

Helse- og omsorgsdepartementet
Postboks 8011 Dep

0030 OSLO

Deres referanse
200804460-/BA

Vår referanse (bes oppgitt ved svar)
08/01708-2 /CBR

Dato
12. januar 2009

Høringsuttalelse - Tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av virksomhetsovergrepene behandlingsrettede helseregistre mm

1 Innledende merknader

Det vises til departementets høringsbrev av 20. oktober 2008.

Etter tilsynets vurdering åpner departementets forslag for en langt mer omfattende informasjonsdeling innen helsesektoren enn det departementet dokumenterer er nødvendig av hensyn til forsvarlig pasientbehandling. Tilsynet stiller endog spørsmål ved om den praksis man ønsker å etablere lar seg gjennomføre i tråd med gjeldende bestemmelser om helsepersonellens taushetsplikt.

Departementet skisserer ulike behov for informasjonsdeling, avhengig av behandlingssituasjon. Tilsynet savner imidlertid at departementet vurderer konkret hvilke samhandlingsløsninger som best ivaretar de ulike hensyn i den enkelte behandlingssituasjon. Etter tilsynets vurdering er det konkrete forslaget til løsning, i flere sammenhenger, alt for vidtgående.

2 Nærmere om helsepersonellens taushetsplikt og informasjonsdeling

Spørsmålet om hvem som skal få kunnskap om innholdet i en pasientjournal er et prinsipielt og vanskelig spørsmål. Det soleklare utgangspunktet er at helsepersonellet har en aktiv og *personlig* plikt til å bevare *taushet* om de opplysninger han besitter som følge av sin stilling, om pasienten, dennes pårørende osv. Prinsippet følger av den hippokratiske ed, og har således

vært et grunnleggende legeetisk prinsipp i nærmere 2500 år. I dag er taushetsplikten lovbestemt, jf helsepersonellovens kapittel 5 og 8.

Helsepersonellets taushetsplikt er begrunnet i personvern hensyn; pasienten skal sikres mot at opplysninger om ham blir spredt uten hans viten og vilje. Pasienter vil i varierende grad ha motforestillinger mot at deres helseopplysninger blir spredt. Her vil konkrete forhold som opplysningenes art og omfang, formålet med spredningen og mottaker av opplysningene være av avgjørende betydning. Utgangspunktet er derfor at pasienten i størst mulig grad skal sikres kontroll med egne helseopplysninger, blant annet med tanke på hvem som besitter eller har kunnskap om opplysningene. I de tilfeller hvor pasienten ikke selv kan *bestemme* hvem som får ta del i hans opplysninger, skal pasientene i det minste innrømmes *kunnskap og forutberegnlighet* i forhold til hvor opplysningene videreformidles og til hvilket formål.

Taushetsplikten er ikke absolutt. For det første kan pasienten selv frita helsepersonellet fra deres taushetsplikt. Videre kan lovgiver pålegge helsepersonellet å videreformidle pasientopplysninger til samfunnsnyttige formål som for eksempel forskning, samfunnsplanlegging, kvalitetssikring, bekjempelse av trygdemisbruk, forsikringssvindel, etterforskning av straffbare forhold med mer. Stadig vedtas det nye bestemmelser som gjør innhugg i taushetsplikten. Dette er en utvikling som Datatilsynet uttrykker bekymring for. Slik tilsynet ser det er taushetsplikten under sterkt press.

Endelig gjøres det lovbestemte unntak, når hensynet til pasienten selv tilsier det. Dette gjelder blant annet etter helsepersonellovens §§ 25 og 45.

I enhver sammenheng hvor det gjøres lovbestemte unntak fra taushetsplikten skal helsepersonellet begrense informasjonsdelingen til kun å omfatte opplysninger som er *nødvendige og relevante* for mottakers formål. De opplysninger som ikke er nødvendige og relevante skal helsepersonellet bevare taushet om.

