

Fornyings- og administrasjonsdepartementet

E-post: postmottak@fad.dep.no

Deres ref.
200900158

Deres dato
17.02.2009

Vår ref.
140/09 ToNy

Vår dato
20.08.2009

Høringsuttalelse - NOU 2009:1 Integritet og individ

Vi har med interesse lest *NOU 2009:1 Integritet og individ* og mener Personvernkommisjonen har levert en grundig og god utredning som det er viktig blir fulgt opp.

Som kompetansesenter for IT i helse- og sosialsektoren, har vi funnet det naturlig å kun kommentere utredningens kapittel 16, *Personvern i helsesektoren*. Vi mener kommisjonens situasjonsbeskrivelse er god og at de problemstillinger de tar opp er viktige. Vi støtter også i all hovedsak kommisjonens anbefalinger og forslag til tiltak.

Vi vil likevel benytte anledningen til å kommentere enkelte punkter i utredningen.

Til 16.4.3 Helsepersonells og andre yrkesgruppers taushetsplikt

Til 16.4.3.4 Uautorisert tilgang til taushetsbelagte helseopplysninger

Kommisjonen drøfter her problemet med uautorisert tilgang til helseopplysninger. Vi er enige med kommisjonen i at innføringen av elektronisk pasientjournal (EPJ) har gitt helt nye muligheter for de som ønsker å tilegne seg helseopplysninger urettmessig. Men om dette har ført til flere eller alvorligere tilfeller av misbruk, er vi derimot mer usikre på.

EPJ-systemene er langt fra ideelle, men de gir en helt annen mulighet til å differensiere tilgangen enn ved bruk av papirjournaler. Videre, mens den som snoker i papirjournaler ikke etterlater seg noe spor, blir all tilgang til EPJ logget, noe vi mener har en betydelig preventiv effekt. Selv om kontroll av slike logger er såpass ressurskrevende at muligheten for å avsløre snokere ved stikkontroll er begrenset, vil en ut fra loggen kunne få en mistanke om uautorisert tilgang bekreftet eller avkreftet.

Datatilsynet har som nevnt i utredningens kapittel 16.5.1, ved tilsynsbesøk hos flere helseforetak og andre virksomheter i helsesektoren, påvist vesentlige mangler med måten tilgang til opplysninger i EPJ blir håndtert på. En viktig del av denne kritikken er at svært mange er gitt autorisasjon som muliggjør tilgang til et meget stort antall pasientjournaler uten at "noen" på forhånd foretar en eksplisitt vurdering av nødvendigheten av tilgang i det konkrete tilfellet. Selv om dette nok på mange måter er en korrekt beskrivelse av de faktiske forhold, så betyr ikke dette journalene er fritt tilgjengelige for de aktuelle brukerne. Tilgang gis automatisk dersom det er etablert en relasjon mellom brukeren av EPJ-systemet og den aktuelle pasienten. Dersom en slik relasjon ikke er etablert, må brukeren eksplisitt angi en begrunnelse før tilgang gis. Denne selvbetjeningsmuligheten skal selvsagt kun benyttes når det foreligger et tjenestelig behov, og begrunnelsen for tilgangen registreres i en særskilt logg som

rutinemessig kontrolleres. KITH er imidlertid enig med Datatilsynet i at det kan synes som om for mange er tildelt en for vid mulighet for selvbetjening.

Det kan være nærliggende å tro at muligheten til å gi seg selv tilgang til en pasients journal ville resultere i et betydelig misbruk. Men så synes ikke å være tilfelle, antall tilfeller av snoking som er avslørt er i hvert fall lavt sett i forhold til antall ansatte i helsesektoren.

Ut fra det vi kjenner til, så foreligger det heller ikke forskningsresultater som tilsier at innføring av elektronisk pasientjournal har ført til flere brudd på taushetsplikten. Tvert imot så konkluderer en australsk undersøkelse¹ med at så ikke er tilfelle. Inntil det eventuelt blir gjennomført ny forskning i Norge eller andre sammenlignbare land som kommer til en annen konklusjon, mener vi at det ikke er grunnlag for å påstå at innføringen av EPJ samlet sett har ført til økt uautorisert tilgang til taushetsbelagte helseopplysninger.

