Datatilsynet

Helse- og omsorgsdepartementet
Postboks 8011 Dep

0030 OSLO

Deres referanse	Vår referanse	Dato
201001921-/ASD	10/00551-3 /bso	17. september 2010

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

Det vises til departementets høringsbrev av 10. mai 2010 om forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre. Datatilsynet fikk utsatt høringsfrist til 17. september 2010.

1 Innledning

Tillit til helsevesenet er viktig og helt nødvendig for å kunne gi forsvarlig pasientbehandling. Den enkelte skal ha tillit til at helsepersonell har rask tilgang til nødvendige opplysninger når det trengs for pasientbehandlingen, men skal også ha tillit til at personvernet ivaretas. Godt personvern skaper tillit. Det er skjæringspunktet mellom disse behovene denne forskriften skal ivareta. Dersom sensitive helseopplysninger urettmessig gjøres tilgjengelig over store deler av landet og pasientenes tillit svekkes, slik at pasienter holder tilbake informasjonen som føles særlig privat, kan hensikten med denne forskriften tvert imot resultere i negativ effekt på helsehjelpen.

Datatilsynet ser behovet for bedre samhandlingsløsninger og er positive til en samtykkebasert kjernejournal i kombinasjon med elektronisk meldingsutveksling. Kjernejournal er en samhandlingsform som godt ivaretar behovet for tilfredsstillende informasjonsdeling og samtidig sikrer pasientens autonomi. En kjernejournal vil kunne løse samhandlingsbehovet for pasienter som har et særskilt behov for at visse opplysninger skal være mer tilgjengelige for eksempel kronisk syke, akutte tilfeller eller andre som vil slippe å gjenta sine helseopplysninger hver gang de oppsøker ny behandler eller helseinstitusjon.

Datatilsynet ser at det kan være samhandlingsbehov også utover det en samtykkebasert kjernejournal og meldingsutveksling kan ivareta, og at tilgang på tvers i visse tilfeller er nødvendig for å gi forsvarlig pasientbehandling.

Datatilsynet vil her påpeke at dette forslaget til forskrift fremstår som vesentlig bedre enn det som tidligere har vært fremlagt. Datatilsynet er positive til at forskriften nå har implementert en rekke av lovgivers forutsetninger for tilgang på tvers.

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

Det fremheves i forarbeidene at det er akkurat den samme tenkingen som ligger til grunn for tilgang på tvers og kjernejournal, og at det er en veldig begrenset del av journalen som skal gjøres tilgjengelig på tvers.

Datatilsynet ser et klart behov for å sikre at systemene faktisk oppfyller regelverkets krav for tilgang på tvers og mener det er behov for en nærmere klargjøring. Tilgangsstyringen må sikre at det bare er nødvendige, relevante og strukturerte opplysninger det gis tilgang til. Lovforarbeidene har også oppstilt krav til strukturering av pasientjournaler. Datatilsynet mener en nærmere klargjøring også bør ses i sammenheng med arbeidet omkring nasjonal- og regional kjernejournal. Datatilsynet ser på det som viktig og ønskelig å få bistå i arbeidet både med kravene til systemer for tilgang på tvers og kjernejournal.

Datatilsynets gir her en relativt omfattende uttalelse. Det er viktig for tilsynet å støtte opp under den retning arbeidet med forskriften nå har tatt med å implementere lovgivers intensjoner og støtte departementet på punkter vi mener ivaretar personvernet på en god måte. Datatilsynet mener det hadde vært mer hensiktsmessig med et nærmere samarbeid ved utarbeidelsen av forskriftsforslaget, slik lovforarbeidene til helseregisterloven forutsetter.[1] Datatilsynet har kompetanse og erfaringer fra tilsyn med tilgangsstyring og logg i behandlingsrettede helseregistre, som er relevant i forbindelse med dette forskriftsarbeidet. Vi ønsker derfor et konstruktivt samarbeid rundt det videre arbeidet med kravene til systemer for tilgang på tvers og kjernejournal.

Det er viktig, men ikke tilstrekkelig, at forskriften oppstiller overordede krav for å åpne opp for tilgang på tvers. Det må i tillegg utarbeides gode systemer som sikrer at kravene etter gjeldende rett etterleves i praksis. Det er viktig at regelverkets krav til teknologi klargjøres nærmere. En slik klargjøring trenger ikke nødvendigvis å fremkomme i forskriften, men kan komme på et nivå under forskrift for eksempel i form av rundskriv. Helsedirektoratet har allerede utarbeidet et forslag til minstekrav for tilgang på tvers. Datatilsynet mener direktoratets forslag til minstekrav er et godt utgangspunkt for videre arbeid på dette punkt.

Ekstern tilgang til pasientjournaler i en virksomhet forutsetter god styring og kontroll internt. Det er vanskeligere å føre kontroll med ansatte i andre virksomheter, enn det er å holde kontroll med egne ansatte. Helseforetakenes interne tilgangsstyring har allerede vært gjenstand for en rekke kontroller og kritikk fra både Helsetilsynet og Datatilsynet. Tilsynsmyndighetene har avdekket at de elektroniske pasientjournalene som benyttes ved sykehusene ikke er egnet til å gi den enkelte en tilgang som er tilfredsstillende begrenset til vedkommendes tjenstlige behov. Det er videre avdekket at helseforetakene har dårlig kontroll med hvilke opplysninger den enkelte ansatte faktisk tilegner seg gjennom sin tilgang. Tilsvarende funn er gjort ved mange helseforetak. Dette tyder på at avvikene til en viss grad er systemavhengige.[2]

---

[1] I Ot.prp.nr.5 (1999-2000) side 195 er følgende uttalt om helseregisterloven § 16 fjerde ledd: "Som faginstans har Datatilsynet som hovedoppgave å formulere de overordnede sikkerhetsbehov i form av konkrete krav til konfidensialitet, integritet og tilgjengelighet. Fastsetting av eventuelle særlige krav for
behandling av helseopplysninger må derfor gjøres i tett samarbeid med Datatilsynet, og være mest mulig i harmoni med sikkerhetskravene som stilles etter personopplysningsloven." (Vår utheving)

[2] Datatilsynets rapport april 2009 Sviktende tilgangsstyring i elektroniske pasientjournaler

På bakgrunn av disse svakhetene bør man gå forsiktig frem med å utvide tilgangen til også å gjelde eksterne parter. Datatilsynet mener fastsetting av minstekrav til systemer er et velegnet verktøy for å sikre at kravene i regelverket etterleves. Det er viktig at pasienter har tillit til at det verken er juridisk, teknisk eller faktisk mulighet for uvedkommende å tilegne seg informasjon de ikke skal ha.

Lovendringene vil kreve betydelige ressurser. Departementet har fastslått at gjennomføringen av kravene skal skje innenfor de ordinære budsjettrammer. I en virkelighet hvor helsetjenesten opplever at økonomien er presset, er det en fare for at dette arbeidet ikke vil bli prioritert og at pasient- og personverninteresser blir satt til side av rene ressursøkonomiske hensyn. Tilsynet anbefaler derfor at det bevilges øremerkede midler for å sikre at tilgangen til landets pasientjournaler er sammenfallende med de ansattes legitime behov.

Datatilsynet mener departementet har et viktig ansvar med å påse at forskriften ikke trer i kraft for tidlig. Datatilsynet er derfor bekymret for at departementet mener kravene i forskriftens kapittel 1,2,3 og 5 kan tre i kraft allerede fra 1. juni 2011. Datatilsynet mener riktig rekkefølge må være å konkretisere minstekravene på et nivå under forskrift før forskriften trer i kraft og sikre at kravene kan etterleves i praksis.