Dersom *mottaker* skal vurdere hvilke konkrete opplysninger som er nødvendige og relevante i den enkelte journal, må han nødvendigvis gis tilgang til hele journalen. Faren er stor for at han derved får tilgang til opplysninger som ikke er nødvendige og relevante. For at helsepersonellet i realiteten skal bevare taushet om forhold som ikke er nødvendige og relevante for mottaker, må den taushetspliktige selv foreta vurderingen.¹

Datatilsynet vil bemerke at departementet synes å legge til grunn en annen forståelse av taushetspliktens innhold. I høringsnotatet heter det:

"Per i dag er praksis på sykehus i all hovedsak slik at papirjournalen utleveres fra arkivet på forespørsel." ... "Mottas det forespørsel fra eksterne leger om utlevering av journal kopi, så vil slik kopi normalt bli utlevert. Såfremt den som behandler forespørselen ikke fatter

¹ Dette er et prinsipp som tilsynet har hevdet også når det gjelder NAV og forsikringsbransjens tilgang til journalopplysninger. Helsepersonellet må foreta en vurdering av hvilke opplysninger (om noen) som skal leveres ut fra journalen. Bare unntaksvis skal den fulle journalen leveres ut.

mistanke om at noe er galt, vil en vanligvis ikke kontrollere de opplysninger den som forespør kommer med."²

Departementet synes å akseptere denne praksisen. Forslaget om tilgang på tvers av virksomhetsgrensene synes endog å innebære en automatisering av den beskrevne prosessen. Datatilsynets stiller imidlertid spørsmål ved om praksisen er lovlig i henhold til gjeldende bestemmelser om taushetsplikt (med mindre man har pasientens samtykke til utleveringen).

Departementets forutsetter at de foreslåtte lovendringene ikke skal medføre en svekkelse av taushetsplikten. Departementet forutsetter således at **metoden** for informasjonsutveksling ikke får betydning for hvilken **informasjon** som faktisk blir utvekslet.

Datatilsynet deler ikke departementets oppfatning. Det å gi noen *tilgang* til en pasientjournal skiller seg, etter tilsynets vurdering, vesentlig fra det å *utlevere* journalopplysninger. Det vises til at utlevering muliggjør en vurdering hos utleverende helsepersonell av om vilkårene for å avgi hele eller deler av pasientjournalen er tilstede. Med andre ord å fastslå om pasienten samtykker til utleveringen eller om utleveringen er nødvendig for å gi helsehjelp. Departementets forslag åpner for selvbetjening i den enkelte pasients journal. Dette medfører en svekkelse av taushetsplikten som Datatilsynet sterkt vil fraråde.

Datatilsynet ønsker å bemerke at taushetsplikten for opplysninger som ikke er relevante og nødvendige i teorien kan ivaretas også når man gir *tilgang* til opplysninger. Det forutsetter imidlertid at man er faktisk i stand til å gi tilgang bare til de journalopplysninger som man på forhånd har vurdert å være nødvendige og relevante. De elektroniske pasientjournaler som i dag brukes ved landets helseforetak er imidlertid bygget opp slik at opplysningene ikke er systematiserte, utover at opplysningene føres kronologisk. Selve journalnotatene skrives som fritekst, og det er ikke noe logisk skille mellom ulike sykdoms- eller behandlingsforløp hos en og samme pasient. Tilgang til slike journaler vil derfor lett medføre en utlevering av opplysninger som ikke er relevante og nødvendige, og derfor ikke skulle ha vært utlevert. Endringer i dagens journalsystemer for å muliggjøre den nødvendig systematiseringen av journalopplysningene er ikke berørt i departementets forslag, og vil etter det tilsynet erfarer medføre betydelige kostnader.

I det at taushetsplikten er en *personlig plikt* for det enkelte helsepersonell ligger at helsepersonell også skal bevare taushet *overfor hverandre*. Dette gjelder selv når man er kolleger innen et helseforetak eller på et lokalt fastlegekontor.

