiders beslutning. Det at beslutningen gjøres av den enkelte helsearbeider, og at dette også omfatter sekretærer og et stort antall pleiepersonell, er i følge tilsynsmyndighet ikke i samsvar med hva de tolker som regulert i lov. Beslutning om tiltak kan ikke gjøres av alle de som har fått denne tekniske tilgangen. Det som da hindrer dem i å gjøre oppslagene er at de ikke har lov, ref uttalt i sykehusets Sikkerhetsinstruks, men det gir ikke noen teknisk hindring.

Dette er avdekket av Helsetilsynet og Datatilsynet på deres tilsyn som det finnes offentlig tilgjengelige rapporter fra. Det jobbes kontinuerlig med å forsøke å forbedre dette med eksempelvis noe henvisningsbasert tilgang. En slik endring vil eksempelvis kunne benyttes for å gi patologer, laboranter, rtg-avdelinger tilgang til pasientens journal, når det er rekvirert prøver/bilder. Selv om tankearbeidet for dette er kommet et langt stykke på vei, er likevel den faktiske situasjonen som beskrevet i avsnittet over, og svært mange ansatte har dermed en teknisk tilgang som gir dem mulighet til å åpne en hvilken som helst journal i sykehuset. Dette er videre også kjent av ansatte på sykehusene, og er fremkommet under tilsyn og kjent hos tilsynsmyndighet etter bekymrede telefoner fra ansatte som er pasienter. Det er også kjent som årsak til at ansatte enten ikke vil være pasient på eget sykehus, eller ber legen ikke føre journal. Det siste går jo da på bekostning av tilgjengelighet, og når det ikke journalføres, vil neste behandler ikke kunne vite hva som er gjort.

En åpning av teknisk tilgang på tvers mellom foretak vil ytterligere øke denne mulighet for teknisk tilgang uten hjemmel for oppslag. Det er søkt å sette krav til at den tekniske tilgangen skal begrense oppslagene i annet foretak til aktuell pasient som er til behandling i eget foretak. Selv om tanken er god, er den harde realitet at det ikke finnes tekniske løsninger som kan realisere dette. En realisering av teknisk løsning som skal etterkomme intensjonen i lovforslag og også intensjonen i inneværende lov innen den enkelte juridiske enhet, vil forutsette store økonomiske ressurser og en større endring i eksisterende journalsystemer. Det tar lang tid å få slike strukturelle endringer gjennomført. Dette gjelder alle leverandørene av journaler.

3.3.3. Sperrefunksjon

Pasientene har som kjent sterk medbestemmelsesrett i hvem som skal kunne få gjøre oppslag i sin journal, og kan derav kreve sperring av hele eller deler av egen journal. Denne mulighet er for så vidt etablert i journalløsningene, men gir i liten grad tilstrekkelig funksjonalitet for å etterkomme pasienters ønsker om å nyansere hvem det skal sperres/åpnes for.

Det er grunnlag for å tro at bruken av krav om sperring vil øke med en økt tilgang. Det vil videre også bli behov for å kunne sperre mellom juridiske enheter. Ansatte som også er pasienter velger nå i noen grad annet enn eget foretak som behandlingssted. Disse vil med stor sannsynlighet kreve sperring mot ansatte fra eget foretak.

Også disse endringer er ønskelige, men det skal ikke undervurderes hva dette vil koste i direkte utgifter for endring hos journalleverandør, samtidig som det trolig vil kreve en større bemanning for å etterkomme krav om sperring fra pasienter.

3.3.4. Opplæring i ulike journalløsninger

Foreslått håndtering med at helsepersonell gis lesetilgang til andre foretaks journalsystem, setter krav til at helsepersonellet må læres opp til et visst minimum på de relevante journalløsninger de vil ha tilgang til. Dette er ikke minst ressurskrevende for helsepersonellet, som får et langt større antall elektroniske løsninger å forholde seg til.

Dette vil også innebære en kost, som i større grad krever ressurser fra selve helsepersonellet for å kunne gjennomføres. Se neste kapittel som alternativ løsning/håndtering av å gi alle tilgang til alle løsninger.

3.3.5. ”Digital Interhospital Forløpsjournal” (DIF)

Et alternativ til at alle journalløsninger skal åpnes opp for å leses i på tvers, ville være å etablere ”Digital Interhospital Forløpsjournal” (DIF), som etableres som en organisering og tilgjengeliggjøres av opplysninger mellom foretak ved behov, og hvor kun de som er behandlende helsepersonell for aktuell pasient tilknyttes mulighet for tilgang. Den som behandler pasienten, tilknytter på denne måten neste behandlingsledd/-foretak identifisert ved relevant personell. Denne måten å organisere delingen på tvers av foretak begrenser delingen til de pasienter som behandles på tvers, og forhindrer at øvrige pasienter blir eksponert ut over eget foretak.