Til 16.4.3.5 De mange unntakene fra taushetsplikten

Kommisjonen peker her på et vesentlig problem. Unntakene fra taushetsplikten har etter hvert blitt påtakelig mange, og det kommer stadig forslag om flere. Forslag til et meget omfattende unntak var inkludert i høringsnotatet vedrørende etablering av et nasjonalt register over hjerte- og karlidelser. Her heter det i forslag til ny helsepersonelloven § 29 b:

Departementet kan bestemme at helseopplysninger kan eller skal gis til bruk til kvalitetssikring, administrasjon, planlegging eller styring av helsetjenesten, og at det skal skje uten hensyn til taushetsplikt. [...]

Dette forslaget vil, dersom det blir vedtatt, frata pasientene enhver mulighet for innflytelse når det gjelder bruk av personidentifiserbare opplysninger til dette svært brede spektret av formål. Fra før finnes som kommisjonen påpeker, en rekke andre slike unntak. Det er på mange måter et paradoks at opplysninger som pasienten motsetter seg at helsepersonell skal få tilgang til, selv om opplysningene er relevante i behandlingssammenheng, "fritt" skal kunne benyttes i en rekke andre sammenhenger uten at pasienten gis noen rett til å hindre slik bruk.

Når det gjelder flere av bestemmelsene om unntak fra taushetsplikten, så kan det synes som om de er utformet av rene bekvemmelighetshensyn. I stedet for å utforme konkrete bestemmelser som ivaretar konkrete og veldokumenterte behov hvor hensynet til andre personer eller viktige samfunnsinteresser må gå foran personvernet, har en valgt å utforme svært generelle bestemmelser som åpner for det meste.

Til 16.5 Personvernkommisjonens observasjoner

Til 16.5.1.3 Journaltilgang på tvers av virksomheter

Når det gjelder tilgang til helseopplysninger, så mener KITH at virksomhetsgrensene i seg selv ikke bør være av avgjørende betydning for hvem som kan få tilgang til originalopplysninger i EPJ, og hvem som kun kan få utlevert kopi av opplysningene.

Det sentrale bør etter vår mening ikke være hvor den som får tilgang til helseopplysninger er ansatt, men i hvilken grad opplysningene er relevante i forhold til den helsehjelp som skal ytes. Under forutsetning av at det foreligger et dokumentert tjenestelig behov og at pasienten ikke har motsatt seg seg att opplysningene gis, bør enhver metode kunne benyttes for å gi tilgang

¹ Mulligan E, Braunack-Mayer A. Why protect confidentiality in health records? A review of research evidence. Australian Health Review 2004; 28:48-55

til opplysningene, da selvsagt under den absolutte forutsetning av at informasjonssikkerheten kan ivaretas på en betryggende måte.

Vi mener derfor at den endring i helseregisterloven § 13 som åpner for en kontrollert og begrenset tilgang til EPJ, og som Stortinget nå har vedtatt, er til beste for pasientene og at den ikke innebærer noen svekkelse av personvernet.

Selv om utviklingen av EPJ-systemer på langt nær er kommet så langt at det vil være teknisk mulig å åpne for tilgang mellom EPJ-systemer fra forskjellige leverandører, er denne lovendringen og de bebudede forskriftene en forutsetning for nødvendig videreutvikling av systemene. For leverandørene er det klart enklere å utvikle gode mekanismer for tilgangsstyring i EPJ-systemer dersom det foreligger et klart regelverk og gjerne også standarder som støtter opp under dette regelverket.

Et uklart regelverk er etter vår mening en sterkt medvirkende årsak til en del av de uheldige forhold som Datatilsynet har påpekt i sine rapporter fra tilsynsbesøk. Det store tolkningsrommet for en del sentrale bestemmelser i helsepersonelloven og helseregisterloven har gitt virksomhetene i helsevesenet mulighet til å tolke bestemmelsene på en måte som ikke har hemmet effektiviteten og som heller ikke har hatt større kostnadmessige konsekvenser. Og deres leverandører har naturlig nok utviklet EPJ-systemene i tråd med disse tolkningene.

På den annen side kom det daværende Sosial- og helsedirektoratet årsskiftet 2006/2007 med et rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler (IS-7/2006), hvor tolkningen på et par sentrale punkter var så forskjellige fra den etablerte praksis at det knapt var tenkbart at tolkningen kunne bli etterlevd.

