Høringsuttalelse

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Innhold

Generelt 2
Til Kapittel I Innledende bestemmelser 3
Til § 1 Forskriftens formål 3
Til § 2 Forskriftens virkeområdet 3
Til § 3 Definisjoner 4
Til Kapittel II 4
Generelle krav til informasjonssikkerhet 4
Teknologiske forhold 4
Til Kapittel III 5
Krav om system for utstedelse av autorisasjoner og krav til autentisering 5
Til § 14 Autorisasjon for ytelse av helsehjelp 5
Til Kapittel IV 5
Tilgang til helseopplysninger i behandlingsrettet helseregister 5
Til Kapittel V 5
Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter 5
Til §§ 22 - 24 6
Til § 25 Krav til autentisering 6
Til Kap VI 6
Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter 6
Til §§ 27 – 28 Om samtykke 6
Til §§ 29 – 30 Om sperring 6
Til økonomiske og administrative konsekvenser 6
Konklusjon 7

Innledning

Det vises til høringsbrev av 10.5.2010 med høringsfrist 10.september 2010 med vedlagt høringsnotat

http://www.regjeringen.no/nn/dep/hod/Dokument/Hoyringar/Hoyringsdokument/2010/Horing-av-forslag-til-forskrift-om-informasjonssikkerhet-tilgangsstyring-og-tilgang-til-helseopplysninger-i-behandlingsrettede-helseregistre/Horingsnotat.html?id=604372

Generelt

Forskriften stiller store krav til systemer før pasientinformasjon kan deles. Dette gjelder både innenfor og utenfor virksomhet. Slik bestemmelsene er utformet sørger de for at personvernet blir godt ivaretatt dersom kravene blir fulgt.

Høringsbrevet etterspør om balansen mellom det praktikable og pasientenes tillit til at sensitive informasjon ikke kommer på avveie, blir ivaretatt i forskriften. Kommunen har kommet til at reglene i praksis vil være for tids- og ressurskrevende både på system- og tilgangsnivå. Resultatet av dette kan da enten bli at reglene ikke etterleves, eller at informasjonsdeling er så vanskeliggjort at formålet med forskriften ikke oppnås.

I kommunen vil informasjonsdeling stille relativt store krav til ressurser både mht til personell og system. Umiddelbart kan en også se utfordringen med at kravene i kapittel II og III oppfylles, men at disse i praksis, ved tilgangsdeling, ikke følges fordi systemet blir for tungvint og komplekst. En annen utfordring er at det gis tilgang til pasientinformasjon etter retningslinjene, men at tilgangskontrollen ved avslutning blir for svak og sikkerhetssjekk/sporing ikke blir utført.

Det er ved gjennomgang av høringsnotatet, utfordrende å se hvilke konsekvenser forslagene vil få i detalj for den kommunale helsetjenesten. HOD ber imidlertid konkret om at høringsinstansene vurderer om balansen mellom praktikable regler som er til hjelp for helsepersonell i deres arbeid med å gi helsehjelp til pasienter, og de organisatoriske og administrative rutiner som må på plass for å etterleve forskriften.

Kommunal helsetjeneste er bl.a. preget at mange aktører, som trolig faller inn under begrepet ”virksomheter” i det aktuelle regelverket. Dette er døgnkontinuerlige tjenester, ofte med begrenset tilgang til IT-kyndig personell i store deler av døgnet/uken. Mange aktører bidrar i korte og lengre perioder med helsehjelp overfor samme pasient på kort varsel, ofte utenom arbeidstid, med behov for å dele EPJ-/informasjon i behandlingsrettede registre.

Tilgangsstyring og autorisasjon må for eksempel fungere slik at når en legevaktslege kommer på sykebesøk til en pasient på et sykehjem kl. 03 en søndag morgen, må det være personell til stede som kan gi vedkommende anledning til å lese hele pasientens EPJ og skrive i denne, samt samhandle elektronisk med helseforetak om pasienten fra samme system.

Mange virksomheter er små, andre er både små og organisert i fellesskap mellom enkeltmannsforetak, og således trolig i denne sammenheng hver for seg i hht. forskriften det som defineres som en ”virksomhet.” Dette gjelder for eksempel fastleger. Disse vil med regelmessighet ha behov for å arbeide i EPJ til pasienter tilhørende hverandres lister ved fravær, for eksempel når en lege arbeider med offentlig legearbeid for kommunen 1-2 dager/uke. Dette vil det i hht.

