Oslo universitetssykehus

Helse- og omsorgsdepartementet
postmottak@hod.dep.no

Dokumentet sendes bare elektronisk

Oslo universitetssykehus HF
Postboks 4950 Nydalen
0424 Oslo

Sentralbord: 02770

Medisin og helsefag

Vår ref.:	Deres ref.:	Saksbeh.:	Dato:
2010/20181	201001921-/ASD		07.09.10
(oppgis ved all henvendelse)			

Svar på høring: Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Generelt

Det vises til forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.

Taushetsplikten er en forutsetning for tillitsforholdet mellom pasient og helsepersonell. Det er derfor en utfordring for alle som skal behandle helse- og personopplysninger at folks tiltro til helsevesenet synes å ha falt de siste årene, ref tilsyn samt uttalelser fra ansatte som vegrer seg for å bruke eget helseforetak fordi opplysningene oppfattes til å være for lett tilgjengelig. Forslaget til ny forskrift vil kunne bedre tilgjengeligheten av pasientinformasjon, - noe som er ønskelig for pasienter som behandles på tvers av de juridiske skillelinjer som danner helseforetakene, og som kan medføre bedre og mer forsvarlig pasientbehandling for disse pasienter. Dersom man åpner for at flere kan få tilgang til pasientens sensitive helse-opplysninger, vil dette samtidig medføre en økt risiko for spredning av sensitive person-opplysninger. Dersom informasjonssikkerheten ikke er tilstrekkelig ivaretatt når informasjonen blir gjort tilgjengelig for flere enn de som i dag har tilgang, vil forslaget til ny forskrift kunne få negative konsekvenser for konfidensialiteten og personvernet til pasientene. Dette kan påvirke tilliten pasientene har til håndteringen av sensitive personopplysninger, og føre til at viktige helseopplysninger derfor holdes tilbake. Dette igjen kan påvirke negativt den helsehjelp den enkelte dermed gis. Hensikten som er ment med denne lovendring og forskrift, vil dermed kunne resultere i negativ effekt for helsehjelpen. Det vil også være et brudd med Stortingets forutsetning, som ved lovforslaget danner grunnlaget for den foreslåtte forskrift, og som presiserte at taushetsplikten ikke skulle påvirkes av den utvidede tilgangsmuligheten.

Det er positivt at forskriften vil styrke informasjonssikkerheten ved å innføre gode prinsipper for tilgangsstyring som minsker faren for at pasientopplysninger kommer på avveie. Likevel er det slik at de løsninger som skisseres i forskriften, i svært begrenset grad eksisterer som muligheter i de journalsystemene som benyttes ved de ulike helseforetakene. Forslagene til løsning som forskriften skisserer, vil medføre formidable økonomiske kostnader. Disse kostnadene er utvilsomt langt utenfor virksomhetens ordinære budsjettrammer. Det stilles derfor spørsmål ved realiserbarheten av de nevnte forslag.

Forskriften som er på høring, setter til dels svært detaljerte krav til journalsystemene. Dette innbefatter i tillegg til store tekniske utfordringer for journalleverandørene, også betydelige økonomiske konsekvenser. Det fremgår av høringsnotatet at det legges opp til at kravene i forskriften kan settes i verk på forskjellige tidspunkt. Helse- og omsorgsdepartementet mener kravene i forskriften kap. 1, 2, 3 og 5 kan settes i verk fra 01.06.2011. Dette er etter vårt syn svært urovekkende, særlig med tanke på at kapittel 5 omhandler tilgang på tvers med direkte lesetilgang. En slik tilgang på tvers hvor helsepersonell autentiseres i eget system, krever *federering*. Dette vil si at man autentiseres i ett system, og så gis tilgang til et annet system basert på "tillitssamarbeid" mellom ulike system. Systemet en autentiseres i, skal med andre ord kontrollere og sikre tilgangen i det andre systemet. Dette er ikke etablert i nåværende løsninger, og vil kreve store investeringer for å etableres. En delvis innføring av forskriften vil dermed bryte med forutsetningene lagt i Stortinget da lovendringene ble vedtatt, og vil kunne påvirke pasienters tillit til helseforetakenes evne til å sikre journalopplysninger og ivaretakelse av taushetsplikten. Dette igjen kan gjøre at pasienter holder tilbake inngripende, men viktig informasjon for den helsehjelp de skal motta. Den faktiske innføringen av tilgangen på tvers, må derfor ha tilstrekkelige sikkerhetsmekanismer i det funksjonalitet blir innført for at forutsetningene om opprettholdelse av taushetsplikten kan ivaretas.