Etter vår mening er det betydelig fare for at respekten for regelverket blir svekket dersom sentrale bestemmelser oppleves som umulig å etterleve uten å komme i alvorlig konflikt med forsvarlighetskravet og/eller Stortingets krav til effektiv drift. Dette er på ingen måte bra i forhold til personvernet, dersom en virksomhet føler seg tvunget til rutinemessig å bryte enkelte bestemmelser, kan en fort ta lett på andre også.

Vi mener derfor at det løp Helse- og omsorgsdepartementet har lagt opp til når det gjelder journaltilgang på tvers av virksomheter, er fornuftig. Det gir håp om at en innen rimelig tid kan få på plass et tilstrekkelig konkret regelverk som leverandørene kan ta hensyn til ved utvikling av ny funksjonalitet i EPJ-systemene, og som det kan være mulig å etterleve for virksomhetene i helsevesenet.

Vi mener også at det arbeid Helse- og omsorgsdepartementet har satt i gang for å utarbeide mer detaljerte forskrifter vedrørende informasjonssikkerhet og tilgang til opplysninger i behandlingsrettede helseregistre, er meget viktig. Det er etter vår mening godt håp om at en her kan komme fram til bestemmelser som vil styrke personvernet samtidig som helsepersonells behov for tilgang til relevante opplysninger fra EPJ, blir ivaretatt.

Til 16.5.6 Registre og de mange formål

KITH mener det er riktig og viktig at opplysninger som blir registrert i forbindelse med behandling av pasienter, kan gjøres tilgjengelig for forskere. Vi har derfor i hovedsak vært positive til forslag om opprettelse av nye slike registre, men har i de fleste tilfeller hatt kritiske merknader til valget av registerform og de personvernmessige vurderinger som er gjort.

Stortingets sosialkomité uttalte i Odelstingsinnstilling nr.62 (2000-2001) at dersom det er konflikt mellom personvernet til den enkelte pasient og andre interesser, skal det svært tungtveiende argumenter til for at personvernet til enkeltindividet skal vike. KITH støtter dette fullt ut og mener at dersom et register ikke skal baseres på samtykke eller i det minste

reservasjonsrett for den enkelte, så bør registret være pseudonymt. Kun i helt spesielle tilfeller hvor viktige samfunnsinteresser gjør det påkrevd, bør det tillates opprettet helseregistre med personidentifiserbare opplysninger uten krav om innhenting av samtykke.

Til 16.5.6.2 Norsk pasientregister

Norsk pasientregister (NPR) hadde eksistert som et aidentifisert register siden 1997 da det i 2004 kom forslag om å gjøre registret personentydig. KITH støttet dette forslaget ettersom vi var (og er) enige i at NPRs opprinnelige formål ikke kan oppfylles på en fullgod måte når opplysningene er aidentifiserte. Men vi fant ikke at formålet krevde at opplysningene måtte være personidentifiserbare, vi mente og mener fremdeles at behovene vil kunne dekkes med pseudonyme opplysninger.

Personvernkommissjonen har etter vår mening et godt poeng når de på side 179 sier følgende:

"Den tilbakeholdenheten som kan spores hos politikere og enkelte forskningsmiljøer når det gjelder pseudonymisering, kan tyde på problemer med å forstå hva pseudonymisering innebærer og forståelse for at de fleste formål med registrene kan realiseres på tross av tiltaket."

Her kan vi for egen regning tilføye at mange synes å legge til grunn at det knapt har skjedd noen utvikling fra papirjournalene sin tid og at rapportering til registrene må baseres på ustrukturerte opplysninger av dårlig kvalitet. Selv om det nok er et stykke igjen før de ideelle løsninger er på plass, finner vi grunn til å påpeke at alle helseforetak og de aller fleste allmennleger benytter elektronisk pasientjournal (EPJ). Vi mener derfor at det både ut fra kvalitetsmessige og personvernmessige betraktninger vil være mest hensiktsmessig å etablere løsninger for registrering, kvalitetssikring og innrapportering på pseudonym form av de ønskede opplysninger i tilknytning til EPJ-systemene.