Datatilsynet har erfart at helsepersonellet i praksis ikke evner å etterleve dette utgangspunktet. Det har skjedd en dramatisk utglidning i forbindelse med innføring av elektroniske informasjonssystemer i helsesektoren. Datatilsynets kontroller har vist at både helsepersonell og andre ansatte i helsesektoren gjennomgående har alt for vid tilgang til å tilegne seg pasientopplysninger i den elektroniske journalen og de administrative systemer. Samtidig er virksomhetens kontroll med hvilke opplysninger den enkelte ansatte faktisk tilegner seg alt for svak.

² Kapittel 5, fjerde avsnitt

Bransjen har altså ikke lyktes med å etablere informasjonssystemer med en tilgangsstyring som reflekterer den enkelte ansattes tjenstlige behov. Når den enkelte behandlingsinstitusjon ikke makter å sørge for at informasjonskontrollen internt støtter opp om den enkelte ansattes *personlige* plikt til å bevare taushet overfor sine kolleger, representerer *virksomhetens* grenser en nødvendig ytre grense for informasjonsflyten.

Denne grensen er etter tilsynets vurdering alt for vid, sett hen til utgangspunktet om at taushetsplikten er en personlig plikt. Det er imidlertid den eneste reelle grensen som eksisterer per i dag. Datatilsynet vil derfor advare mot departementets lovforslag, som i realiteten innebærer at også virksomhetsgrensene viskes ut. Man står derved i fare for en fri flyt av pasientopplysninger, ikke bare blant ansatte i den enkelte virksomhet, men blant de ansatte i hele sektoren som sådan.

Den muligheten en pasient har til å føre en viss kontroll med sine opplysninger, gjennom for eksempel å velge et annet behandlingssted enn det sykehuset hvor naboen er ansatt, vil bortfalle som følge av denne utviklingen. Pasienten må da påregne at de opplysninger som gis til ett sykehus kan bli gjort tilgjengelige for samtlige ansatte i hele helsesektoren.

Taushetsplikten er den bærende bjelken i tillitsforholdet mellom pasient og helsepersonell. En situasjon hvor journalføring medfører en større spredning av helseopplysninger enn det behandler og pasient føler er komfortabelt, vil kunne få svært uheldige konsekvenser.

Man kan risikere at det føres færre eller andre opplysninger i journalen enn det som ellers ville ha blitt ført. Dette antas å gjelde særlig hos fastlegen. I forlengelsen av dette risikerer man at helsepersonellet i stedet nedtegner opplysninger på steder hvor informasjonssikkerheten ikke er tilfredsstillende ivaretatt (skyggejournaler). Dersom pasienten ikke har tillit til at helsepersonellet evner å bevare sin taushet, vil man i verste fall risikere at pasienter vegrer seg mot å gi helsepersonellet opplysninger som en nødvendige for helsehjelpen.

En uthuling av taushetsplikten fremmer etter tilsynets vurdering ikke forsvarlig helsehjelp.

3 Nærmere om det helsefaglige behovet

I høringsnotatet begrunnes forslaget med at det foreligger et helsefaglig behov³. Det anføres at tilgang på tvers av virksomhetsgrenser, og etablering av virksomhetsovergrepene journaler er *nødvendig for å gi forsvarlig helsehjelp*.

3.1 Generelt

Innledningsvis vil Datatilsynet bemerke at det er et tankekors at initiativet til de foreslåtte endringene ikke kommer fra et samlet medisinsk fagmiljø, fra pasientorganisasjoner eller fra helsetilsynsmyndighetene, men fra helsedepartementet og de regionale helseforetak. Dersom

³ Høringsnotatets kapittel 5

man har en situasjon hvor manglende tilgang til helseopplysninger fører til uforsvarlig helsehjelp, antar tilsynet at både pasientene, fagmiljøet og helsetilsynsyndighetene ville tatt initiativ til de nødvendige endringene. Datatilsynet har i den forbindelse merket seg at departementets forslag heller ikke er overensstemmende med fagdirektoratets anbefalinger⁴.