Datatilsynet anmoder departementet sterkt om at ikrafttredelse av forskriften skjer etter tett dialog med tilsynsmyndighetene og øvrige aktører.[3] Datatilsynet ønsker å bidra konstruktivt i det videre arbeidet med krav til systemer for tilgang på tvers og kjernejournal, men vil også prioritere tilsyn med tilgang på tvers. Det vil imidlertid være en umulig oppgave for tilsynet å påse at alle virksomheter oppfyller minstekravene til informasjonssikkerhet før det åpnes opp for tilgang på tvers av virksomheter. Det vil ikke være en heldig situasjon for noen parter, dersom Datatilsynet og Helsetilsynet om et år avdekker på tilsyn at en rekke helseforetak ikke overholder forskriftens krav for å gi tilgang på tvers.

2 Enkelte betingelser og rammer for å åpne for tilgang på tvers

2.1 Enkelte av forutsetningene til lovgiver

Lovforarbeidene har lagt klare forutsetninger og rammer for fullmakten regjeringen fikk til å regulere tilgang på tvers i forskrift. Datatilsynet anser det som viktig at disse forutsetningene og rammene gjenspeiles i forskriften, og at det utarbeides systemer som faktisk kan etterleve kravene til lovgiver. Datatilsynet ser ikke bort i fra at tilnærmingen som er lagt i forskriften kan bli utfordret i andre høringsuttalelser. Av den grunn henviser tilsynet her til de sentrale momenter fra forarbeidene.

Det er forutsatt at forskrift om informasjonssikkerhet for behandlingsrettede helseregistre skal bedre og sikre økt informasjonssikkerhet ved behandling av helseopplysninger, og at tilgang på tvers av virksomheter ikke skal svekke informasjonssikkerheten på helseopplysningene.[4]

---

[3] Det fremgår av lovforarbeidene for tilgang på tvers at det er viktig at arbeidet med strukturering av pasientjournal gjøres i tett samarbeid med Legeforeningen og de ulike fagmiljøene, se møte i Odelstinget onsdag den 10. juni 2009 sak nr. 11 hvor blant annet Harald T. Nesvik og Bjarne Håkon Hanssen uttaler dette.

[4] Se Ot.prp.nr.51 (2008-2009) side 39 og Innst. O . nr.110 (2008-2009) side 7

Pasientenes vern mot at uvedkommende får tilgang til taushetsbelagte opplysninger skal være like sterk uavhengig av virksomhetsgrenser.[5]

Det er uttalt som et helt nødvendig premiss at tilgangsstyringen må sikre at det bare er nødvendige, relevante og strukturerte opplysninger det gis tilgang til.[6] Ingen skal ha tilgang til flere opplysninger enn det er behov for.[7]

Viktigheten av at taushetsplikten etterleves er også fremhevet. En pasient skal føle seg trygg på at utveksling av taushetsbelagt informasjon mellom helsepersonell bare skal skje når det er nødvendig for behandling eller oppfølging av pasient.[8]

Utnyttelse av de vedtatte lovendringene krever at det gjøres store tilpasninger i de elektroniske pasientsystemene.[9] En overordnet forutsetning er at virksomhetene har systemer som faktisk er i stand til å gi tilgang til kun journalopplysninger som er relevante og nødvendige for å kunne gi forsvarlig og nødvendig helsehjelp til pasienten, og at det ikke gis tilgang til opplysninger som ikke er nødvendige for helsehjelpen.[10]

En helt sentral forutsetning er at det blir gjort tilpasninger i de elektroniske journalsystemene, slik at de i alle deler av helsevesenet blir strukturert. Dette er helt avgjørende for å kunne skille nødvendig helseopplysninger fra annen sensitiv personinformasjon.[11] Det følger av odelstingsdebatten at det som nærmere ligger i dette er at det skal være en veldig begrenset del av journalen som skal gjøres tilgjengelig på tvers, og at det kun er tale om kjerneopplysninger. [12]

Videre forutsettes det at det i praksis må foreligge en forhåndsvurdering av om opplysninger i journal kan deles med annet helsepersonell. Vurderingen må gjøres ved registrering av opplysningene.[13] Dersom opplysningene ikke blir avgrenset/strukturert ved selve registreringen, må det gjøres senere og senest før det gis elektronisk tilgang.[14]

2.2 Om forholdet til menneskerettighetene

Den europeiske menneskerettskonvensjonen (EMK) er inkorporert i norsk lov i lov om menneskerettigheter av 21. mars 1999 og bestemmelsene er gitt forrang i norsk rett.

Plikten til å sikre den grunnleggende retten til privatliv etter EMK artikkel 8 (1) er særlig viktig ved utarbeidelsen av denne forskriften. Retten til privatliv er utsatt ved uberettiget tilgang på helseopplysninger internt og på tvers av virksomheter, noe som også kommer klart

[5] Se Innst. O . nr.110 (2008-2009) side 7.
[6] Se Innst. O . nr.110 (2008-2009) side 7 og Ot.prp.nr.51 (2008-2009) side 46.
[7] Innst. O . nr.110 (2008-2009) side 7.
[8] Innst. O . nr.110 (2008-2009) side 3.
[9] Innst. O . nr.110 (2008-2009) side 7.
[10] Innst. O . nr.110 (2008-2009) side 5.
[11] Innst. O . nr.110 (2008-2009) side 3.
[12] Odelstinget – Møte onsdag den 10. juni 2009 sak nr. 11 [13:32:34]
[13] Innst. O . nr.110 (2008-2009) side 3.
[14] Ot.prp.nr.51 (2008-2009) side 35.

frem i en dom fra den europeiske menneskerettsdomstolen.[15] Dommen omhandler en HIV-positiv sykepleier som hevdet at sykehusets datasystem ikke beskyttet henne mot uautorisert innsyn i hennes pasientdata fra andre ansatte fra sykehuset. Domstolen fremhever at statens forpliktelse ikke er begrenset til en negativ plikt til selv å avstå fra privatlivskrenkelser, men også en positiv forpliktelse til å iverksette effektive tiltak for å verne om borgernes privatliv. Dette innebærer en plikt for helsetjenesten til å sørge for et effektivt vern om pasienters privatliv i form av et system som gir sikker beskyttelse mot uberettiget innsyn i og flyt av helseopplysninger. Sikringsplikten omfatter også vern mot krenkelser av tredjemenn som ikke handler på vegne av det offentlige, for eksempel privat ansatt helsepersonell.[16]

Det påpekes i dommen at det ikke er tilstrekkelig at lovgivningen garanterer beskyttelse mot uautorisert innsyn i data, så lenge det ikke etableres tilfredstillende systemer og rutiner som i praksis gir et effektivt vern om den enkeltes privatliv. Domtolen trekker frem at det ikke er tilstrekkelig å etablere klageordninger med muligheter for kompensasjon for ulovlig innsyn. Domtolen uttaler blant annet følgende: *"What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here."*

Dommen er omtalt av Personvernkommisjonen.[17] Finland ble dømt for konvensjonskrenkelse, fordi det ikke forelå tilstrekkelig beskyttelse mot uautorisert innsyn internt på et sykehus.

Datatilsynet mener risikoen for uberettiget tilgang i utgangspunktet øker betraktelig når forskriften åpner opp for tilgang på tvers av virksomheter. Med tanke på de svakhetene tilsynsmyndighetene har avdekket når det gjelder tilgangskontroll internt[18], mener Datatilsynet departementet bør forsikre seg om at det er utarbeidet systemer som faktisk kan etterleve regelverket før forskriften trer i kraft også for å ivareta den positive sikringsplikten som følger av EMK artikkel 8 (1). Datatilsynet anbefaler at det oppstilles klare minstekrav til systemer for tilgang på tvers.