I tilfellet NPR ble det i høringsnotatet foreslått en utvidelse av registrets formål som trolig var sterkt medvirkende til at Stortinget til slutt vedtok å etablere NPR som et helseregister med personidentifiserbare opplysninger. I følge formålet skal NPR også danne grunnlag for etablering og kvalitetssikring av sykdoms- og kvalitetsregistre. Et register som skal kunne danne grunnlag for etablering av registre som inneholder personidentifiserbare opplysninger, kan naturlig nok ikke være pseudonymt. Det utvidede formålet til NPR kan derfor ikke oppfylles fullt ut av et pseudonymt register.

Mens det opprinnelige formålet for NPR (statistikk, innsatsstyrt finansiering mv) gjorde at registret måtte være komplett og dermed ikke basert på samtykke, medførte det utvidede formålet at registret måtte inneholde personidentifiserbare opplysninger.

KITH mener denne sammenblandingen av formål var uheldig og resulterte i at verken pseudonymisering, samtykke eller reservasjonsrett kunne benyttes som personvern fremmende tiltak for NPR. KITH mener videre at en i framtiden bør legge større vekt på utredningen av hvilke konsekvenser de enkelte elementene i det formål som foreslås for et nytt register, vil kunne få for personvernet.

Helt til slutt i dette kapitlet uttaler kommisjonen:

"Personvernkommissjonen erkjenner at pseudonymisering er kostbart, både i forhold til etablering, vedlikehold og bruk. Dette bør imidlertid ikke være til hinder for at pseudonymisering blir vurdert som et reelt alternativ ved etablering av helseregistre."

KITH er enig i at pseudonymisering medfører merkostnader, men er mer usikre når det gjelder størrelsen av disse. Pseudonymisering krever at det etableres en infrastruktur for pseudonymisering, inkludert en Tiltrodd PseudonymForvalter (TPF), men når denne er på

plass kan den benyttes av alle registre. Prosessene i tilknytning til pseudonymisering kan i stor grad automatiseres og det kan også etableres felles tekniske løsninger som kan benyttes ved innrapportering mv.

Manglende kunnskap om hva etablering av et pseudonymt helseregister faktisk medfører av kostnader både i etablerings- og driftsfasen, kan være en medvirkende årsak til at denne registerformen sjeldent blir valgt. KITH mener derfor det bør foretas en utredning med sikte på å komme fram til hvilke kostnader som vil være forbundet med etablering av en nasjonal infrastruktur for pseudonymisering. Videre bør det utredes hvilke ekstra kostnader som må påregnes for hvert register som skal etableres pseudonymt, i stedet for personidentifiserbart eller med intern kryptering.

Til 16.6 Kommisjonens anbefalinger og forslag til tiltak

KITH støtter kommisjonens anbefalinger og forslag til tiltak, og har kun en del utdypende kommentarene til enkelte av disse.

Til 16.6.2 Utelatelse av individualiserende kjennetegn

KITH støtter forslaget om å utvide EPJ-standarden med krav som gir mulighet for å skjule pasientens identitet og andre individualiserende kjennetegn i de situasjoner hvor disse ikke er nødvendige.

Videre bør det tas inn krav som beskriver hvordan rapportering til og samhandling med pseudonyme helseregistre skal skje. Disse kravene bør bl.a. dekke korrigerende av rapporterte opplysninger og andre kvalitetsfremmende tiltak, mulighet for pasientinnsyn i registret og mulighet for tilbakemelding til avgiver (sykehus, fastlege e.l.) dersom det på grunnlag av opplysninger om en pasient avdekkes forhold av helsemessig betydning for pasienten.

Til 16.6.3 System for identitetsadministrasjon

KITH er enig i at arbeidet med å få på plass gode systemer for identitetsadministrasjon innen helsesektoren bør ha høy prioritet. Vi tror imidlertid at dette bør være et todelt system slik at all håndtering av pseudonymer blir lagt til en Tiltrodd PseudonymForvalter (TPF) som bør være helt uavhengig av den enhet som tillegges ansvaret for den øvrige identitetsadministrasjonen.