Tilsynet tillater seg også å peke på det ulogiske i at tilgang på tvers av foretaksgrenser skal bero på frivillighet i det enkelte helseforetak (avtaleinngåelse). Dersom tilgang på tvers faktisk er nødvendig for å gi forsvarlig helsehjelp, så burde vel ordningen være obligatorisk?

3.1.1. Særlig om ivaretagelse av pasientens råderett

Forslaget reflekterer ikke det forhold at det først og fremst er hensynet til pasientene selv som begrunner lovendringene.

Datatilsynet mener det er grunn til å anta at de aller fleste pasienter *ikke* har behov for at *alle* deres helseopplysninger potensielt er tilgjengelige ved *alle* behandlingsinstitusjoner i hele landet. Samtidig er det viktig å imøtekomme behovet til de som har et *spesielt behov* for økt tilgjengelighet til *hele eller deler* av sin journal (kronisk syke, allergikere osv).

Med utgangspunkt i pasientens rett til å råde over egne opplysninger, bør pasienten 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 vil derfor anbefale en ordning hvor den obligatoriske "normalsamhandlingen" mellom virksomhetene er moderat, og hvor det etableres frivillige "tilleggs løsninger" spesielt tilpasset den enkelte pasients egendefinerte behov.

3.2 Nærmere om alternative samhandlingsformer

Datatilsynet erkjenner at dagens løsninger for samhandling i forbindelse med pasientbehandling er uhensiktsmessige. Heller ikke Datatilsynet støtter en praksis hvoretter pasientjournaler sendes med taxi mellom de ulike sykehus.

Tilsynet vil imidlertid peke på at det finnes alternative samhandlingsløsninger som tilfredsstiller behovet for informasjonsdeling, samtidig som de ivaretar personvern hensyn.

Datatilsynet savner at den enkelte samhandlingsformen er utredet konkret i forhold til behovet i den enkelte behandlingssituasjon.

3.2.1. Elektronisk meldingsutveksling

Etter Datatilsynet oppfatning er elektronisk meldingsutveksling en samhandlingsform som godt ivaretar hensynet til taushetsplikten. Meldingsutveksling innebærer en *utlevering*, og muliggjør således en konkret medisinsk faglig vurdering av om taushetsplikten er til hinder for utlevering av pasientopplysninger i det enkelte tilfellet.

⁴ Jf Helsedirektoratets rapport, våren 2008

Elektronisk meldingsutveksling er en svært effektiv samhandlingsform. Selve meldingsutvekslingen er ikke nødvendigvis mer tidkrevende enn det å benytte en egen tilgang inn i pasientjournalen⁵.

Det som tar tid er avgivers ivaretagelse av taushetsplikten, altså vurderingen av hvorvidt det er adgang til å levere ut opplysninger. Den totale tidsbruk vil derfor bestemmes av avgivers ressursbruk og interne rutiner knyttet til avgivelsen, ikke av om opplysningene sendes som melding eller gjøres tilgjengelige i avgivers journalsystem.

Er pasienten i stand til å avgi et samtykke, vil avgiver kunne sende elektronisk de opplysningene pasienten ber om nærmest umiddelbart. Egen tilgang til journalen gir kun en marginal tidsmessig gevinst i disse tilfellene.

Dersom pasienten ikke er i stand til å avgi et samtykke skal avgiver foreta en egen vurdering av hvilke opplysninger som er nødvendige og relevante for mottaker. I visse tilfelle kan uansett hele journalen sendes. Heller ikke her spiller det en avgjørende rolle hvorvidt opplysningene går tilbake som en melding eller om man benytter en tilgang inn i journalen.