Denne måten å organisere tilgang til journalopplysninger på tvers av foretak vil også kreve ressurser, men vil gi en målrettet tilgang pr pasient, som samtidig sikrer taushetsplikten for øvrige pasienter og imøtekommer behovet for å ikke dublere opplysninger.

3.4. Ansvar og konsekvens for å innhente mulige opplysninger

Når opplysninger i en ordinær virksomhetsintern pasientjournal brukes ved ytelse av helsehjelp til en pasient, får virksomheten ansvar for at helsehjelpen foregår forsvarlig og i tråd med anerkjente faglige prinsipper. Det kan spørres om muligheten til tilgang til helseopplysninger i andre registre medfører aktivitetsplikt i forhold til å skaffe seg de opplysninger som ligger i registeret. Den samlede mengde av opplysninger vil kunne gi et annet bilde av pasientens situasjon enn hva opplysningene i den enkelte virksomhets pasientjournal gir. Det er ikke upraktisk å tenke seg at det kan forekomme motsetninger mellom de opplysninger om en og samme pasient som ligger i de forskjellige virksomheters EPJ system.

For eksempel kan det i et register være opplysninger om at en pasient står på en bestemt type medikasjon som innebærer at man må utvise særskilt aktsomhet for eksempel ved kirurgiske inngrep. Ut fra hensynet til pasienten bør ansvarsforholdene knyttet til dette være betryggende. I det minste bør det være slik at den som yter helsehjelp og gjør oppslag i et annet register må få ansvar for å opptre faglig forsvarlig i forhold til det samlede informasjonstilfang vedkommende har gjort seg kjent med. Derfor er det av stor viktighet å bevare det øyeblikksbildet som ble presentert da et helsepersonell benyttet direkte tilgang til registeret.

Det bør derfor i mer detalj avklares:

- hvilket ansvar påhviler den enkelte lege å søke alle opplysninger, dvs må legen sjekke alle steder pasienten har journal?
- hvilken konsekvens medfører det for den enkelte lege og foretak om ikke alle opplysninger søkes og gjennomgås?
- hvem er ansvarlig for konsekvens ved feilaktige opplysninger eller feilaktige tolkningen av det man finner hos andre juridiske enheter? Bruken av medisinske begreper og måter å bruke journalen på er forskjellig.

3.5. Rett til fornyet vurdering

Hvordan gi reel mulighet til fornyet vurdering for den enkelte pasient hvis den enkeltes journal i andre virksomheter er tilgjengelig eller synlige som sperrede dokumenter?

3.6. Logging – og gjennomgang av logger

Aktivitet i journalløsninger logges. I denne sammenheng er det relevant å understreke at loggingen likevel ikke hindrer uberettigede oppslag, men gir mulighet for å dokumentere slike i ettertid.

Gjennomgang av hva som er ikke akseptable oppslag, er svært ressurskrevende, og kun gjennomførbart med stikkprøver. Det er flere initiativ for å forsøke å systematisere og målrette logg-gjennomganger, slik at den manuelle gjennomgangen kun blir på et håndterbart antall logger. Dette gjør at effekten av loggjennomgang foreløpig er svært begrenset.

Oslo universitetssykehus – Ullevål erfarte følgende i en sak som ble meldt Helsetilsynet. Den ansatte som ble mistenkt for å ha gjort opp mot 30 ulovlige oppslag mot en pasients journal, forklarte til Helsetilsynet at vedkommende enten måtte ha gått fra PC-en pålogget, eller at noen hadde lest vedkommendes passord som var nedskrevet i en bok. Alle ansatte signerer på å ha lest virksomhetens Sikkerhetsinstruks, hvor slik atferd angis som ikke akseptabel. Helsetilsynet tilla ikke Sikkerhetsinstruksen og den krav noen tyngde, og mente at HF-et ikke hadde gjort nok for å undersøke om den ansatte faktisk var på arbeid angitte tidspunkt i loggen. Sammenlignet med Kreditinstitusjoners krav til og Kredittilsynets tilhørende forutsetning for kundens påpasselighet av pin-kode, var Helsetilsynets reaksjon overraskende. Dersom ikke den ansattes påpasselighet av passord for tilgang skal kunne forventes og vektlegges, vil det kun være de som faktisk innrømmer uberettiget innsyn, som vil kunne identifiseres. Dersom Helseforetaket ikke kan tillegge forventning og forutsetning om påpasselighet av passordet hos den ansatte, vil logging ha en tilnærmet null-effekt på sikkerheten.

3.7. Midlertidig sperring av tilgang

§ 16 Krav om register over og kontroll av autorisasjonene - merknader:
Det er satt krav til at midlertidig fravær på eksempelvis 4 ukers ferie, skal medføre en midlertidig sperring av brukerkonto. Dette er ikke praktisk mulig i en virksomhet med mange tusen ansatte. Samtidig er det viktig at tilganger/autorisasjoner jevnlig skal kontrolleres. Krav må imidlertid settes mer generelt, slik at det kan være mulig å få dette praktisk gjennomført.