Vi vil her også påpeke at dersom et og samme pseudonym benyttes til mange formål, så kan det lede til at pseudonymet i seg selv nærmest blir en personidentifikator. Den som har tilgang til flere registre mv. hvor samme pseudonym benyttes, vil selv kunne foreta koblinger som kan gjøre det mulig å identifisere enkelte av de registrerte. Vi mener derfor at pseudonymer bør opprettes for et bestemt formål, f.eks. bruk i IPLOS, og ikke være tilgjengelig i andre sammenhenger. Det bør benyttes en felles TPF for all pseudonymisering og denne vil også kunne forestå kobling mellom uttrekk av opplysninger fra registre som benytter forskjellig pseudonym.

Til 16.6.4 Personvernvennlig bruk av elektronisk pasientjournal (EPJ)

Som nevnt i våre kommentarer til kapittel 16.5.1.3 ovenfor, mener vi at et uklart regelverk som gir et for stort rom for tolkninger, er en sterkt medvirkende årsak til problemene på dette området. De bebudede detaljerte forskrifter vedrørende informasjonssikkerhet og tilgang til opplysninger i behandlingsrettede helseregistre må kunne forventes å bringe nødvendig avklaring på mange områder og det er all grunn til å tro at forskriftene raskt vil bli fulgt opp med nødvendig ny funksjonalitet i EPJ-systemene.

Vi håper at disse forskriftene skal komme med nødvendige avklaringer på flest mulig av de områder relatert til tilgang til EPJ hvor gjeldende regelverk leder til misforståelser og/eller uenighet mellom tilsynsmyndighetene og virksomhetene i helsesektoren. Dette innebærer at det varslede nye høringsutkast til forskrifter bør bli noe mer omfattende enn det første.

Av de forhold vi mener bør tas med, er en konkretisering av den enkeltes rett til å sperre enkeltopplysninger i egen journal som en selv anser som spesielt følsomme. Slik sperring bør kunne differensieres slik at den enkelte selv kan bestemme i hvilke situasjoner det kan gis tilgang til bestemte opplysninger, hvilke personellgrupper som kan få tilgang til opplysningene, om de kan utleveres til forskningsformål, etc.

Videre mener vi det er svært viktig at de nye forskriftene gjør det klart hva som kreves for at den potensielle rett til tilgang til EPJ som følger av den enkelte tjenesteuyters autorisasjon, skal utløses. I følge rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler (IS-7/2006) fra det daværende Sosial- og helsedirektoratet kreves det at "noen", fortrinnsvis avdelingsleder eller journalansvarlig på et sykehus, skal foreta en eksplisitt, detaljert vurdering av hvilke opplysninger i en pasients journal f.eks. en lege skal få tilgang til i forbindelse med behandling av en pasient. Selv om dette nok kan være en grei prosedyre for å behandle eksterne forespørsler om journalopplysninger, er det nærmest praktisk umulig å gjennomføre en slik eksplisitt vurdering og manuell utvelgelse av hvilke opplysninger hvert enkelt helsepersonell som deltar i behandlingen av en pasient, skal få tilgang til. Vi kjenner da heller ikke til noen sykehus som følger prinsippene fra nevnte rundskriv når det gjelder intern tilgang til EPJ.

Vi mener en mulighet for sperring kombinert med en regelstyrt tilgang basert på roller og normalbehov for opplysninger ved gjennomføring av bestemte typer tiltak, og som utløses av de helsehjelprelaterte beslutninger som registreres i EPJ, vil være en personvernmessig bedre løsning enn å kreve at "noen" må foreta en eksplisitt vurdering av behov i hvert enkelt tilfelle.

Til 16.6.6 Forbedring av pasienters rett til innsyn i journallogg

Stortinget har nå foretatt en lovfesting av pasientens rett til innsyn i journallogg. Slike logger er imidlertid ofte så omfattende og uoversiktlige at det vil være vanskelig for pasienter flest å forholde seg til disse. Det er derfor viktig at det foretas nødvendig tilrettelegging bl.a. med nødvendig funksjonalitet i EPJ-systemene slik at rettigheten kan ivaretas på en god måte. Vi mener derfor at det med fordel kan inkluderes noe mer detaljerte bestemmelser på dette området i de tidligere nevnte bebudede forskriftene.

Kontaktperson i denne saken er sjeffrådgiver Torbjørn Nystadnes, tlf. 73 59 86 10, e-post: tony@kith.no.

Med vennlig hilsen

Tom Christensen
Adm. dir.

Torbjørn Nystadnes
Sjeffrådgiver