Datatilsynet

Helse- og omsorgsdepartementet
Postboks 8011 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
14/3724-	14/01084-2/EOL	14. november 2014

Datatilsynets høringsuttalelse - Forskrift om tilgang til helseopplysninger mellom virksomheter

Datatilsynet viser til oversendt høringsnotat av 19. september 2014. Våre synspunkter på høringsnotatet og Helse- og omsorgsdepartementets forslag til forskrift om tilgang til helseopplysninger mellom virksomheter er som følger:

Tilgjengelighet fremfor konfidensialitet

Innledningsvis vil vi bemerke at det fremstår som underlig at Helse- og omsorgsdepartementet i høringsnotatet legger til grunn at det å gi helsepersonell mulighet til å gjøre oppslag i andre virksomheters elektroniske pasientjournaler styrker personvernet. Dette er en feilslutning som vi mener må korrigeres. Det må være åpenhet omkring det faktum at departementet lar hensyn til tilgjengelighet gå foran hensyn til konfidensialitet ved vedtakelsen av denne forskriften. Dette sier vi ikke fordi vi er motstandere av å åpne for at helsepersonell skal ha tilgang til nødvendige opplysninger om sine pasienter, men fordi vi mener en erkjennelse av at tilgjengeligheten i denne sammenhengen går på bekostning av konfidensialitet er viktig for å kunne fastslå under hvilke forutsetninger slik tilgang skal tillates.

Mer detaljregulering eller godkjenningsordning

Departementet har flere steder i forslaget presisert at de ytre rettslige rammene for tilgang til helseopplysninger mellom virksomheter er **helsepersonellets taushetsplikt**, samt at opplysningene som innhentes skal være **relevante og nødvendige** for å yte, administrere eller kvalitetssikre **helsehjelp til den enkelte pasient**. Datatilsynet oppfatter dette som at pasientjournalloven § 19 og den foreliggende forskriften ikke innebærer faktiske endringer i rammene for hva helsepersonell har adgang til å skaffe av helseopplysninger om den enkelte pasient. Pasientjournalloven § 19 endrer imidlertid rammene for hvordan helseopplysningene kan innhentes, og forskriften her skal gi en nærmere beskrivelse av hvordan dette skal skje i praksis. Endringen består i at helsepersonell i en virksomhet selv skal kunne hente helseopplysninger om en gitt pasient hos en annen virksomhet.

De ytre rettslige rammene gjelder som nevnt allerede i dag. Dette har ikke forhindret at helsepersonell har tilgang til helseopplysninger om pasienter de ikke er involvert i behandlingen av, samt tilgang til flere helseopplysninger om enkeltpasienter enn det som er

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

relevant og nødvendig for den helsehjelpen de skal gi. Dette er en situasjon som Datatilsynet ved flere tilfeller har avdekket ved kontroll av tilgangsstyring i helsesektoren, og som blir bekreftet av Riksrevisjonens rapport «Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013» som ble levert Stortinget 11. november 2014. Riksrevisjonen er tydelig på at det pr i dag er for enkelt for ansatte i helseforetakene å få tilgang til helseopplysninger utover det de har behov for i arbeidet sitt, og at det er Helse- og omsorgsdepartementets ansvar å sørge for at helseforetakenes praksis blir i tråd med regelverket som gjelder for tilgang til helseopplysninger.

Datatilsynet mener Riksrevisjonens rapport peker på svakheter ved dagens journalsystemer som det er helt grunnleggende å få korrigert før det åpnes for tilgang til pasientjournaler mellom virksomheter. For å komme i mål med utviklingen av systemer som ivaretar den funksjonaliteten som er nødvendig for konfidensialitetssikring må det stilles klare krav til systemleverandørene. Datatilsynet er enig med Riksrevisjonen i at dette er et ansvar som ligger på sentrale myndigheter, i denne sammenheng Helse- og omsorgsdepartementet.

Departementet sier i høringsnotatet at det ikke vil være hensiktsmessig med konkrete tekniske krav fordi det er viktig at reglene tar høyde for teknologisk utvikling. Datatilsynet er ikke uenig i dette utgangspunktet, men samtidig mener vi at forskriften må ha en merverdi sammenlignet med de krav som allerede følger av blant annet pasientjournalloven, personopplysningsloven og personopplysningsforskriften. Med det innholdet forslag til forskrift har nå mener vi at merverdien er minimal.