Samhandlingsreformen bli mer av for hver lege. Turnusleger arbeider for eksempel konsekvent på flere leger sine lister samtidig, og må således ha tilgang til alle "virksomhetene" sine EPJ-databaser/registre. Disse skifter hver 6. måned.

I høringsnotatet s. 18 står det at informasjonssikkerhetstiltakene må være tilpasset virksomhetens art, aktiviteter og størrelse. Denne holdningen gjenfinnes imidlertid ikke i selve forskriftsforslaget, med unntak av merknadene til § 5 annet ledd.

Til Kapittel I Innledende bestemmelser

Til § 1 Forskriftens formål

Viser til § 1 andre punktum*: Videre er formålet å bidra til god informasjonssikkerhet*
Hensikten med å etablere en forskrift om virksomhetsovergripende, behandlingsrettede helseregistre er å gi helsepersonell mulighet til å gi forsvarlig helsehjelp til pasienter i et samarbeid mellom virksomheter. Det framgår av tidligere utredninger og forarbeider til helseregisterloven at balansegangen mellom effektiv utveksling av informasjon om pasienter og personvernhensyn krever gode systemer som ivaretar kvaliteten på den informasjon som blir delt mellom flere virksomheter. Kommunen mener at formålsbestemmelsen i *§ 1 andre punktum* ikke ivaretar dette hensynet tilstrekkelig idet uttrykket "bidra til" i det siste forskriftsforslaget blir for lite forpliktende.

I drøftelsen til bestemmelsen i pkt 4.1.3 vurderes det om uttrykket "tilstrekkelig informasjonssikkerhet" skal endres til "god informasjonssikkerhet". Her har departementet falt på at formålsbestemmelsen skal synliggjøre styrket informasjonssikkerhet og forskriftsforslaget benytter "god informasjonssikkerhet". Det er imidlertid ikke gitt noen drøftelse av bruken av uttrykket "bidra til".

I forrige forslag til forskrift av 20. oktober 2008 hadde formålsbestemmelsen en annen formulering:

> *§ 1 Forskriftens formål*
> *Formålet med forskriften er å bidra til å gi helsepersonell nødvendig elektronisk tilgang til helseopplysninger slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte uten å krenke personvernet. For å virkeliggjøre dette skal forskriften sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, kvalitet, integritet og tilgjengelighet.*

I dette forslaget ble uttrykket "sørge for" benyttet uten at det framgår av høringsnotatet hvorfor departementet har gått bort fra dette mer forpliktende uttrykk. Det er mulig man har vurdert at informasjonssikkerheten blir ivaretatt andre steder i forskriften, men kommunen mener at formålsbestemmelsen vil være av avgjørende betydning for hvordan den blir forvaltet. Hvis begge punktumene i formålsbestemmelsen skal ha like stor vekt i praksis, bør kravet til bestemmelsen om informasjonssikkerhet styrkes med et annet uttrykk. Dette kan gjøres ved å uttrykke "sørge for" eller "ivareta". Ordet "videre" bør også fjernes for å gi setningen et mer presist uttrykk som f. eks *"Formålet er også å ivareta/sørge for god informasjonssikkerhet*". Det vises også til forskriftens § 4 hvor det pålegges virksomhetene å "sørge for"….. forsvarlig informasjonssikkerhet.

Til § 2 Forskriftens virkeområdet

Det er vanskelig å forstå innholdet i denne bestemmelsen fordi den inneholder uttrykket "som skjer" som ikke viser tilbake på noe. I tidligere forslag viste uttrykket "som skjer" tilbake på "behandling av helseopplysninger". Denne delen av bestemmelsen er endret, og den nye utformingen gir ikke lenger en forståelse av hvilken handling som henviser til helseregisterloven § 6 og helsepersonelloven § 46.

Til § 3 Definisjoner
Det antas at det er gjort en nummereringsfeil ved at pkt 5 er blitt en a). Definisjonene vil bli tydeligere dersom ”helseopplysninger” verken blir tatt med i definisjonsuttrykkene eller i påfølgende definisjon. Fokus er i for stor grad på helseopplysninger der hvor det er ”tilgang”, ”direkte tilgang” og ”sperrede” som skal defineres. Det bør vurderes om ”helseopplysinger” skal defineres for seg.