Det synes også som umulig for foretaket som besitter opplysningene og som leses av ansatte i andre foretak, å vite om grunnlaget for oppslag og lesing faktisk har et gyldig hjemmelsgrunnlag.

Det virker derfor som det er et alvorlig gap mellom hva Stortinget satte som forutsetning, det vil si opprettholdelse av taushetsplikten, og den faktiske evnen til å få dette realisert. Per i dag finnes det ikke tekniske løsninger for slik funksjonalitet. Det synes heller ikke som vi har de økonomiske krefter som skal til for å implementere den skisserte løsning. Spørsmålet blir da fort om dette resulterer i en avkorting på kravene til sikkerhet, hvilket slett ikke er å anbefale. Det vil etter vår mening få store konsekvenser for informasjonssikkerheten ved virksomhetene, dersom man velger å sette i verk deler av kravene i forskriften uten at systemene er tilfredsstillende.

Det understrekes av høringsnotatet at forskriften som er på høring, er mer detaljert og bedre tilpasset helsesektorens virkelighet enn personopplysningsforskriften. Vi kan ikke se at forskriftens kapittel 2 om generelle krav til informasjonssikkerhet stiller andre særlige krav til informasjonssikkerhet, enn hva som følger av gjeldende lovverk. En uheldig konsekvens av dette kan være at man leser forskriften og samtidig tror at man ikke trenger å forholde seg til annet regelverk. Et alternativ kan derfor være å utarbeide rundskriv med fortolkninger av hvordan regleverket skal forstås.

Det vil bemerkes at man i forskriften opererer med en ulik begrepsbruk. I forskriften § 4 benyttes begrepet "forsvarlig informasjonssikkerhet", mens det i §§ 1 og 7 omtaler begrepet "god informasjonssikkerhet". Det er ikke tydeliggjort hva forskjellen er i de nevnte begreper. En slik ulik begrepsbruk synes uheldig. Det vises videre til at kravene i henhold til personopplysningsloven og helseregisterloven er "tilfredsstillende informasjonssikkerhet", jf. personopplysningsloven § 13 og helseregisterloven § 16, og som krever en gjennomført risikovurdering som grunnlag for hva "tilfredsstillende informasjonssikkerhet" innebærer, og som tilsynsmyndighet har myndighet til å overprøve.

Merknader til de enkelte paragrafene i forskriften:

§ 3 Definisjoner
Det følger av forskriften § 3 nr. 4 at "Pålogging kan skje fra den interne virksomhet eller fra den eksterne virksomhetens system." I høringsnotatet (s.30) fremgår det at "Forespørselen skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet." Det er uklart hva departementet egentlig mener her.

I merknaden til § 3 brukes begrepet to-faktor autentisering for å betegne et høyere nivå av sikkerhet enn ved bruk av bruker-ID og passord. Autentisering har ulike grader av styrke og to-faktor autentisering er et eksempel på en praktisk løsning for sterk autentisering. Bruken av begrepet *sterk autentisering* anbefales benyttet for høyere nivå av sikkerhet enn kombinasjon av bruker-ID og passord.

§ 4 Krav om forsvarlighet
I merknaden til § 4 fremgår det at "Kravet om forsvarlighet kan ivaretas ved gode beredskapsrutiner som sikrer manuell håndtering av personopplysninger eller tilgang til opplysninger i en teknisk offline løsning." Ved en driftsstans, vil en teknisk offline løsning ikke være gjennomførbart. Det synes heller ikke hensiktsmessig å ha (sikkerhets)kopier av alle data i tilfellet systemet skulle være nede.

§ 9 Krav om system for administrering av autorisasjoner
I merknaden til § 9 fremgår det at helsepersonell som gis myndighet til å treffe beslutning om innholdet i en autorisasjon, må ha helsefaglig kompetanse. Det er ikke alle ledere i virksomheten som administrerer autorisasjoner, som har "helsefaglig kompetanse". Leder uten slik kompetanse selv, vil innen eget myndighetsområde ha tilgjengelig den nødvendige kompetanse for de vurderinger som må gjøres. Videre kan det reises tolkningstvil rundt hva som ligger i begrepet "helsefaglig kompetanse".