Vi mener det er fullt mulig å stille krav til teknologisk modenhet som ikke vil være til hinder for teknologisk utvikling. For eksempel vil et krav om at pasientjournalene skal være strukturerte være krav til den tekniske plattformen som ikke vil påvirke videre utviklingen. Vi mener dessuten at krav til at det skal være mulig å sortere helseopplysningene i en pasientjournal er grunnleggende for å kunne hevde at tilgang på tvers mellom virksomheter ivaretar taushetsplikt og kravet om at tilgangen kun skal omfatte relevante og nødvendige opplysninger for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte pasient.

På denne bakgrunn mener vi at departementet enten må gi en større grad av detaljregulering i forskrift eller sørge for en godkjenningsordning for de virksomheter som skal åpne for tilgang på tvers. Vi har noen forslag til presiseringer og tilføyninger som vi mener vil bidra til både å gi forskriften et innhold som er nyttig for de som skal innrette seg etter den, samt bidra til et bedre personvern for pasientene.

Forskriftens § 1 Formål
Datatilsynet støtter at rammene for tilgang til helseopplysninger mellom virksomheter presiseres til å gjelde opplysninger som er **relevante og nødvendige for** å yte, administrere eller kvalitetssikre **helsehjelp til den enkelte pasient**.

Forskriftens § 2 Virkeområde
Datatilsynet mener det er positivt at departementet gjør det klart at forskriften ikke gjelder tilgang til helseopplysninger for andre formål enn helsehjelp til den enkelte pasient.

Det er også positivt at begrepet «tilgang» defineres, men vi mener at den valgte ordlyden ikke gjør det tydelig at det er et prinsipielt skille mellom lese- og skrivetilgang. Vi går utfra at bakgrunnen for dette er at departementet holder det åpent om tilgang i visse tilfeller skal kunne inkludere skrivetilgang.

Skillet mellom lese- og skrivetilgang er sentralt for ivaretagelsen av informasjonssikkerhet og opplysningers integritet. Datatilsynet mener det er helt sentralt å opprettholde dette skillet. Enten må skrivetilgang uttrykkelig forbys, eller så må slik tilgang reguleres spesielt. Slik ordlyden i forslaget er nå er det altfor åpent hva en tilgang på tvers kan omfatte av rettigheter.

Departementet redegjør i høringsnotatet for grunner til at det ved åpning for tilgang til helseopplysninger hos andre virksomheter i utgangspunktet ikke skal være adgang til å registrere eller endre opplysninger i registeret. Blant annet vektlegges viktigheten av at det skal være enkelt å skaffe seg oversikt over hva som er gjort hvor. Vi støtter disse betraktningene, og mener at de veier så tungt at det skal mye til for å åpne for unntak. Dersom det skal åpnes for skrivetilgang må dette defineres som unntak og tillates etter særskilte vilkår.

Forslag til klargjørende tekst:
«Med tilgang menes at helsepersonell gis adgang til å søke frem og lese et avgrenset sett med helseopplysninger om pasienter som de aktivt deltar i behandlingen av».

Forskriftens § 3 Grunnvilkår
Datatilsynet støtter departementets forslag om en bestemmelse som angir tekniske og organisatoriske forutsetninger som må være på plass før en virksomhet kan inngå avtale om tilgang til helseopplysninger på tvers av virksomhetsgrenser.

Vi støtter også forslaget om å presisere at grunnkravene i forskriften ikke erstatter andre sikkerhetskrav, men kommer i tillegg.

Departementet har valgt å trekke frem avtale, risikovurdering og tilfredsstillende informasjonssikkerhet som de tre grunnvilkårene som må være oppfylt. Dette er viktige vilkår, men av disse tre er det kun kravet om avtale som går noe lengre enn de plikter som allerede følger av lov. For å gi forskriften en merverdi mener vi at det må stilles krav til **strukturering av pasientjournal**.

I sin behandling av pasientjournalloven la Stortinget vekt på at en eventuell deling av helseopplysninger mellom virksomheter ville kreve at det forelå en viss grad av strukturering av opplysninger i de pasientjournalsystemene virksomhetene bruker. Journalsystemene må kunne gjøre et skille mellom opplysninger som kan deles og opplysninger som ikke kan deles. Dette henger sammen med at tilgangen som gis kun skal være til opplysninger som er

relevante og nødvendige for helsehjelpen til den enkelte. Et grunnvilkår om strukturering vil således være i tråd med de forutsetninger som Stortinget la vekt på da pasientjournalloven ble vedtatt.