3 Særskilte problemstillinger

3.1 Behov for en nærmere klargjøring av regelverkets krav til systemer

Departementet har i høringsnotatet i liten grad tydeliggjort hvordan man skal sikre at systemene faktisk oppfyller regelverkets krav. Dette er uheldig fordi regelverket omkring tilgang på tvers forutsetter betydelige krav til systemer, spesielt med hensyn til strukturering av journalens innhold. Datatilsynet mener først og fremst at forskriften bør slå uttrykkelig fast at systemene må etterleve de krav som følger av regelverket.

---

15 I mot Finland (no.20511/03)

16 Se Jacoks og White 2006 side 243 og NOU 2009 nr 1 side 164.

17 NOU 2009:1 side 164-165. Det vises blant annet til følgende uttalelse: "Dommen er en viktig påminnelse om at retten til privatliv og beskyttelse av private opplysninger i helsevesenet i stor grad handler om praktiske løsninger som gir den nødvendige beskyttelse i praksis. Det er derfor nødvendig å stille to spørsmål i forhold til beskyttelse av personopplysninger på helsevesenets område: Er den eksisterende rettslige regulering tilstrekkelig? Er reguleringen gjennomført på en måte som faktisk sikrer et effektivt vern om privatlivet til den enkelte?"

18 *Datatilsynets rapport april 2009 Sviktende tilgangsstyring i elektroniske pasientjournaler*

Videre mener Datatilsynet at klargjøringen av hva som nærmere ligger i regelverkets krav bør komme på et nivå under forskrift. Departementet kan delegere myndighet til noen for å fastslå nærmere minstekrav til systemer. Datatilsynet minner om at Helsedirektoratet allerede har laget en rapport om forslag til minstekrav for tilgang på tvers. Minstekravene som foreslås i rapporten bygger på høringsnotat av 20. oktober 2008 og Ot.prp. nr. 51. 2008-2009. Minstekravene er forslag til hvilke forutsetninger som må tilfredstilles for at det skal kunne åpnes for tilgang til helseopplysninger på tvers av virksomheter. Minstekravene utdyper krav i regelverket og bygger en bro mellom jus, praksis og system.

Helsedirektoratets forslag til minstekrav kom før Stortinget vedtok lovendringene i juni 2009. Dette innebærer at presiseringer av krav og nye krav som følge av Innst. O. nr.110 (2008-2009) og odelstingsdebatten ikke er tatt inn i direktoratets forslag til minstekrav. En endelig oppstilling av minstekrav til systemer for tilgang på tvers må implementere disse kravene.

Datatilsynet mener direktoratets forslag til minstekrav er et velegnet utgangspunkt, og at departementet bør legge til rette for videreutvikling og formalisering av disse. Datatilsynet kan ikke se at departementet i høringsnotatet har klargjort om man skal bygge videre på direktoratets forslag.

Det pekes spesielt på at det er viktig å få klarlagt nærmere krav til tilgangsstyring og krav til ensartet organisering og strukturering av de elektroniske pasientjournalsystemene. Dette blir omtalt nærmere.

Helsedirektoratet har utarbeidet en sluttrapport om utredning av videre arbeid med en nasjonal kjernejournal. Datatilsynet antar at det i hovedsak er de samme juridiske vurderingene som gjøres både i forhold til nasjonal- og regional kjernejournal. Rapporten vil på denne måten fastlegge de nærmere krav til forskrift om regional kjernejournal.

Det fremgår av lovforarbeidene at det er *"akkurat den samme tekningen"* som ligger til grunn for tilgang på tvers som for kjernejournal, herunder at det skal være en *"veldig begrenset del"* av journalen som skal gjøres tilgjengelig på tvers. [19] Ut fra forarbeidene er det grunn til å tro at arbeidet omkring fastlegging av krav for tilgang på tvers bør ses i sammenheng med kravene til regional og nasjonal kjernejournal. Ut fra høringsnotatet er det imidlertid vanskelig å fastslå om det videre arbeid med tilgang på tvers og kjernejournal skal ses i sammenheng.

Departementet har uttalt at de siste endringer i helseregisterloven medfører at normen må oppdateres slik at det blir bedre samsvar mellom norm og regelverk. Det er imidlertid uklart for Datatilsynet i hvilken grad implementering av nærmere minstekrav for tilgang på tvers blir en del av oppdateringen av normen. Datatilsynet mener uansett kravene for tilgang på tvers bør fremkomme som en fastsettelse med hjemmel i lov og forskrift.

---

[19] Odelstinget – Møte onsdag den 10. juni 2009 sak nr. 11. Det vises for eksempel til følgende uttalelse fra Statsråd Bjarne Håkon Hanssen: *"Jeg har bare lyst til å kommentere ett forhold. Jeg er glad for at representanten Nesvik understreket at den delen av journalen som skal gjøres tilgjengelig på tvers, skal være veldig begrenset del, og det skal nå jobbes med sikte på å lage den forskrift som regulerer det. Det skal lovreguleres, det skal være en begrenset del av journalen. Så er det mange i debatten som har påpekt at dette er teknologisk krevende, at løsninger ikke finnes i dag, men at svaret er kjernejournal. Det er jo akkurat den samme tenkningen som ligger til grunn for en kjernejournal, at det er deler av journalen som skal gjøres tilgjengelig for flere."*

3.1.1 Krav til systemer - forskriftens § 4.

Datatilsynet er positive til at departementet i forskriftens § 4 har utformet en bestemmelse om krav til systemer. Datatilsynet mener det er viktig både for pliktsubjekter og tilsynsmyndigheter at det klargjøres i regelverket at det er en plikt til å sørge for å ha systemer som gjør det mulig å ivareta lovens krav.

Forskriftens § 4 oppstiller kun et generelt krav om at systemene skal gi forsvarlig informasjonssikkerhet. Denne bestemmelsen gir etter tilsynets syn ikke tilstrekkelig nytteverdi. Datatilsynet mener at det først og fremst bør være et minstekrav at bestemmelsen uttrykkelig slår fast at systemene må støtte etterlevelse av de krav som følger av regelverket.

Videre mener Datatilsynet at klargjøringen av hva som nærmere ligger i regelverkets krav til systemer bør komme på et nivå under forskrift. Datatilsynet foreslår at departementet gir direktoratet myndighet til å fastslå nærmere minstekrav til systemer.

Selv om det ikke fremkommer uttrykkelig av høringsnotatet, legger Datatilsynet til grunn at departementet har sett kravene til informasjonssikkerhet i sammenheng med kravene til forsvarlig journalsystem i spesialisthelsetjenesteloven § 3-2 og pasientjournalforskriften § 4.

Datatilsynet er enig med departementet i at disse kravene bør ses i sammenheng.
Krav til systemer i forskriftens § 4 kan utformes etter modell fra kravene i pasientjournalforskriften § 4.[20] Dette vil si at det bør fremgå generelt av bestemmelsen at systemene må støtte etterlevelse av de krav som er fastsatt i lov eller i medhold av lov. Deretter bør bestemmelsen konkretisere de sentrale krav for tilgang på tvers. At systemene på en god måte støtter disse kravene ses av Datatilsynet som avgjørende for at formålet med forskriften skal ivaretas.

På bakgrunn av nærheten mellom denne forskriften og pasientjournalforskriften § 4 antar Datatilsynet at første del av forskriftens § 4 krav til systemer for eksempel vil kunne lyde: "Virksomheter som tar i bruk behandlingsrettede helseregistre, skal sørge for at systemene organiseres slik at der er mulig å etterleve krav fastsatt i eller i medhold av lov, blant annet regler om:" Bestemmelsen bør videre trekke frem de sentrale krav for å åpne opp for tilgang på tvers. Datatilsynet trekker for eksempel frem krav til tilgangsstyring, krav til ensartet organisering og strukturering av de elektroniske pasientjournalsystemene og krav til sperring av pasientjournalen.

Gjennom en felles kontroll gjennomført av Helsetilsynet og Datatilsynet med Akershus universitetssykehus HF ble det konstatert avvik fra de nevnte bestemmelser i

---

[20] Pasientjournalforskriften § 4 om journalsystem lyder:
"Virksomheter hvor det ytes helsehjelp må opprette pasientjournalsystem. Systemet må organiseres slik at det er mulig å etterleve krav fastsatt i eller i medhold av lov, blant annet regler om:
a) innsyn i journal, jf helsepersonelloven § 41 og pasientrettighetsloven § 5-1,
b) tilgang til og utlevering av journal, jf helsepersonelloven § 25 og § 45 samt pasientrettighetsloven § 5-3,
c) meldeplikter og opplysningsplikter, jf helsepersonelloven kapittel 6 og 7,
d) redigering av journal, jf. helsepersonelloven § 39 andre ledd,
e) retting og sletting, jf helsepersonelloven § 42, § 43, og 44 og
f) sikring mot innsyn fra uvedkommende, jf helsepersonelloven kapittel 5, herunder forsvarlig oppbevaring, jf helsepersonelloven § 21."

helselovgivingen. I den konkrete saken fremstod den klare plikten til å ha forsvarlige systemer som en svært hensiktsmessig regulering av kontrollhensyn.

Det bemerkes videre at Datatilsynet finner det noe uklart hvorfor departementet har brukt begrepet forsvarlig når kravet ellers i forskriften er "god" informasjonssikkerhet.

3.2 Krav til ensartet organisering og strukturering av de elektroniske pasientjournalsystemene

Utnyttelse av de vedtatte lovendringene krever som nevnt at det gjøres store tilpasninger i de elektroniske pasientjournalsystemene. Datatilsynet viser til uttalelsen i Innst. O. nr.110 (2008-2009) side 3: *"Flertallet forutsetter at det blir gjort tilpasninger i de elektroniske journalsystemene, slik at de i alle deler av helsevesenet blir strukturert slik at nødvendig helseopplysninger kan skilles fra annen sensitiv personinformasjon."*

Datatilsynet antar at uttalelsen forutsetter et krav om ensartet organisering og strukturering av de elektroniske journalsystemene i helsetjenesten før det åpnes opp for tilgang på tvers.[21]

Det er fastsatt krav om strukturering i forskriftens kapittel V. I merknaden til forskriftens § 24 er det uttalt at det kreves at journalføringen kan struktureres og er strukturert på en slik måte at det er mulig å bare gi tilgang til et avgrenset sett av klinisk informasjon.

På overordnet nivå savner Datatilsynet en tydeliggjøring fra departementet på hvordan en ensartet organisering og strukturering av journalen i helsetjenesten skal sikres. Det anbefales at departementet iverksetter et felles arbeid omkring organisering og strukturering av journal.

3.2.1 Nærmere om krav til strukturering av de elektroniske pasientjournalsystemene

Det følger av odelstingsdebatten hva som nærmere ligger i kravet til strukturering. Det er uttalt at det skal være en veldig begrenset del av journalen som skal gjøres tilgjengelig på tvers, og at det kun er tale om kjerneopplysninger. [22]

Det vises for eksempel til følgende uttalelse fra Statsråd Bjarne Håkon Hanssen: *"Jeg har bare lyst til å kommentere ett forhold. Jeg er glad for at representanten Nesvik understreket at den delen av journalen som skal gjøres tilgjengelig på tvers, skal være veldig begrenset del, og det skal nå jobbes med sikte på å lage den forskrift som regulerer det. Det skal lovreguleres, det skal være en begrenset del av journalen. Så er det mange i debatten som har påpekt at dette er teknologisk krevende, at løsninger ikke finnes i dag, men at svaret er kjernejournal. Det er jo akkurat den samme tenkningen som ligger til grunn for en kjernejournal, at det er deler av journalen som skal gjøres tilgjengelig for flere."*

Departementet har som nevnt fastsatt krav om strukturering i forskriftens kapittel V, og i merknadene til § 24. Datatilsynet savner imidlertid en nærmere klargjøring fra departementet på hvordan man skal sikre at helsetjenesten strukturer journalen i henhold til de krav som er

[21] Uttalelsen ble også fremhevet eksplisitt av Harald T. Nesvik i Odelstinget – Møte onsdag den 10. juni 2009 sak nr. 11.
[22] Odelstinget – Møte onsdag den 10. juni 2009 sak nr. 11.

oppstilt i lovforarbeidene. I lovforarbeidene er det som tidligere nevnt også forutsatt at strukturering av journalene skal skje i tett samarbeid med de ulike fagmiljøene.[23]

Siden strukturering av journalene er et sentralt krav for å åpne opp for tilgang på tvers mener Datatilsynet departementet bør definere begrepet strukturering i forskriftens § 3.

Helsedirektoratet har i sin rapport om forslag til minstekrav for tilgang på tvers definert begrepet struktur på følgende måte:
"Med struktur menes i denne rapporten en inndeling av journalens innhold som muliggjør en ensartet organisering av journalinformasjon i de ulike EPJ-system, slik at brukere kan navigere forsvarlig og gjenkjenne journalens struktur og oppbygning i ekstern virksomhets EPJ." Datatilsynet antar dette kan være et naturlig utgangspunkt for utforming av definisjon til begrepet strukturering.

Nærmere fastlegging av krav til strukturering bør imidlertid etter Datatilsynets vurdering fremkomme på et nivå under forskrift.[24]

Datatilsynet antar at journalene internt i en virksomhet også må struktureres for å imøtekomme kravet om at det kun skal gis tilgang til relevante og nødvendig helseopplysninger. Det anbefales at departementet sikrer at det bekjentgjøres hvorledes journalene skal struktureres, for eksempel gjennom rundskriv.

3.3 Forholdet til personopplysningsforskriften

Datatilsynet ser det som grunnleggende at forskriften er harmonisert med personopplysningsforskriftens regulering av informasjonssikkerhet og internkontroll i henholdsvis kapittel 2 og 3. Datatilsynet er ikke av den oppfatning at dette er et vesentlig problem i det forelagte forslaget til forskrift. Imidlertid ser tilsynet behov enkelte tiltak for å sikre en god harmonisering. Datatilsynet har i den sammenheng generelle kommentarer til §§ 5 til 8 i forslaget til forskrift.

Datatilsynet ser det som naturlig at den generelle reguleringen av internkontroll og informasjonssikkerhet finner sted i personopplysningsforskriften, mens øvrige forskrifter gir utfyllende bestemmelser innen sitt virksområde. I praksis må også helsetjenesten og helseforvaltningen forholde seg til personopplysningslovens og personopplysningsforskriftens generelle regler, både for behandlinger som faller utenfor helseregisterlovens virkeområde og i de tilfeller personopplysningsloven gjelder utfyllede for helseregisterloven. Dersom reguleringen i denne forskriften ikke er harmonisert med personopplysningsforskriftens 2. og 3. kapittel, vil det samlede regelverket fremstå som upedagogisk og lite egent for etterlevelse.