§ 10 Krav til tilgangsstyringen – forholdet til taushetsplikt
Det er i dag en stor utfordring for helseforetakene å sørge for en riktig tilgangsstyring. Tilgang til helseopplysninger i pasientjournalen skal i utgangspunkt kun gis til helsepersonell i den grad dette er nødvendig for å yte pasienten helsehjelp og i den grad pasienten ikke motsetter seg det.

I § 10, 1. ledd bokstav a-c er det listet opp tre ulike faktorer som skal inngå i vurderingen av tilgangskontrollen. Det er etter vårt syn uhensiktsmessig med en slik mengdekvantifisering av tilgangskontroll, da tilgang til helseinformasjon alltid vil måtte gis ut fra det enkelte helsepersonell sitt behov i forhold til helsehjelpen som skal ytes.

Sikkerheten skal i henhold til personopplysningsforskriften være forholdsmessig, dvs. stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Her vil både størrelsen på det aktuelle systemet, antall brukere og antall pasienter påvirke risikonivået. En risikovurdering skal underbygge hva som er tilfredsstillende sikkerhet (akseptabelt risikonivå). Kravene som er listet opp i pkt a-c fremstår som svært detaljerte og uttømmende, og burde forslagsvis heller stå i merknaden som eksempler på hva som bør vurderes. Der vil også være andre forhold som må vurderes enn de som er angitt i punkt a-c. Andre elementer som vil være av betydning for sikkerheten vil være hvilke opplysninger og hvordan disse står i forhold til formålet med

opplysningene, Detaljerte krav bør tas ut av forskriften, slik at databehandlingsansvarlige selv må tallfeste eller konkretisere hvilke parametre tilgangen skal vurderes og konfigureres etter i henhold til akseptabelt risikonivå og tilfredsstillende sikkerhet.

Det fremgår av høringsnotatet at autorisasjonen skal være tidsbegrenset. Etter departementets vurdering, er det ikke noe i veien for at en autorisasjon kan ha en varighet på 1 til 2 år. Dette er etter vår mening urealistisk, særlig med tanke på de større virksomhetene. Det viktigste etter vårt syn er at kravene til tilgangsstyringen er gode nok og at når det gjelder tidsbegrensning av autorisasjoner, så må den følge den ansattes funksjon og virke. Endres arbeidsforhold/oppgaver, så må autorisasjonen endres.

§ 14 Autorisasjon for ytelse av helsehjelp
Det fremgår av merknaden til § 14 at pasientens journal må struktureres slik at det er mulig å autorisere for særskilte deler av journalen. Det gis eksempel på at en autorisasjon til å behandle helseopplysninger registrert på bakgrunn av gynekologisk helsehjelp, ikke uten videre også innebærer at ansatt på ortopedisk kirurgisk avdeling har tilgang til opplysningene.

Direkte tilgang på tvers av virksomheter forutsetter at opplysningene er registrert på en standardisert måte, og bestemmelsen setter store krav hva gjelder journalens struktur. Dagens pasientjournal består i stor grad av fritekst, og en slik strukturering av journalen vil være svært ressurskrevende å etablere. Det er dessuten uhensiktsmessig å avgrense journalen i forhold til graden av stigmatisering. Det vil etter vårt syn være mer hensiktsmessig å sperre deler av journalen dersom den inneholder informasjon som bør være sperret.

Det fremgår av § 14, 4. ledd at det kan gis autorisasjon til elever og studenter som gir helsehjelp i forbindelse med helsefaglig opplæring. Merknaden til bestemmelsen omtaler også bruk av journalopplysninger til kvalitetssikring. Vi viser til at hjemmelsgrunnlaget for bruk av helseopplysninger til kvalitetssikring er helsepersonelloven § 26. Videre fremgår det "at opplysninger og bilder som brukes til undervisning i størst mulig krav kan fremstå som anonyme for mottakerne/tilhørerne." Denne setningen er egnet til å skape misforståelser da opplysningene som brukes til undervisning *skal* være fullstendig anonyme. Dersom de ikke er det, kreves det konsesjon fra Datatilsynet for slik bruk.