Forskriften regulerer deling av pasientinformasjon for både store og små virksomheter. Forskriften stiller store krav til systemene i de enkelte virksomheter som vil anvende forskriften for å ha muligheten til å dele/få informasjon. Reglene bør derfor være utformet på en måte som gjør det mulig også for de små virksomhetene å lett oppfatte innholdet i forskriften. Av den grunn er det ønskelig med en definisjon av ”virksomhet” slik at den enkelte virksomhet rask kan fastslå hvilke krav som stilles til den. I høringsnotatets side 31 gis det en oversikt over virksomheter, men dette er lite ”brukervennlig”. Forklaringen bør stå allerede i § 3 sammen med de andre definisjonene.

Til Kapittel II
Generelle krav til informasjonssikkerhet

Under høringsnotatets kap. 4.4.3 (side 17) står det følgende i avsnitt 2:

> ”*God informasjonssikkerhet krever organisatoriske så vel som tekniske og fysiske tiltak. Organisatoriske tiltak omfatter klare ansvarslinjer, gode rutiner hos alle som bruker systemet/behandler helseopplysninger, risikovurderinger, dokumentasjon av informasjonssystemene m.v.”*

Tiltak som opplæring/holdningsskapende arbeid kunne med fordel vært med i denne setningen, selv om opplæring fremheves mange steder senere i høringsnotatet. Et annet stikkord under organisatoriske tiltak er et godt internkontrollsystem. Dette skal både forebygge brudd i sikkerheten og ivareta en beredskap som skal sikre skadebegrensning når brudd skjer. Videre står det:

> *”God informasjonssikkerhet kan ikke alene ivaretas eller måles ut fra de tekniske funksjonalitetskrav et system har”.*

Hele høringsnotatets innhold bærer preg av, med rette, at det er på det organisatoriske området utfordringen i forhold til sikkerhet ligger.

Teknologiske forhold
Når det gjelder de delene av sikkerheten som er knyttet til tekniske forhold, er det vanskelig å være spesifikk. Kommentarene nedenfor er derfor ”runde og generelle”.

En hovedårsak til at det er vanskelig å være spesifikk på teknologi, er at det finnes et ukjent antall ulike systemer innenfor helsesektoren som faller inn under kategorien ”behandlingsrettede helseregistre”. Disse systemene er basert på ulik teknologi, og de varierer i størrelse fra små lokale systemer med 1-2 brukere og opp til de store foretakene og nasjonale registre med tusenvis av brukere.

Generelt kan det sies at de tekniske sikkerhetsmekanismene er mange og gode, og de er under løpende utvikling og forbedring. Verktøyet ligger altså der, og det er opp til det enkelte foretak og registereier å sikre at disse brukes riktig slik at kravene til teknisk sikkerhet blir ivaretatt.

En utfordring i denne sammenheng er å finne en fornuftig balansegang mellom sikkerhetstiltak (både organisatoriske og tekniske) og kompleksiteten for brukerne. Jo flere og mer komplekse tekniske sikkerhetsbarrierer en bruker må forholde seg til, jo større er muligheten for å feile. Likeså kan rutiner gjøres så detaljerte og innfløkte at brukerne blir illojale og finner "snarveier" rundt dem.

Den største teknologiske utfordringen når det gjelder sikkerhet, blir antakelig i utveksling av data mellom ulike systemer og ulike foretak. I definisjonen for *direkte tilgang til helseopplysninger* i forskriftsforslagets § 3 pkt. 4 heter det:

> *"Helsepersonell kan logge seg rett inn på et behandlingsrettet helseregistersystem og fra dette systemet logge seg rett inn på andre behandlingsrettede helseregistersystem, internt i virksomheten eller i ekstern virksomhet. Pålogging kan skje……"*

En ting i denne sammenheng er de rent sikkerhetsmessige tekniske forhold knyttet til pålogging, overføring av data over nettet etc. En annen ting er hvorledes data er lagret i de ulike systemene, hvorledes pasienten identifiseres i systemene etc. Konvertering av data lagret i ett spesielt format i et system, må ofte konverteres til et annet format for å kunne håndteres i et annet system.

Som det også står i høringsnotatet, er forarbeidet som må gjøres mellom de ulike foretakene og systemene særdeles viktige.

Til Kapittel III
Krav om system for utstedelse av autorisasjoner og krav til autentisering

Til § 14 Autorisasjon for ytelse av helsehjelp
Kravene i merknadene til § 14 første ledd (s 51) om at pasientjournalen skal struktureres slik at psykisk og somatisk sykdom skal kunne skilles helt ad, er umulig. I kommunal helsetjeneste vil dette vanskelig la seg gjennomføre. Både hjemmesykepleie og fastleger skal se pasienten i en helhet, i sitt sosiale miljø. Psykisk og somatisk helse er så sammenknyttet at dette skillet ikke faller logisk, videre vil det gi en uryddighet i journalen som vil svekke dens funksjonalitet.

Til Kapittel IV
Tilgang til helseopplysninger i behandlingsrettet helseregister

Se merknader til kapittel II.

Til Kapittel V
Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

Kravene i kap. V synes i utgangspunktet vel funderte. Det vil imidlertid kunne bli en utfordring for kommuner som har for eksempel fysio- og ergoterapitjenesten organisert i annen virksomhet enn pleie- og omsorg. Disse har allerede erfaring for at det å be om særskilt tilgang for hver enkelt pasient er så krevende at det ikke er praktikabelt. Dette gjelder altså i en tjeneste som fungerer kun på dagtid på hverdager. For døgnbaserte tjenester med et betydelig innslag av øyeblikkelig hjelp funksjoner vil denne utfordringen trolig mangedobles

Til §§ 22 - 24
Når det gjelder bestemmelsen om avtale (kap V) som på forhånd skal inngås mellom virksomheter, vil dette i praksis sannsynligvis bli ordnet ved at en virksomhet inngår avtale med de virksomheter den til enhver tid samhandler mest med.

Forskriftsteksten og merknadene til bestemmelsene henviser til at det er tenkt at det skal ligge en generell avtale til grunn mellom de enkelte virksomhetene før det kan gis lesetilgang. Kravene til at en avtale kan inngås er likevel så spesifikke jfr. § 22 med behovs- og nødvendighetsvurderinger, at det ser ut til at det må være et konkret behov for å yte helsehjelp som utløser en avtale. Dette vil være tidkrevende og lite anvendelig i praksis. Det burde være tilstrekkelig med en avtale hvor avtalepartene sjekker hverandres sikkerhetssystemer m.m. uten nærmere krav om beskrivelse av hva informasjonsutvekslingen skal inneholde. De sistnevnte opplysninger og vurderinger bør heller kreves i forbindelse med en konkret forespørsel, jfr. § 26.

I forhold til balansen mellom behov for å yte helsehjelp og personvernsikkerheten i forhold til avtalekravene er det etter kommunens syn blitt for omstendelig å få tilgang til informasjon. Det vil også være tids- og arbeidskrevende for kommunen som har flere samhandlende virksomheter som vil komme til å ønske tilgang i våre systemer.

Til § 25 Krav til autentisering
I merknadene til bestemmelsen vises det til at "kvalifisert sertifikat" er nærmere regulert i e-signaturloven § 4. Forskriftens § 25 bør ha en henvisning til denne bestemmelsen slik at det er lettere å forstå hva et kvalifisert sertifikat innebærer.

Mht spørsmålet om det skal gis muligheter for unntak fra kravet om bruk av kvalifisert sertifikat støtter kommunen departementets absolutte forslag i § 25. Dette blir en sikkerhetsmekanisme i forhold til den enkelte som gis tilgang til helseregistre og det vil kunne fange opp svikt i de andre generelle systemene.

Til Kap VI
Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

Til §§ 27 – 28 Om samtykke
Til §§ 29 – 30 Om sperring
Disse to første bestemmelsene om samtykke er så vesentlige for hele informasjonsdelingen at de bør synliggjøres bedre ved å flyttes til de innledende bestemmelsene. Et annet alternativ er å sette dem i samme kapittel som sperringsbestemmelsene *"Om samtykke til og sperring av helseopplysninger".*

Til økonomiske og administrative konsekvenser
For å sikre et godt personvern(ivareta rettsikkerheten til pasient/bruker) må pasient/bruker være sikker på at egne helseopplysninger sikres for innsyn av helsepersonell som trenger opplysninger for å yte forsvarlig helsehjelp. I høringsnotatet henvises det til en Norm for informasjonssikkerhet, http://www.kith.no/templates/kith_page____1912.aspx Normen er utgitt som en veileder sammen med et faktaark (nærmest en IK- prosedyre).