At de generelle reglene oppstilles i personopplysningsforskriften er også sentralt for revisjon av bestemmelsen og harmonisering mot annet regelverk som regulerer informasjonssikkerhet.

---

[23] Se punkt om forutsetning om tett samarbeid om strukturering av journal på side 2.

[24] Det vises også til KITH's EPJ standard når det gjelder hvordan EPJ kan bygges opp med en felles struktur.

3.3.1 Henvisning til personopplysningsforskriften - § 8

Henvisningen i forskriften § 8 er begrenset til å gjelde sikkerhetsbestemmelsene i personopplysningsforskriftens kapittel 2. Datatilsynet legger til grunn at tilsvarende henvisning til kapittel 3 om internkontroll er utelatt ved en inkurie.

Videre ser Datatilsynet at begrepet "utfyllende" kan fremstå som uklart for brukerne av forskriften, selv om bruken av begrepet er en alminnelig lovteknikk. Grunnen til dette er at forskriften her gjentar enkelte av personopplysningsforskriftens sentrale elementer i en komprimert form. Dette gjelder for systemkomponentene for informasjonssikkerhet (gjengitt i forskriftens §§ 5 og 7) og for internkontroll (gjengitt i forskriftens § 6). Brukeren kan her forstå at systematikkravene etter personopplysningsforskriftens ikke kommer til anvendelse. Tilsvarende for de generelle internkontrollkravene i kapittel 3.

Datatilsynet ser det som klart at personopplysningsforskriftens kapitler 2 og 3 kommer til anvendelse, og anbefaler at departementet klargjør dette for brukeren av forskriften. Dette kan trolig løses på merknadsnivå. Videre anbefaler Datatilsynet at en henvising til personopplysningsforskriftens kapittel 3 tas inn i forskriftens § 8.

3.3.2 Regulering av internkontroll – forskriftens § 6

Forskriftens § 6 omtaler først internkontrollplikten generelt, deretter presiseres konkrete krav til internkontroll for ivaretakelse av krav etter denne forskriften.

Datatilsynet stiller spørsmål ved om den generelle omtalen av internkontroll er hensiktsmessig, da den etter tilsynets syn bør føres i personopplysningsforskriften av hensyn til et harmonisert regelverk. For øvrig bemerkes det at personopplysningsforskriftens kapittel 3 har et forbedringspotensial hva gjelder systematikk. Dette håpes imidlertid utbedret.

Datatilsynet anbefaler departementet å vurdere en regulering av internkontroll på linje med de ulike registerforskriftene etter helseregisterloven, som for eksempel Norsk pasientregisterforskriften.

3.3.3 Systemkomponenter for informasjonssikkerhet - forskriftens §§ 5 og 7

Bestemmelsene utgjør systemkomponenter fra en tradisjonell tilnærming til informasjonssikkerhet i samsvar med personopplysningsforskriftens kapittel 2, og tilnærmingen gjennom anerkjente standarder for informasjonssikkerhet, som ISO27000-serien[25]. Bestemmelsene begrenser seg imidlertid til ledelsesforankring av ansvar (forskriftens § 7) og krav om rutiner (forskriftens § 5), og vil gi begrenset verdi uten at en foreholder seg til de øvrige kravene i personopplysningsforskriftens kapittel 2.

Datatilsynet ser at forskriftens § 5 innebærer en skjerping og konkretisering av dokumentasjonskravet. Datatilsynet er ikke negativ til dette, men ser det som nødvendig at det går tydeligere frem at reguleringen ikke er komplett, og at brukeren av regelverket aktivt må forholde seg til personopplysningsforskriftens kapittel 2.

[25]Med begrepet ISMS menes Information Security Management System

3.3.4 Andre forhold

Datatilsynet ser det som hensiktsmessig at bestemmelsenes rekkefølge endres slik at forskriftens § 7 om sikkerhetsledelse kommer før forskriftens §§ 5 og 6.

Til slutt henviser Datatilsynet til arbeidet i regi av Koordineringsorgan for informasjonssikkerhet (KIS). KIS arbeider blant annet for en hensiktsmessig samordning og videreutvikling av regelverk som er relevant for informasjonssikkerhet. Spesielt vises det til arbeidet i Samarbeidsgruppe for regelverk for informasjonssikkerhet (SARI).

3.4 Krav til tilgangsstyring

3.4.1 Tilgang må knyttes til pasientens behandlingsforløp

Datatilsynet har de siste årene gjennomført kontroller med fokus på tilgangsstyring, både innen kommunesektoren og spesialisthelsetjenesten[26]. En sentral problemstilling som tilsynet har identifisert er at tilgangen som gis helsepersonell i for liten grad er knyttet til behandlingsforløpet til pasienten. Dette medfører at langt flere enn de som er involvert i helsehjelpen til pasienten gis elektronisk tilgang til pasientens journal. Dette medfører at det enkelte helsepersonells taushetsplikt undergraves ved at opplysningene gjøres tilgjengelige for en langt videre krets enn rammen for samarbeidende helsepersonell tilsier.

Tilsynet har dokumenterte eksempler på at vid tilgang også har medført at helsepersonell ikke har dokumentert ytt helsehjelp, og at ansatte ved virksomhetene har valgt seg bort fra institusjonen når de selv har behov for helsehjelp. I tillegg melder fagmiljøene i fra om at pasienter i økende grad ber om at det de forteller legen ikke blir journalført.

Etter Datatilsynets syn grunner denne tilstanden i at journalsystemene i vesentlig grad baseres på en statisk tilnærming til tildeling av tilgang i forhold til hvor i virksomheten pasienten ytes helsehjelp, i kombinasjon med en dynamisk virkelighet hvor pasienten ytes helsehjelp ved en rekke avdelinger (og andre organisatoriske nivåer) og hvor helsepersonell arbeider på tvers av avdelinger. Dette resulterer i at langt flere enn de som deltar i helsehjelpen gis tilgang til journalen.

For å korrigere dette ser tilsynet det som nødvendig at tilgangsstyringen knyttes nærmere behandlingsforløpet til pasienten (beslutningsstyrt tilgangsstyring eller forløpsorientert tilgangsstyring). Et konkret eksempel på at vide tilganger systematisk blir gitt er legers tilsynsfunksjoner på tvers av avdelinger. Det gis her ofte statiske tilganger til pasienter ved andre avdelinger i tilfelle legen skal ha tilsyn med pasienten, samtidig som tilsynsfunksjonen normalt følger av at legen blir anmodet om å bistå. Manglende funksjonalitet i journalsystemene for å involvere annet helsepersonell, og følgelig gi de tilgang, medfører unødvendig vide tilganger.

Datatilsynet er kjent med at journalleverandørene gradvis gjør fremskritt på dette området, selv om implementeringen per i dag må sies å ha kommet kort. Etter tilsynets syn avhenger en

[26] Datatilsynets rapport april 2009 Sviktende tilgangsstyring i elektroniske pasientjournaler

god informasjonssikkerhet i sektoren av interne forhold, ved at virksomheten implementerer en tilgangsstyring som faktisk støtter opp under taushetsplikten.

Dette berøres overflatisk i forslagets § 19, og noe mer utfyllende i kommentarene til bestemmelsen. Datatilsynet ser dette som en så vesentlig faktor at omtalen bør klargjøres i forskriftens bestemmelse.

Datatilsynet foreslår at forløpsorientering konkretiseres i forskriften for eksempel ved at følgende tas inn i forskriftens § 10 og/eller forskriftens § 19 "Tilgangen skal tilpasses behandlingsforløpet til pasienten slik at tilgang begrenses til helsepersonell som yter helsehjelp til pasienten".

Det bør videre knyttes et systemkrav til forløpsorienteringen.

3.4.2 Plikt til å vurdere den faktiske tilgangen

Departementet har i forslagets § 10 1.ledd, 2. setning foreslått et krav om at den databehandlingsansvarlige skal vurdere gitte tilganger med hensyn til a) antall, b) mengde og c) varighet. Datatilsynet støtter tilnærmingen, og ønsker å begrunne dette ytterligere.

Datatilsynet har benyttet tilsvarende tilnærming for å illustrere mangler ved tilgangsstyring observert under kontroller. Tilnærmingen er etter tilsynets syn nødvendig for at den behandlingsansvarlige kan ivareta sin plikt til å gjennomføre risikovurderinger etter personopplysningsforskriftens § 2-4 og forslagets § 9.

Parametrene antall, mengde og varighet gir et uttrykk for "volumet" av tilgangen. En slik tilnærming vil være nødvendig både for å vurdere konsekvenser av sikkerhetsbrudd, samt sannsynligheten i form av å ha tilgang til interessant informasjon. Hensikten er ikke å sette øvre grenser, blant annet for antallet journaler det gis tilgang til, men å sørge for at den databehandlingsansvarlige ser det reelle omfanget av tilgangene som gis. Den databehandlingsansvarlige kan da avdekke tildelinger av tilganger som representerer en uakseptabel risiko, slik at det kan innføres tiltak på system- eller administrativt nivå.

Selv om plikten, etter Datatilsynets syn, kan utledes av gjeldende rett, vil en konkretisering bidra til bedre etterlevelse.

3.5 Autentisering

Reguleringen av autentisering i forslaget til forskriften kan etter Datatilsynets syn bedres, og tilsynet foreslår å samle og systematisere forskriftens omtale av autentisering. Forskriftens kapittel 3 har etter tittelen som utgangspunkt å regulere blant annet autentisering, og forskriftens § 13 omhandler krav til autentisering. Samtidig omhandles autentisering spredt i de øvrige deler av forskriften.

3.5.1 Spesielt om forskriftens § 13

Forskriftens § 13 har tittelen autentisering. Dette samsvarer imidlertid dårlig med det materielle innholdet i bestemmelsen, jf. definisjonen av autentisering i forskriftens § 3 nr 1[27]. Det bemerkes at kommentarene til bestemmelsen synes å gå lengre mot autentisering. Det er bruken av begrepet *identifiseres* som fremstår som uklar i bestemmelsen. I en systemteknisk sammenheng benyttes identifisering om å gjenkjenne en entydig bruker – som gjøres før brukeren autentiseres – identiteten bekreftes. I daglig anvendelse gis imidlertid *identifisering* en videre betydning. Bestemmelsen sett sammen med kommentaren skaper ikke klarhet i hva som menes her.

Datatilsynet foreslår følgende endring:
Endret § 13 Tittel: Knytning av autorisasjoner til identitet og rolle
Autorisasjoner skal kun knyttes til entydig identifiserte brukere i bestemte roller.

Bestemmelsen foreslås beholdt under kapittelet om autorisering.

Datatilsynet har her ikke tatt hensyn til at det av kommentarene kan virke som om ulike autentiseringsfaktorer skal benyttes for de ulike rollene brukerne kan ha. Departementet anbefales å vurdere dette nærmere, og eventuelt ta det inn i en egen bestemmelse slik at det fremstår som klart.

3.5.2 Nivå på autentisering – fullmakt til å fastsette nivå

Datatilsynet ser det som naturlig at sektoren beveger seg i en retning mot bruk av sterkere former for autentisering, også internt i virksomhetene.

Datatilsynet støtter derfor departementets i forslaget til forskriftens § 25 om krav om sterk autentisering i form av bruk av kvalifiserte sertifikater når det gjøres tilgang mellom virksomheter. Den rettslige reguleringen rundt kvalifiserte sertifikater er etter tilsynets syn nødvendig for ulike juridiske enheter skal ha tilstrekkelig tillit til at autentiseringen er korrekt.

Generelt ser Datatilsynet at det er behov for å styrke autentiseringen også for intern tilgang i virksomhetene. Helseforetakenes størrelse kan blant annet tilsi at lignende vurderinger som legges til grunn ved tilgang utenfra eget kontrollert område, også bør legges til grunn internt i virksomhetene. Mistanker om helsepersonells misbruk av journalsystemet har ved minst ett tilfelle blitt frafalt, da det har blitt reist tvil om det var helsepersonellet selv som gjennomførte misbruket, eller om en annen person som hadde tilegnet seg brukernavn og passord. Tilsvarende er aktualisert i en pågående sak, hvor den som mistenkes for uautorisert bruk, hevder at andre har disponert helsepersonellets brukernavn og passord.

Datatilsynet ser det som nødvendig, både for helsepersonellets rettssikkerhet og pasientenes integritetsvern, at det innføres krav om sterk autentisering også internt i virksomhetene. Datatilsynet ser at en slik innføring bør komme gradvis, og foreslår at Helsedirektoratet gis fullmakt til å fastsette nærmere krav om autentisering. En slik tilnærming vil etter tilsynets

[27] Som samsvarer ryddig med definisjonen i ISO 27001pkt 2.5

syn bidra til en reell heving av informasjonssikkerheten i sektoren samtidig som implementering kan gjennomføres gradvis.

3.5.3 Bedre strukturering av autentisering i forskriften

For å samle og systematisere reguleringen av autentisering foreslår Datatilsynet at det lages et nytt kapittel i forskriften om autentisering. Tilsynet ser også behov for å styrke reguleringen rundt autentisering, spesielt med tanke på tildeling og tilbakekalling av autentiseringsfaktorer, og gi Helsedirektoratet fullmakt til å fastsette nivå på autentisering.

Datatilsynet anbefaler at departementet ser hen til omtale av autentisering i Fornyings, administrasjons- og kirkedepartementets retningslinje 03.04.2008 Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.

3.6 Autorisering for å treffe beslutning om helsehjelp

I forslagets § 19, 2. ledd omtales tilgang for personell som på selvstendig grunnlag kan fatte beslutning om å yte helsehjelp. Etter Datatilsynets syn mangler det en omtale av autorisasjon for slik tilgang i kapittel III.

Personell som har anledning til å treffe beslutningen har i praksis tilgang til enhver journal ved virksomheten. Anledningen til å på selvstendig grunnlag beslutte ytelse av helsehjelp bør derfor klart begrenses til den kretsen av personell som har en slik funksjon. Datatilsynet ser at tilsvarende tillatelser benyttes i dag som en erstatning for manglende styring av tilgangen i journalsystemene.

Datatilsynet foreslår forskriftens § 15 utvides med ett annet ledd som regulerer autorisasjon til å treffe beslutning om å yte helsehjelp, alternativt til § 11, eller at det tas inn en ny bestemmelse ei kapittel III. Forslag til § 15, nytt 2. ledd:
"Autorisasjon til å fatte beslutning om helsehjelp skal kun gis personell som i kraft av sin stilling kan ta en slik beslutning."

3.7 Håndtering av forespørsler mellom virksomheter

Datatilsynet ser et generelt forbedringspotensial med hensyn til hvordan det faktisk skal gis tilgang til journal mellom virksomheter i forskriften .

Det fremstår ikke som klart, om eller når, det bør gjøres en konkret vurdering ved virksomheten i forbindelse med forespørselen.

Begrensingen i forskriftens § 22 1. ledd "Det kan bare gis tilgang til opplysninger som det på forhånd er vurdert kan deles med annet helsepersonell..." fremstår for tilsynet som for uklar. Etter tilsynets forståelse vil det meste av journalens innhold kunne være gjenstand for deling under de rette forutsetningene, og etter en konkret vurdering. Datatilsynet viser til tidligere merknader om behov for nærmere krav med hensyn til strukturering og forutsetninger for tilgang på tvers.

På forskriftsnivå ser tilsynets det som hensiktsmessig at enkelte konkretiseringer gjøres, slik at det innføres en plikt til å vurdere hos virksomheten som forespørres.

Datatilsynet ser det som et minimumskrav at det innføres en konkret vurdering hos utleverende virksomhet på tidspunktet for forespørselen, for annen informasjon enn kjerneinformasjon eller opplysninger hvor det foreligger et konket samtykke hos den utleverende virksomheten.

3.8 Logg

Datatilsynet er generelt positiv til forskriftens regulering av logging og bruk av loggene. Datatilsynet ser imidlertid behov for å forbedre forkriftsens regulering av logging på tre områder.

3.8.1 Krav om å kunne sikre logg

Datatilsynet ser at kravet til lagring av loggen i to år kan være hensiktsmessig. Lagring må også begrenses av hensyn til de ansatte. Det er imidlertid kjent at det kan ta lang tid fra en sak starter til loggen utleveres. Datatilsynet har for eksempel hatt en sak hvor det har tatt pasienten et par år å få tilbakemelding på krav om utlevering av logg. Datatilsynet mener derfor at regelverket og journalsystemene må utformes slik at logg kan tas ut eller sikres slik at loggen ikke går tapt gjennom automatisk sletting av logg.

3.8.2 Behov for konkretisering av gjennomgang av logg

Datatilsynet ser det som nødvendig at merknadene til forskriften i større grad klargjør hvordan gjennomgang av logg skal gjennomføres, herunder gjennom stikkprøver, analyser av logg, og undersøkelser basert på risiko/mistanke.

Et klart eksempel på et område som bør undersøkes for mulige uautoriserte oppslag, er tilfeller hvor det kan stilles spørsmål ved om helsepersonellet har vært involvert i helsehjelpen eller ikke. Dersom det er gitt helsehjelp vil det normalt være ført journal, enten av helsepersonellet eller noen i teamet til helsepersonellet.

Tilsvarende kan rene frekvensbaserte undersøkelser eller undersøkelser av oppslag utenfor eget normalt arbeidsfelt, være et naturlig utgangspunkt for loggundersøkelser.

Etter Datatilsynets erfaring bør gjennomgang av logg bestå av en kombinasjon av undersøkelser. Denne bør foretas av sentral administrasjon ved virksomhetene og av personell som er nærmere pasienten i behandlingskjeden for eksempel på avdelingsnivå eller journalansvarlig lege.

3.8.3 Tiltak for å sikre personvernet til den ansatte

Loggføring griper inne i arbeidstakernes personvern. Datatilsynet ber departementet foreta en nærmere vurdering av tiltak som også kan ivareta personvernet til arbeidstaker. Det bemerkes at loggføring av ansatte er et kontrolltiltak etter arbeidsmiljøloven kapittel 9.

3.8.4 Logg er kun et supplement til god tilgangsstyring

Tilsynet presiserer til slutt at problemet med manglende tilgangsstyring ikke kan løses gjennom gode rutiner for etterkontroll. Logging kan ikke hindre urettmessig tilegnelse av helseopplysninger, men er et verktøy for å avdekke brudd på taushetsplikten eller andre ulovlige handlinger som allerede er begått. Loggføring må derfor kun være et supplement til god tilgangsstyring. Det vises i denne forbindelse til avgjørelsen i saken EMD I mot Finland. Der ble det slått fast at det sentrale er å hindre urettmessig tilegnelse av helseopplysninger.

3.9 Krav til opplæring

Datatilsynet er positive til at departementet har fastsatt krav til opplæring i forskriften for å styrke ivaretakelsen av taushetsplikten til helsepersonell. Tilsynet er imidlertid av den oppfatning at det ikke er helsepersonellet som utgjør den største trusselen mot personvernet i helsesektoren.

Trusselen skyldes først og fremst systematiske svakheter ved at journalsystemene ikke tilpasses tilgangsstyringen til den enkelte ansattes legitime behov.

Helseopplysninger er av en slik art at sikkerheten rundt dem ikke kan bero på det enkelte menneskets moral og ryggmargsrefleks alene. Det er derfor viktig både med gode systemer, som i størst mulig grad hindrer urettmessig tilegnelse av opplysninger, og i tillegg krav til opplæring og holdningsskapende arbeid som et viktig supplement.

3.10 Pasientens rett til å rå over egne opplysninger

Med utgangspunkt i pasientens rett til å råde over egne opplysninger, bør pasienten også i størst mulig utstrekning gis anledning til å bestemme i hvilken grad man vil at ens opplysninger skal tilflyte andre enn dem man har avgitt opplysningene til.

Datatilsynet er fornøyde med at forskriften ivaretar retten til å råde over egne opplysninger med hovedregelen om uttrykkelig samtykke fra pasienten før det gis tilgang på tvers. Det bemerkes at journalen må være strukturert slik at pasient kan samtykke til innsyn i deler av den. Samtykke vil i denne sammenheng oppheve taushetsplikten, og må derfor være i samsvar med kravene til samtykke etter helsepersonelloven § 22. For at samtykke skal være gyldig forutsettes det blant annet at vedkommende har fått informasjon om hvilke opplysninger det gjelder, jf. Ot.prp.nr13 (1998-1999) side 227-228. Det er noe uklart for Datatilsynet hvordan man skal sikre at tilgangen til journalopplysninger avgrenses til det man har fått samtykke til å gå tilgang til.

Datatilsynet har ingen innvendinger til departementets utforming av unntaket fra kravet om samtykke i forskriftens § 28.

Datatilsynet er også fornøyde med at departementet i forskriftens § 29 har gitt den registrerte en uttrykkelig rett til å sperre journalopplysninger. Datatilsynet bemerker at journalene må være strukturerte slik at pasienten kan sperre deler av journalen. Datatilsynet mener det bør klargjøres nærmere hvordan man skal ivareta retten til å sperre deler av journalen.

Datatilsynet har ingen innvendinger mot at det gis tilgang til sperrede opplysninger når tungtveiende grunner taler for det i henhold til forskriftens § 30. "Tungtveiende grunner" vil i praksis være situasjoner hvor tilgang til opplysninger anses nødvendig for å hindre fare for liv eller alvorlig helseskade.[28] Datatilsynet bemerker at rene personvernhensyn må normalt vike dersom en pasients liv og helse er truet, og vedkommende kan reddes, dersom det gis tilgang til vedkommendes journal.

3.11 Tilgang direkte i annen virksomhets journalsystem

Det fremstår som uklart for Datatilsynet om forskriften ivaretar en praksis hvor helsepersonell søker tilgang til en annen virksomhets journalsystem, uten først å gå gjennom sin egen virksomhets journalsystem.

En konkret problemstilling innen helseregion Nord har tidligere blitt diskutert med Datatilsynet. Etter tilsynets forståelse er problemstillingen slik: Universitetssykehuset i Nord-Norge HF (UNN) er tildelt regionale funksjoner. For å redusere mengden pasientreiser har UNN hatt ambulerende helsepersonell, som reiser rundt på de øvrige sykehusene (helseforetakene) i regionen. Disse har etter tilsynets forståelse utøvd helsehjelp i regi av UNN, og ikke i regi av sykehuset de besøker. I denne situasjonen vil det være naturlig å anse UNN som databehandlingsansvarlige for den dokumentasjon som blir gjort av det ambulerende helsepersonell. I denne situasjonen er det reist spørsmål om helsepersonellet lovlig kan benytte journalsystemet til virksomheten som besøkes. Videre hvor helsehjelp, som UNN er den ansvarlige utøver for, skal dokumenteres den tid helsehjelpen utøves ved en annen virksomhet.

En tilsvarende problemstilling er diskutert i kontrollsak med Helse Finnmark[29] i tilknytning til dialysetjenester som ble gjennomført ved foretaket, men hvor UNN var ansett som faglig ansvarlig og databehandlingsansvarlig.

Datatilsynet har ikke konkludert med at løsningene er i konflikt med eksisterende regelverk. Det har vært gjort tiltak for å sikre at journaler ble ført i UNNs journalsystem, og deretter kommunisert til det andre foretaket. Datatilsynet ser imidlertid at det bør avklares hvorledes slikt samarbeid skal, og kan, foregå etter ikrafttredelsen av denne forskriften. Datatilsynet ser følgende to problemstillinger som sentrale:

Forskriftens § 26, 1. ledd stiller krav om helsepersonell må gå via autorisasjons- og autentiseringsmekanismene i egen virksomhet, og ikke direkte hos den andre virksomheten. Dette kan fremstå som et hinder mot at ambulerende personell gjør direkte oppslag ved besøk hos andre sykehus, uavhengig av om virksomheten de tilhører anses for å være databehandlingsansvarlig eller ikke, jf. merknader til forskriftens § 22.[30]

---

[28] Ot.prp. nr 12 (1998-1999) side 137.

[29] Datatilsynets 05/01251-9, Endelig kontrollrapport, kapittel 7

[30] Det bemerkes at Datatilsynet anser begrensingen i § 26 som viktig for annen (normal) tilgang mellom virksomheter.

Skriveadgangen etter forskriftens § 23 fremstår ikke som dekkende for ambulerende personell som utøver helsehjelp i regi av egen virksomhet. Etter Datatilsynet vil det her fremdeles være behov for en journalføring i egen (sentral) virksomhet, med utlevering til annen (lokal) virksomhet, jf. merknadene til forskriftens § 22 om databehandlingsansvar.

Datatilsynet anbefaler at departementet vurderer hvorledes disse problemstillingen stiller seg i forhold til forskriften, og klargjør dette på egnet vis.

3.12 Tilgang for andre formål

I tidligere forslag til forskrift har det vært åpnet for tilgang for andre formål enn pasientbehandling. Datatilsynet har vært svært kritisk til disse forslagene. Bestemmelsene om tilgang for andre formål enn helsehjelp var knapt berørt i departementets høringsuttalelse. Datatilsynet kan heller ikke se at tilgang for andre formål i nevneverdig grad har vært omtalt i lovforarbeidene til lovendringene om tilgang på tvers.

Tilsynet bemerket i sin høringsuttalelse av 12. januar 2009 at bestemmelsene om tilgang for andre formål enn helsehjelp var oppsiktsvekkende vide, og særlig tidligere foreslåtte § 15. Det var i denne bestemmelsen ikke angitt hvem som skulle få tilgang, og hvilket formål tilgangen skulle benyttes (bare formålet var "forhåndsbestemt"). For Datatilsynet var det et paradoks at man i regelverket før øvrig gjennomgående begrenser tilgangen til å gjelde formålet medisinsk behandling, for deretter å gi en generell åpning for tilgang til alle andre formål. Utkastet til forskrift kunne forstås slik at det var mindre problematisk å gi tilgang pasientjournaler for andre formål enn pasientbehandling.

Den eneste skranken som var satt for tilgang til pasientjournalen for andre formål var taushetsplikten. Etter sin ordlyd ville bestemmelsen derfor gitt tilgang for en stor personkrets, herunder, NAV, politi, forsikringsselskaper, forskere og administrativt personell fordi taushetsplikten ikke lenger er like absolutt som den var før. En rekke unntak følger av lovgivningen.[31]

Datatilsynet ville vært svært kritisk til å gi en slik tilgang for andre formål enn helsehjelp. En slik tilgang ville også stilt krav til strukturering av journalen for andre formål enn helsehjelp.

Datatilsynet er fornøyde med at departementet i dette forslaget til forskrift ikke har åpnet opp for tilgang for slike andre formål. Tilsynet understreker viktigheten av at denne begrensingen ikke fravikes når forskriften gjøres endelig.

[31] Se Asbjørn Kjønstad 2007 Helserett: Gyldendal Akademisk side 311- 312. Kjønstad viser der til ca 50 bestemmelser som pålegger helsepersonell plikt til å gi meldinger av ulike slag eller som gir adgang til å meddele ellers taushetsbelagte opplysninger. Det vises også til den nylig vedtatte bestemmelsen i helsepersonelloven § 29b som gir departementet fullmakt til å bestemme at helseopplysninger kan eller skal brukes til kvalitetssikring, administrasjon, planlegging eller styring av helsetjenesten, og at dette skal skje uten hinder av taushetsplikt.

4. Oppsummering

Datatilsynet vil påpeke at dette forslaget til forskrift fremstår som vesentlig bedre enn det som tidligere har vært fremlagt. Datatilsynet er positive til at forskriften nå har implementert en rekke av lovgivers forutsetninger for tilgang på tvers. Det er imidlertid en svakhet at høringsnotatet i liten grad redegjør for hvordan man skal sikre at systemene faktisk oppfyller regelverkets krav. Datatilsynet mener derfor det er behov for en nærmere klargjøring.

Det pekes spesielt på at lovforarbeidenes har fastsatt en rekke forutsetninger for å åpne opp for tilgang på tvers. For eksempel at tilgangsstyringen må sikre at det bare er nødvendige, relevante og strukturerte opplysninger det gis tilgang til. Lovforarbeidene har også oppstilt klare krav til strukturering av pasientjournaler.

Datatilsynet mener direktoratets forslag til minstekrav for tilgang på tvers er et velegnet utgangspunkt for et videre arbeid omkring klargjøring av regelverkets krav til systemer.

En nærmere klargjøring også bør ses i sammenheng med arbeidet omkring nasjonal- og regional kjernejournal. Forarbeidene fremhever at det er akkurat den samme tenkingen som ligger til grunn for tilgang på tvers og kjernejournal, og at det er en veldig begrenset del av journalen som skal gjøres tilgjengelig på tvers. Datatilsynet ser behovet for bedre samhandlingsløsninger og er positive til en samtykkebasert kjernejournal. Kjernejournal er en samhandlingsform som godt ivaretar behovet for tilfredsstillende informasjonsdeling og samtidig sikrer pasientens autonomi.

Plikten til å sikre den grunnleggende retten til privatliv etter EMK artikkel 8 (1) er særlig aktuell når det kommer til forskriften som nå er på høring. Retten til privatliv er utsatt ved uberettiget tilgang til helseopplysninger internt og på tvers av virksomheter. Det er viktig at departementet i det videre arbeid har fokus på hvordan man skal sikre at gjennomføringen av lovreguleringen faktisk gir et effektivt vern om privatlivet til den enkelte. Det er viktig at det etableres systemer som etterlever regelverkets krav for å sikre et slikt effektivt vern.

Datatilsynet ser på det som viktig og ønskelig å få bistå i det videre arbeidet både med kravene til systemer for tilgang på tvers og kjernejournal.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Monica Fornes
Seniorrådgiver

Saksbehandlere: Helge Veum og Bård Soløy Ødegaard