Meldingsutveksling vil, etter tilsynets vurdering tilfredsstillende det meste av behovet for samhandling i forbindelse med *planlagte* behandlingsforløp (etter timebestilling, henvisning osv)

Meldingsutveksling har bare i begrenset grad blitt tatt i bruk innen helsesektoren. Dette skyldes i hovedsak at for få enheter er koblet til meldingssystemet (Norsk Helsenett), og at det er utviklet for få standardiserte meldingstyper. Tilsynet mener at det ligger et stort potensial i elektronisk meldingsutveksling, og at en vesentlig del av behovet for elektronisk samhandling innen helsesektoren vil kunne ivaretas meldingsbasert.

3.2.2 Samtykkebasert kjernejournal

Tilsynet ser at det vil foreligge et behov som den meldingsbaserte samhandlingen ikke avhjelper tilfredsstillende. Dette behovet er etter tilsynets vurdering så begrenset at det ikke nødvendiggjør en så omfattende og personverntruende endring som departementet her legger opp til.

Datatilsynet vil her særlig peke på samtykkebasert kjernejournal, som en samhandlingsform som godt ivaretar behovet for tilfredsstillende informasjonsdeling, samtidig som pasientens autonomi bevares.

En kjernejournal vil kunne løse samhandlingsbehovet for pasienter som har et *særskilt behov* for at visse opplysninger skal være mer tilgjengelige enn det den meldingsbaserte samhandlingen tillater. Som eksempel nevnes kronisk syke eller andre som vil slippe å gjenta sine helseopplysninger hver gang de oppsøker ny behandler eller helseinstitusjon⁶.

⁵ Forutsatt at taushetspliktens innhold ikke endres, jf tilsynets innledende merknader

⁶ kapittel 5, sjette avsnitt

En frivillig kjernejournal vil også kunne inneholde *vitale opplysninger* som er nødvendige i forbindelse med akuttsituasjoner, for eksempel relevant medisiner og allergier.

En kjernejournal bør imidlertid være en *fleksibel og frivillig* løsning. Pasientene bør selv bestemme, i samråd med behandlende personell, hvorvidt man ønsker å ha opplysninger i kjernejournalen, hvilke opplysninger som i så fall skal føres inn og hvorvidt journalen skal være tilgjengelig nasjonalt, regionalt eller lokalt. Her kan også konkrete reservasjoner inntas, for eksempel på virksomhetsnivå.

Datatilsynet vil peke på at informasjonstilfanget ved direkte tilgang til hele journalen i mange tilfeller vil bli svært omfattende, og at informasjonen vil ha varierende kvalitet. Det kan derfor stilles spørsmål ved hvilken *umiddelbar* nytte behandlende personell generelt vil kunne dra av en slik tilgang, særlig i en akutfase

Det vises for det første til at det er et velkjent problem (særlig innen sykehussektoren) at det tar uforholdsmessig lang tid før den elektroniske journalen oppdateres. Tekniske løsninger for å korte ned tiden er under utvikling og implementering, men det vil ta lang tid før disse er tatt i bruk i hele sektoren.

Videre vises det til at journalnotater i all hovedsak skrives som fri tekst. De får derved en personlig utforming som kan gjøre opplysningene vanskelig tilgjengelig for andre enn den som selv har nedtegnet dem.

En samtykkebasert kjernejournal vil etter tilsynets vurdering gi et bedre *presisjonsnivå* på de opplysningene som gjøres tilgjengelige for behandlende personell, enn det den direkte tilgangen til hele journalen gir. Behov for ytterligere opplysninger kan ivaretas gjennom meldingsbasert kommunikasjon.

3.3 Nærmere om virksomhetsovergrepene registre

Datatilsynet vil bemerke at både høringsnotatet og bestemmelsen er uklar på dette punktet. Uklarheten knytter seg til omfanget av og behovet for registrene.