§ 17 Krav om register over og kontroll av autorisasjoner
Det skal etter § 17 etableres et eget register over utstedte autorisasjoner som skal inneholde informasjon om hvem som er tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varighet og om et eventuelt tilbakekall av autorisasjonen. Et slikt register vil måtte håndteres manuelt, noe som nærmest er umulig og vil være svært ressurskrevende, dette gjelder særlig de store helseforetakene. En manuell oversikt vil også med stor sannsynlighet ikke være korrekt. Oversikt over autorisasjoner vil måtte tas ut av de aktuelle elektroniske løsninger de ligger i for å være korrekte. Videre vil grunnlaget for gitt autorisasjon måtte leses ut av dette sammen med foretakets prinsipper for tildeling av rettigheter.

§ 19 Tilgang til helseopplysninger for ytelse av helsehjelp
Ifølge merknaden til § 19 forskriftsfester bestemmelsens 1. ledd den beslutningsstyrte tilgangen. Det fremgår av høringsnotatet at tilgangen skal følge av en konkret beslutning om at en bestemt

pasient skal gis helsehjelp. Dette er etter vår mening upresist. Slik *vi* forstår beslutningsstyrt tilgang, innebærer dette at helsepersonell tar en beslutning om å yte helsehjelp, som igjen medfører at annet helsepersonell som også skal yte helsehjelp - gis tilgang til de relevante og nødvendige opplysninger. Basert på vår forståelse av begrepet "beslutningsstyrt tilgang", er dette ikke implementert i vår virksomhet, og finnes etter vår kjennskap heller ikke teknisk i noen av journalløsningene som benyttes.

I § 19, 4. ledd fremgår det at "Dersom opplysningene antas å være følsomme for pasienten eller det kan antas at pasienten vil føle seg ubekvem dersom opplysningene ble kjent av andre, skal helsepersonell gjøre pasienten oppmerksom på sperring". Av merknaden til § 19, 4. ledd fremgår det videre at "Dersom opplysningene i sist nevnte tilfeller ikke kan antas å være nødvendig for annet helsepersonell, bør opplysningene som et utgangspunkt sperres". Etter vår mening legges det nærmest opp til at utgangspunktet skal være at opplysningene bør sperres dersom man antar at de ikke vil være relevante for annet helsepersonell. Det er etter vår vurdering ikke hensiktsmessig å skulle forhåndsvurdere annet helsepersonell sitt behov for informasjon, og generelt bør man være svært varsom med å forsøke å forutse hva som i fremtiden kan være relevante opplysninger. Etter vår vurdering er det den som forespør informasjonen som er best til å vurdere hva som i den aktuelle situasjonen er relevante opplysninger. Slik § 19, 4. ledd er utformet, legges det her opp til at helsepersonell skal vurdere om de skal anbefale pasienten å sperre opplysninger. En eventuell sperring av opplysingene bør skje etter initiativ fra pasienten, og bare unntaksvis av helsepersonellet. Et annen viktig moment er at det vil være arbeidskrevende for virksomheten å skulle håndtere et stort antall forespørsler om sperring av journal. Dette spesielt fordi de tekniske mulighetene for gjennomføring av sperring er svært tungvinne og begrenset i sin funksjonalitet. Sperring av et dokument krever at dokumentene først sperres for alle, og så må hver enkelt helsemedarbeider som skal gis tilgang, individuelt legges inn. Dette gjelder det journalsystem som brukes i hoveddelen av OUS. Forvaltning av dette i stort omfang er nærmest praktisk umulig. Dette vil også være en risiko for helsehjelpen som ytes, siden manglende opplysning om alle som skal ha tilgang, vil kunne medføre at helsepersonell som ikke er oppgitt til å ha tilgang, ikke vil ha teknisk mulighet til å få tilgang. Selv om taushetsplikten krever begrensninger i tilgang, vil en for streng forvaltning av tekniske muligheter for tilgang medføre at helsepersonell ikke har mulighet til å få tilgang til viktige opplysninger for den aktuelle pasients helsehjelp.