Vi ser at departementet har omtalt dette i høringsnotatet og forutsetter det også som en forståelse av vilkåret om tilfredsstillende informasjonssikkerhet. Datatilsynet mener imidlertid at dette er et så viktig premiss for tilgangen at den burde fremgå eksplisitt av forskriften. Det bør følgelig fremgå tydelig at virksomheter som ikke har mulighet til å sortere helsopplysninger innenfor pasientjournalsystemet ikke kan inngå avtale om tilgang for tvers.

I tillegg bør det fremgå hva man mener med begrepet «strukturert» i sammenheng med pasientjournal. Vi foreslår at begrepet gis en definisjon i forskriften.

For krav til journalsystem kan det være relevant å se hen til internasjonale standarder, som ISO/TS 14441[1].

Forskriftens § 4 Avtaleinnhold
Bestemmelsen som er foreslått er ment å angi minstekrav til innholdet i avtalen mellom de virksomhetene som vil gi tilgang på tvers mellom pasientjournaler. Under forutsetning av at disse minstekravene er tilstrekkelig konkrete vil dette være en bestemmelse som er til reell hjelp for de som skal forholde seg til forskriften. Slik minstekravene er formulert i forslaget mener vi at de ikke tilfører nok utover gjeldende regelverk.

Kravet om behovs- og risikovurdering, samt krav om rutiner gjelder for eksempel uavhengig av denne forskriften. Å gjenta disse pliktene har åpenbart en pedagogisk verdi, og vi er enige i at de bør fremgå av denne forskriften. Utarbeidelse av forskrift for en såpass spesifikk måte å behandle helseopplysninger gir imidlertid en mulighet til å gi disse pliktene et mer konkret innhold. Denne muligheten er etter vår mening ikke utnyttet godt nok.

I tillegg introduserer departementet et nytt begrep, *journalmodul*, som gjør at det reelle innholdet i kravet til avgrensning blir uklart. Departementet sier i høringsnotatet at de har vurdert å ta inn en bestemmelse som definerer nøkkelbegreper, men har kommet til dette ikke er nødvendig da begrepene helsehjelp, databehandlingsansvarlig og behandlingsrettet helseregister er definert i pasientjournalloven.

Datatilsynet er enig i at det ikke er nødvendig å gjenta definisjoner av begreper som er definert i pasientjournalloven. Etter vår mening er det heller ikke nødvendig å gi definisjoner av begreper som er godt innarbeidet og som helsepersonell er godt kjent med innholdet i. Når departementet introduserer nye begreper mener vi imidlertid et dette nødvendiggjør forklaringer av hva de betyr. Et eksempel på at departementet har gjort nettopp dette er ved introduksjonen av begrepet «tilgang» som er gitt en definisjon av i forskriftens § 2.

[1] ISO/TS 14441 Health informatics- security and privacy requirements of EHR systems for use in conformity assessment.

Begrepet «journalmodul» er ikke gitt noen forklaring i merknadene, og er så vidt oss bekjent ikke er allment kjent begrep. Til tross for dette er det brukt som en helt sentral avgrensing i forskriften. Avtalen mellom virksomhetene skal angi hvilke journalmoduler det skal gis tilgang til. Hvis en «journalmodul» for eksempel kan være «elektronisk pasientjournal» vil dette ikke være en avgrensning som tar inn over seg kravet til strukturering og muligheten til å hente ut kun relevante og nødvendige helseopplysninger.

Datatilsynet foreslår at begrepet «journalmodul» tas ut og erstattes et innarbeidet begrep som for eksempel «fagsystem». En avgrensning til fagsystem vil dessuten være egnet til å oppnå søkeresultat som nærmer seg kravene til at helseopplysningene som innhentes skal være relevante og nødvendige. Dersom det i tillegg stilles krav om søk på kategorier av opplysninger vil et søkeresultat faktisk være i nærheten av relevante og nødvendige opplysninger.