I forslag til endringer i helseregisterlovens § 6a heter det at registrene skal inneholde ”de nærmere bestemte helseopplysningene som er nødvendig og relevante for samarbeid om forsvarlig helsehjelp”.

Datatilsynet kan ikke se at dette i realiteten innebærer et begrenset innhold, i forhold til ordinær virksomhetsintern journal. Enhver pasientopplysning er etter omstendighetene en potensielt ”nødvendig og relevant” opplysning for medisinsk behandling. Dette gjelder enn mer når man ser flere virksomheters behandlingsområde under ett. Slik tilsynet leser bestemmelsen vil man svært fort havne i en situasjon hvor hver enkelt helseregion har en felles fullstendig pasientjournal, som en samlet kopi av hver enkelt virksomhets interne journal.

Det medisinskfaglige behovet for et ”dobbel” bokholderi er etter tilsynet vurdering ikke dokumentert. Datatilsynet er derfor av den oppfatning at både innhold og tilgang til et

virksomhetsovergripende register i størst mulig grad bør besluttes av pasienten selv, i samråd med behandlende personell.

Datatilsynet vil også bemerke at pasientjournaler etter sin art er unntatt fra konsesjonsplikt, iht personopplysningsforskriftens § 7-26. I utgangspunktet vil dette unntaket også gjelde for virksomhetsovergripende journalsystemer, med mindre annet bestemmes særskilt.

3.4 Særlig om tilgang til pasientjournal for andre formål enn pasientbehandling

I forskriftsutkastets §§ 13 – 15 åpnes det for tilgang for andre formål enn pasientbehandling. Innledningsvis vil Datatilsynet bemerke at høringsnotatet knapt berører disse bestemmelsene, hvilket må være i strid med utredningsinstruksen med veileder⁷.

Tilsynet vil videre bemerke at bestemmelsene er oppsiktsvekkende vide. Dette gjelder særlig § 15. Det er ikke angitt hvem som skal kunne få tilgang, og til hvilket formål tilgangen skal kunne benyttes (bare formålet er ”forhåndsbestemt”). For Datatilsynet er det et paradoks at man i regelverket for øvrig gjennomgående begrenser tilgangen til å gjelde formålet medisinsk behandling, for deretter å gi en generell åpning for tilgang til alle andre formål.

Den eneste skranken som settes, for andre formål enn medisinsk behandling er taushetsplikten. Dette innebærer at lovgiver åpner for at enhver som kan kreve å få utlevert opplysninger fra pasientjournaler, skal kunne få direkte tilgang til journalen. I henhold til merknadene skal adgangen gjelde for eksempel for tilsynsmyndighetene. Etter sin ordlyd vil bestemmelsen allikevel gi tilsvarende adgang for en stor personkrets, herunder NAV, politi, forsikringsselskaper, forskere, administrativt personell osv.

Utkastet kan forstås slik at det er mindre problematisk å gi tilgang til pasientjournaler for andre formål enn medisinsk behandling. Dette kan neppe være intensjonen.

Datatilsynet forutsetter derfor at spørsmålet om tilgang for andre formål enn pasientbehandling utredes på nytt.

4 Informasjonssikkerhet

4.1 Kort om tilgangsstyring internt ved helseforetakene

Man kan ikke vurdere forsvarligheten av å bryte ned betydningen av foretaksgrensene, uten å se på helseforetakenes evne til sørge for en forsvarlig tilgangsstyring internt i egen virksomhet.

Helseforetakenes interne tilgangsstyring har vært gjenstand for utstrakt kontroll og massiv kritikk fra både Datatilsynet og Helsetilsynet. Tilsynsmyndighetene har avdekket at de elektroniske pasientjournalsystemene som benyttes ved sykehusene ikke er egnet til å gi den

⁷”Instruks om utredning av konsekvenser, foreleggelse og høring ved arbeidet med offentlige utredninger forskrifter, proposisjoner og meldinger til Stortinget” (FAD)

enkelte ansatte 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. Tilsynet vil bemerke at det er gjort tilsvarende funn ved en rekke helseforetak. Dette tyder på at avvikene til en viss grad er systemavhengige.

Etter tilsynets vurdering går departementet altfor langt i å "friskmelde" helseforetakenes interne tilgangsstyring⁸. Dette gjøres uten at departementet dokumenterer å ha gjennomført egne kontroller ved angjeldende foretak, og uten at tilsynsmyndighetene er konferert. Tilsynet finner dette oppsiktsvekkende.

Etter tilsynets erfaring vil problemene med tilpasset tilgangstyring hefte ved jorunalsystemene i overskuelig fremtid, med mindre man investerer betydelige beløp i å utvikle eller erstatte eksisterende journalsystemer. Datatilsynet har, i samarbeid med Helsetilsynet, iverksatt nye etterundersøkelser. Arbeidet er ikke sluttført ved høringsfristens utløp, men tilsynet vil holde departementet og allmenheten oppdatert om de funn som gjøres.

4.2 Forslag til forskrift om informasjonssikkerhet

4.2.1. Generelt

Departementet synes å anføre at den nye forskriftens krav til informasjonssikkerhet innebærer en forsterket sikkerhet, som gjør at det er forsvarlig å åpne for tilgang på tvers samt å etablere virksomhetsovergrepene systemer. Dette er en oppfatning Datatilsynet ikke deler.

Datatilsynet er i utgangspunktet positivt til en forskriftsfesting av de nærmere kravene til informasjonssikkerhet i forbindelse med samhandling ved pasientbehandling. Tilsynet beklager derfor at vi ikke har funnet noe som tyder på at forskriften i nevneverdig grad stiller andre eller strengere krav til informasjonssikkerheten i helseforetakene enn det som allerede følger av gjeldende regelverk.

Datatilsynet stiller spørsmål ved hensiktsmessigheten av å erstatte gjeldende krav i personopplysningsforskriften med de foreslåtte krav.

4.2.2 Korte merknader til enkelte bestemmelser

Datatilsynet har en rekke merknader til bestemmelsene. Av ressursmessige hensyn kan vi i denne omgang bare gi korte merknader til enkelte av disse:

- §17 Krav om autentisering

Datatilsynet anser at kravet til autentisering bør styrkes, til 2-faktor autentisering⁹. Dette gjelder også for tilgang internt i virksomheten.

⁸ Høringsnotatet kap 6.2

⁹ Det vises til også til helsepersonellovens § 21b og helsetilsynets foreløpige praktisering av denne. Med dagens krav til autentisering vil forbudet mot smoking fort miste realitet.

- § 21 Krav om logging

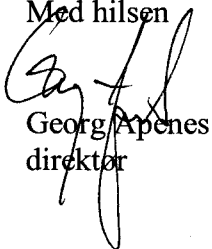
Plikten til logging følger også av dagens regelverk. Plikten har imidlertid ikke ført til at helseforetakene har etablert tilfredsstillende kontroll med de ansattes bruk av tildelt tilgang. Det skal også bemerkes at logging ikke er et egnet substitutt for tilfredsstillende tilgangsstyring.

- § 23 Innsyn i logg

Datatilsynet støtter en tydeliggjøring av pasientens rett til å få tilgang til logg. Prinsippet er viktig. Men den direkte nytte den enkelte pasient vil ha av å få tilgang til egen logg kan i mange tilfeller diskuteres. Dette gjelder særlig hvis man ikke skjerper kravet til autentisering i pasientjournalen.

Datatilsynets utdyper gjerne denne høringsuttalelsen, for eksempel i et møte med departementet.

Med hilsen



Georg Apenes
direktør



Cecilie L. B. Rønnevik
seniorrådgiver

Kopi: Fornyings- og Administrasjonsdepartementet, v/Statsforvaltningsavdelingen,
Pb 8004 Dep, 0030 Oslo