Normen er lite kjent ute i kommunene, og den er p.t. heller ikke samkjørt med gjeldende regelverk. Det er helt nødvendig at dette gjøres før helseregistertilgangene igangsettes. Det er fremkommet at bare 46 % av kommunene er påkoblet Norsk helsenett. Høringsnotatet opplyser om at alle som inngår forpliktende avtale med Norsk helsenett må forplikte seg til å etterleve normen. Dette er igjen et kostnadsspørsmål for kommunene.

For kommunene vil opplæringen i bruk av Normen være svært ressursskrevende, det samme vil innføringen av forskriften om informasjonssikkerhet osv….. I mange kommunene blir det snakk om kjøp, drifting og opplæring av elektroniske systemer.

Helsetjenesten er ressursmessig presset. Mange virksomheter, spesielt de mindre, har begrensede muligheter til å frigjøre de ressursene som skal til for både å etablere den faglige og administrative overbygningen, og for å etablere egen databehandlingsansvarlig ressurs som forskriftsforslaget innebærer uten tilføring av ressurser.

Store deler av helsetjenesten er bundet av egenandelsbestemmelser og andre rammer som gjør at den økonomien som må til for å få dette på plass ikke kan skaffes fra pasientene/egenbetalingen. De tilpasningene som må gjøres i EPJ-systemene vil kostnadsmessig måtte havne hos tjenesteyterne/virksomhetene.

Kravene i kap. VII i forskriften medfører nye, konkrete, regelmessig repeterte arbeidsoppgaver for virksomheten. I tillegg står det eksplisitt i § 34 at det ikke kan kreves betalt for de delene av arbeidet som pasientene evt. genererer direkte. Departementets forutsetninger om at de forelagte myndighetskrav kan gjennomføres innen gitte budsjettrammer i helsevirksomhetene må således være hevdet mot bedre vitende. Det er derfor helt nødvendig at de merkostnader som forslagene medfører for virksomhetene/helsepersonell må kompenseres fullt ut fra statlig hold, både overfor kommuner, fysioterapeuter, fastleger o.a.

Konklusjon

Forskriftsforslaget synes samlet sett i vesentlig større grad å ivareta formålsparagrafens intensjon om informasjonssikkerhet enn forsvarlig og effektiv helsetjeneste. Mange av forslagene for ivaretakelse av informasjonssikkerhet er gode, men vil i en ressursknapp, travel døgnbasert tjeneste med begrenset tilgang til systemeier, ikke være praktikable og gi risiko for begrensede tilganger og muligheter for journalføring og elektronisk samhandling som kan sette pasienters liv og helse i fare. En evt. vilje til å finansiere tilgang til både etablering av systemer, overordnet struktur og håndtering av tilganger til enhver tid vil i noen grad kunne bøte på disse manglene ved forslaget.

Det kan synes som om ønsket om å lage en felles forskrift for virksomheter av svært ulik størrelse har medført at myndighetskravene er lagt på et nivå som fordrer en struktur og ressurser som ikke finnes i mindre kommuner og andre mindre virksomheter.

De tekniske sikkerhetsmekanismene er mange og gode, og de forbedres fortløpende. Forutsatt at systemutviklere og IT-personell utnytter de mulighetene teknologien gir, og forutsatt at systembrukere/databehandlere får kunnskap i å bruke disse, bør den tekniske delen av de sikkerhetsmessige aspektene være tilfredsstillende ivaretatt i forslaget til forskrifter.

- Det må sikres at personvernet ivaretas fullt ut.
- Staten bør utarbeide opplæringsplaner for implementeringen, herunder holdningsskapende arbeid blant all helsepersonell, IK prosedyrer og intern og ekstern informasjon
- Kommunene må gis full kompensasjon for innføring av tilgangen til helseregistrene

- Staten må sikre at det utarbeides et rammeverk for utveksling av data mellom databasene i de ulike EPJ-systemene
- Utgitt Norm for personvern osv må samordnes gjeldende lovverk
- Bruk av Norsk helsenett bør være kostnadsfritt for kommunene