Forskriftens § 4 bokstav c kan for eksempel omformuleres slik:

c) hvilke typer helseopplysninger som det gis tilgang til, og fra hvilke fagsystemer opplysningene hentes.

For å tilføre forskriften en merverdi, og hjelp til de som skal utarbeide avtalene, mener vi det vil være nyttig å stille helt konkrete krav til innholdet i avtalen, samt holde på innarbeidede begreper som helsepersonell er kjent med innholdet i.

Vårt forslag er at det i tillegg til krav om behovs- og risikovurderinger tas inn krav om:

1. Oversikt over hvilke **nødvendige og strukturerte** helseopplysninger det gis tilgang til mellom avtalepartene, og fra hvilke fagsystemer de hentes.

2. Beskrivelse av hvilken tilgang som er avtalt.
   -Gjensidig tilgang, eller bare tilgang fra en av partene.
   -Generell eller spesifikk tilgang. Åpning for alle fagsystemer og alle grupper helsepersonell, for en bestemt gruppe helsepersonell og rettet mot en bestemt pasientgruppe, tilgang i enkelttilfeller etter forespørsel

3. Beskrivelse av ansvarsforhold og fordeling av oppgaver i forbindelse med tilgang på tvers mellom virksomhetene. Herunder hvem som sikrer at de opplysningene som faktisk blir hentet er relevante og nødvendige.

4. Beskrivelse av hva som skal skje ved oppsigelse av avtalen.

5. Avtale om tilgang til helseopplysninger på tvers av virksomheter skal publiseres

Forskriftens § 5 Informasjonssikkerhet
Forskriften setter som forutsetning for deling av helseopplysninger at tilgangen *ikke svekker informasjonssikkerheten i noen av virksomhetene.* Datatilsynet mener at det å åpne for en videre tilgang til pasientjournal per definisjon øker risikoen for svikt med hensyn til konfidensialitet (ivaretagelse av taushetsplikt). For det tilfellet at det åpnes for skrivetilgang øker også risikoen for svikt med hensyn til integritet (at opplysningene er korrekte). Den delen av informasjonssikkerheten som forbedres som en følge av videre tilgang er tilgjengeligheten.

Dersom forutsetningen om at informasjonssikkerheten ikke skal svekkes hos noen av virksomhetene, må det iverksettes konkrete tiltak for å gjenopprette balansen mellom konfidensialitet og tilgjengelighet.

Det bør stilles krav om at både avgivende og mottakende virksomhet skal **vurdere og akseptere** risikoen, og sørge for kompenserende tiltak. Denne forutsetningen bør fremgå eksplisitt av ordlyden i forskriften.

Ordlyden i pasientjournalloven § 19, tredje ledd tilsier at forskriften skal inneholde konkrete krav til risikovurderingene som skal gjøres før det åpnes for tilgang på tvers. Etter vår mening må risikovurderingene omfatte minst følgende:

1. hvorvidt eget system kan sikre at det kun gis tilgang til «relevante og nødvendige» opplysninger.
2. om kommunikasjonspartens systemer i tilstrekkelig grad ivaretar taushetsplikten og lovens øvrige krav.

Det ligger implisitt i dette at en risikovurdering som ikke tar inn over seg en faktisk økt risiko for dårligere ivaretagelse av konfidensialitet ved å åpne for tilgang på tvers, ikke vil være tilstrekkelig.

Forskriftens § 6 Autorisasjon
Datatilsynet støtter forslaget om en egen bestemmelse som stiller krav til autorisasjon av helsepersonell som skal gis tilgang til helseopplysninger i en annen virksomhet.

Forskriftens § 7 Tilgangsstyring
Når tilgang til pasientjournaler skal tillates på tvers av virksomhetsgrenser er tilfredsstillende tilgangsstyring avgjørende for å ivareta pasientenes krav på konfidensialitet omkring sine helseopplysninger.

Virksomhetenes utfordring i denne sammenheng er å sørge for at riktig helsepersonell får tilgang til relevante og nødvendige helseopplysninger om riktig pasient.

For å oppnå dette er det helt nødvendig at opplysningene i pasientjournalen er strukturert på en måte som gjør det mulig å foreta spesifikke søk.