§ 21 Tilgang til helseopplysninger for personell med støttefunksjoner
Forskriften § 16 omtaler autorisasjon for ytelse av nødvendige støttefunksjoner, mens § 21 inneholder bestemmelser om tilgang til helseopplysninger for personer med støttefunksjoner. § 21 er etter vår mening overflødig i og med at dersom man gis tilgang, vil man på forhånd være autorisert.

Fra merknaden til 21 fremgår det at "I utgangspunktet legges det til grunn at service på det elektroniske systemet bør kunne utføres uten at det gis tilgang til helseopplysninger." Dette vil etter vår mening være vanskelig å gjennomføre i praksis.

I merknaden til § 21, 3. ledd er databehandlingsansvaret eksemplifisert. I det andre eksempelet som er vist, kan det se ut som om virksomhet 2 blir databehandlingsansvarlig for opplysninger i virksomhet 1. Det er virksomhet 1 som er databehandlingsansvarlig for opplysninger i virksomhet 1. At to juridiske enheter begge skal være databehandlingsansvarlig for samme

instans av informasjon, synes nærmest umulig. Vi viser for øvrig til personopplysningsloven § 2 vedrørende definisjonen på "behandlingsansvarlig".

§ 22 Avtale om direkte lesetilgang til helseopplysninger på tvers av virksomheter
Dagens pasientjournal består av mange store og små systemer. En muliggjøring av tilgang på tvers vil derfor kreve store økonomiske ressurser. Selv om det kun etableres tilgang mellom virksomhetene for de mest sentrale datasystemene som DIPS og DocuLive, vil dette medføre betydelige kostnader for virksomhetene.

Det fremgår av § 22 at det kun kan inngås avtale om direkte lesetilgang til helseopplysninger på tvers av virksomheter til hva som betegnes som "strukturerte helseopplysninger". Det kan reises tvil om hva som ligger i begrepet "strukturert". Begrepet "strukturert" bør derfor defineres i merknaden til paragrafen. Dersom man med "strukturert" mener kodede opplysninger, vil store deler av journalen ikke kunne leses fra annen virksomhet da pasientjournalen i dag i all hovedsak består av løpende fritekst. Etter vår vurdering tilfredsstiller dagens pasientjournal ikke de krav som stilles i forskriften hva gjelder strukturerte helseopplysninger.

Det kan kun gis tilgang til opplysninger som det *på forhånd* er vurdert kan deles. På et generelt grunnlag vil det påpekes at det er vanskelig å forutse hva som i fremtiden skal deles.

Det er i dag et ønske fra helsepersonell å se pasientjournalen mest mulig samlet, og således ha tilgjengelig mest mulig informasjon om pasienten som er til behandling. På Oslo universitets-sykehus innebærer dette blant annet at psykiatrijournalen er en del av foretakets samlede journal. Dette medfører at alle leger fra somatikk kan aktualisere og dermed få tilgang til psykiatrijournalen. I dag har vi ikke mulighet til å kunne sperre eksempelvis informasjon fra psykiatrijournalen for eksterne, dersom det åpnes opp for tilgang på tvers. Dette gjelder hovedjournalen i OUS. En slik ordning hvor psykiatrijournalen er en del av foretakets samlede journal, vil etter vår mening måtte revurderes, dersom det åpnes for tilgang på tvers uten at systemene understøtter en mer effektiv bruk av sperring. Dette vil kunne medføre negative følger for pasientbehandlingen som foretaket selv gir.

§ 24 Forutsetninger for å kunne inngå avtale om direkte tilgang til helseopplysninger på tvers av virksomheter
§ 24 stiller opp en rekke tekniske forutsetninger som må ligge til grunn før en avtale på tvers kan inngås. Begge virksomheter må ha tekniske løsninger som kan avgrense tilgangen til å omfatte strukturert og forhåndsvurdert klinisk informasjon til en navngitt person relatert til forespørselen. Det er i dag ikke mulig å begrense tilgangen til å gjelde kun en pasient i hovedjournalen som benyttes for OUS. Når det gjelder kravet som stilles til at tilgangen skal avgrenses til strukturert informasjon i journalen, vil det bemerkes at rundt 80 % av dagens pasientjournal består av ustrukturerte data. Denne prosentandelen øker for hvert år. Dersom kravene skal imøtekommes, kreves store endringer i de elektroniske pasientjournaler.

Det fremgår av § 24, 2. ledd at forutsetningen for å kunne inngå avtale om direkte tilgang på tvers er at informasjonssikkerheten ikke svekkes ved noen av virksomhetene. Løsningen som forskriften legger opp til innebærer at det etableres åpninger i brannmuren til virksomhetene, samt at journalsystemene kobles sammen. Når det i tillegg gis tilgang for flere behandlere enn i dag, er det vanskelig å se at informasjonssikkerheten ved noen av virksomhetene ikke vil bli svekket.

§ 25 Krav til autentisering
Det fremgår av § 25 at alle som gis tilgang til helseopplysninger i et behandlingsrettet helseregister skal autentiseres ved bruk av kvalifisert sertifikat.

Det fremstår som uklart hvorfor merknaden til forskriften § 3 definerer 2-faktor autentisering til tross for at kravet etter § 25 vil være kvalifisert sertifikat. Det er etter vår mening et behov for å styrke sertifisering for å sikre at riktig person har tilgang. Det bør likevel utredes nærmere hva som ligger i dette kravet. Etter vår mening er 2-nivå autentisering med kvalifiserte sertifikater en forutsetning før man kan gis tilgang til behandlingsrettet helseregister i annen virksomhet. I dag har vi ikke slike kvalifiserte sertifikater. Kostnaden med å få slike sertifikater tilgjengelig, samt implementering av løsningen ved tidligere Ullevål sykehus ble estimert til rundt 8-10 millioner kroner for 4-5 år siden.

I merknaden til § 25 åpnes det opp for å gi tilgang på tvers selv om en ved autentiseringen ikke har benyttet kvalifisert sertifikat. Forutsetningen er eksempelvis at to helsevirksomheter har felles database med logiske skiller mellom de ulike helseforetakene. Det vil etter vår mening være samme krav til autentisering, selv om opplysningene ligger på felles server. En slik tilgang vil uansett kreve personlig sertifikat for at krav om uendrede forhold til taushetsplikten skal opprettholdes, ref Stortingets forutsetning.

§ 26 Krav til forespørselen m.m.
Det fremgår av § 26 at en forespørsel om direkte tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismene i regi av egen virksomhet. Dersom man skal ha muligheten til i sitt eget grensesnitt til å få opp data fra den andre virksomheten, forutsetter dette samme journalsystem med strukturert informasjon. Når det gjelder retten til å forespørre informasjon, så kan det stilles spørsmål ved hvem som administrerer dette. Det forutsettes at en beslutning om å etterkomme et krav om tilgang må være automatisert.

Det er i dag ikke mulig å begrense spørringen til kun å gjelde en person i virksomheten. Nåværende journalsystem gir ikke tilgang til enkeltpasienter, men er bygget opp slik at geografi, tid og rolle er bestemmende for hva du teknisk kan få tilgang til. Vi har dermed ikke adressering av enkeltpasienter som tilgangskriterier, noe vi ikke er kjent med at noen andre journalsystem leverer.

Det forutsettes videre at oppslag i annet foretaks journal kun skal kunne gjøres på den pasienten som lege har slått opp på i eget foretak. Dette er langt fra dagens løsning, og det bør derfor utredes nærmere hvordan en slik løsning skal være mulig.

§ 29 Sperring av helseopplysninger
Det er i dag ikke mulig å gjøre opplysninger tilgjengelig bare etter samtykke. Den eneste muligheten for å begrense tilgang til deler av informasjonen i de elektroniske journalene, er ved bruk av sperring. Som beskrevet tidligere, er det ikke praktisk mulig å gjennomføre i stor skala i dagens systemer. En slik løsning som skisseres i forslag til forskriften med tilgjengeliggjøring av informasjonen først etter samtykke, har i dagens hovedløsning ikke teknisk understøttelse. Det vil dermed ikke være noen tekniske hindre som begrenser lesing før samtykke er gitt, og tilgjengeliggjøring ut fra dagens løsninger vil dermed kun baseres på tillit, og vil i liten eller ingen

grad kunne etterprøves hva gjelder faktisk innhenting av samtykke for innsyn. Forslaget som er ment å underbygge personvernet og taushetsplikten er dermed vanskelig gjennomførbart, særlig for de store virksomhetene.

§ 31 Krav om dokumentasjon av tilgang
§ 31 skiller mellom dokumentasjon av tilgang og hendelsesregistre. Etter vår mening vil det ene registeret ikke gi noe mer informasjon enn det andre, og vi mener således at det ikke er nødvendig å etablere egne hendelsesregistre som sådan.

Etter § 31, bokstav b skal dokumentasjonen inneholde opplysninger om "grunnlaget for tilgangen". Det kan reises tvil om hva som ligger i dette. Informasjonen kan lett bli veldig omfattende dersom man for all helsehjelp må begrunne behovet for tilgang. Dette er også ressurskrevende og vil enten kreve en endring i de aktuelle løsninger, eller en endring i dagens bruk, hvor det ikke oppgis årsak til oppslag om pasienten er innenfor egen geografi.

§ 32 Hendelsesregistre
Etter vår mening vil ikke hendelsesregisteret gi særlig mer informasjon enn hva som registreres i dag. Behovet for et hendelsesregister bør derfor utredes nærmere.

Det vises til at "stedet hvor vedkommende har vært pålogget fra" skal registreres i hendelsesregisteret. Det kan reises tvil om det her menes fra hvilken virksomhet vedkommende har logget seg på, fra hvilken pc eller lokasjon, eller fra hvilket system? Dette bør etter vår mening utdypes nærmere.

I Norm for informasjonssikkerhet for helsesektoren er det krav til å oppbevare logger i 3 mnd. Forskriften legger opp til at data skal lagres i 2 år. Dette setter store krav til lagringskapasitet, og man bør derfor utrede muligheter for å lagre kun deler av informasjonen. I tillegg kan det være vanskelig for en ansatt å huske detaljer vedrørende et oppslag så lenge som 2 år etter at hendelsen fant sted.

Det fremgår videre at hendelsesregistre skal kunne sammenstilles med lister over tilstedeværelse av personell. Dette er fra et personvernsynspunkt betenkelig. Videre finnes det oss bekjent ikke lister over faktisk tilstedeværelse, selv om informasjonen nok kan trekkes ut fra andre systemer og fremskaffes ved en del tilrettelegging. Det er også grunnlag for å stille spørsmål rundt hva dette vil gi av informasjon. I økende grad vil den enkelte kunne jobbe via mobilkontor, og således gjøre dokumentasjonsarbeid ferdig selv om man ikke fysisk er til stede.

§ 33 Oppfølging og kontroll av elektronisk tilgang
Databehandlingsansvarlig pålegges jevnlig gjennomgang av tilgangskontrollen. Det finnes i dag ikke tilfredsstillende elektroniske verktøy til å gjennomgå logger, og det vil være så ressurskrevende å skulle gjøre dette manuelt, at det ikke er praktisk gjennomførbart. De anstrengelser som hittil er gjort for å etablere logganalyseverktøy, har foreløpig ikke gitt de ønskede resultater. Dette fordi slike løsninger krever en detaljering av ulovlig adferd lagt inn i logganalyseverktøyene, og hvor det ikke er praktisk mulig å detaljere den ulovlige adferden spesifikt nok. Når vi ikke klarer å benytte eksisterende logger ved oppslag innen foretaket, hjelper det ikke på noe at vi får enda flere logger. Vi har ingen god metode til å oppdage sniklesing/taushetspliktsbrudd. Her mener vi at mønstergjenkjenning vil kunne være riktig verktøy å benytte. Mønstergjenkjenning går i hovedsak ut på at verktøyet selv kan identifisere ulovlig adferd basert på at slik aktivitet avviker fra hva som er normalaktivitet. Mønstergjenkjenning som verktøy benytter et sett med matematiske analyser for å identifisere dette.

§ 34 Innsynsrett i logg og annen dokumentasjon av tilgang
For å gjøre tilgangsloggen forståelig for den registrerte, har man etter § 34 mulighet til å sammenstille tilgangsloggen med virksomhetens autorisasjonsregister. Etter vår mening vil en slik sammenstilling ikke gi svar på om tilgangen har vært urettmessig.

Med vennlig hilsen
Oslo universitetssykehus HF

Erik Carlsen, Fagdirektør
Medisin og helsefag
Oslo universitetssykehus

Heidi Thorstensen
KT-sikkerhetssjef/personvernombud
Oslo universitetssykehus