Det er også avgjørende med tekniske og organisatoriske tiltak som sørger for at det er riktig person som blir gitt tilgangen til en annen virksomhets fagsystemer. Datatilsynet støtter derfor departementets krav om sikker autentiseringsløsning. Vi mener imidlertid at det bør tas inn en hovedregel om at det er den forespørrende virksomhet sin tilgangsstyring som skal benyttes i likhet med systemet for loggkontroll. Dette fordi det er virksomheten som skal hente helseopplysninger om en pasient som vet hvem som er involvert i pasientbehandlingen og som har reell mulighet til å styre tilgangen til dette helsepersonellet.

Forslag til ny § 7 d:
«Når en virksomhet skal benytte tilgang til helseopplysninger i en annen virksomhet skal denne tilgangen som hovedregel gå gjennom autorisasjons- og autentiseringsmekanismer i begge virksomheters systemer.

Dersom tilgang kun går gjennom autorisasjons- og autentiseringsmekanismer i virksomheten hvor helseopplysningene som det skal gis tilgang til befinner seg, skal dette eksplisitt risikovurderes, og reguleres i avtalen mellom virksomhetene ».

I tillegg til krav om strukturering, sikker autentisering og presisering av hvilke autorisasjons- og autentiseringsmekanismer som skal gjelde mener vi det vil gi forskriften en merverdi dersom den angir noen helt konkrete spørsmål som skal besvares før det gis tilgang i det enkelte tilfelle. Dette er et tiltak som kan kompensere for at det inngås en generell avtale om tilgang istedenfor at det skal avtales i hvert enkelt tilfelle.

Eksempler på spørsmål skal besvares før helseopplysninger hentes fra en annen virksomhets pasientjournal:

- Hvilken type helsehjelp er pasienten inne for å få?
- Hva er det som begrunner oppslag i pasientjournal hos en annen virksomhet?
- Hvilke opplysninger er det relevant og nødvendig å innhente?

Svarene på disse spørsmålene bør være tilgjengelig i begge parters informasjonssystem.

Forskriftens § 8 Informasjon til pasient
Datatilsynet støtter forslaget om en egen bestemmelse som stiller krav til informasjon til pasienten. Målrettet informasjon til rett tid til pasienten er grunnleggende for å ivareta personvernet i denne sammenheng. Informasjonsplikten bør imidlertid konkretiseres ved å stille krav om en frist for på hvilket tidspunkt informasjonen må være gitt pasienten, samt krav om at informasjonen skal gis skriftlig.

Forskriftens § 9 Sperring
Datatilsynet støtter forslaget om en egen bestemmelse som gir pasienten rett til å sperre sin journal for innsyn, samt informasjon om denne rettigheten. I likhet med retten til informasjon er retten til å velge hvilke opplysninger som skal være tilgjengelige for hvem grunnleggende for personvernet.

Slik bestemmelsen er formulert kan det se ut som pasientens mulighet til å sperre sin journal er begrenset til sperring for innsyn av enkeltpersoner eller grupper av helsepersonell. Dette er

en viktig del av sperremuligheten, men etter vår mening er det like viktig å ha muligheten til å sperre enkeltopplysninger eller opplysninger om enkeltbehandlinger. For eksempel opplysning om abort, HIV-test, psykiatri eller andre behandlinger som er egnet til å stigmatisere en person.

Forskriftens § 10 Dokumentasjon (logg)
Datatilsynet støtter forslaget om en egen bestemmelse som gir en plikt til å særskilt loggføre oppslag i pasientjournal fra andre virksomheter.

Det bør imidlertid fremgå direkte av forskriften at denne type logg skal finnes i begge virksomhetenes fagsystemer. Et konkret oppslag skal med andre ord kunne kontrolleres både hos avgivende og forespørrende virksomhet.

Forskriftens § 11 Oppfølging av logg
Datatilsynet støtter forslaget om en egen bestemmelse som gir en plikt til å følge opp avvik fra bestemmelsene om tilgang, samt plikt til å informere pasienten om slike avvik.

En slik bestemmelse er særlig viktig i lys av at Riksrevisjonen i sin rapport «Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013» avdekket at ingen av de helseforetakene de undersøkte har noen form for systematisk kontroll og oppfølging av ansattes tilganger i EPJ. Dette til tross for at alle helseforetakene har utarbeidet prosedyrer som slår fast at loggkontroller av ansattes oppslag i pasientjournaler skal gjennomføres rutinemessig.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO