NTNU
Det medisinske fakultet

Vår dato 03.09.2010
Vår referanse 2010/6562/TMF
Deres dato 10.05.2010
Deres referanse

Helse- og omsorgsdepartementet

Postboks 8011 Dep.
0030 Oslo

Informasjonssikkerhet helseregistre - Høringssvar

Vi viser til utsendt høringsbrev av 10. mai 2010 med vedlagt utkast til forskrift om informasjonssikkerhet med mer for behandlingsrettede helseregistre. Det medisinske fakultet (DMF) og Norsk senter for elektronisk pasientjournal (NSEP) ved NTNU er begge oppført som høringsinstanser. Fagmiljøet ved NSEP har utarbeidet et høringssvar og dette dokumentet er forankret i instituttledermøtet ved DMF 31.08.10.

Følgende felles uttalelse kommer fra NSEP og DMF ved NTNU:

Vi vil først få rose departementet for å ta tatt tak i et så viktig, men også vanskelig tema. Området informasjonssikkerhet er utsatt for en rivende teknologisk utvikling med raske forandringer. I vår uttalelse har vi både noen generelle betraktninger og konkrete kommentarer til noen av de foreslåtte paragrafene.

Generell tilbakemelding på høringsnotatet

Forskning som er utført ved NSEP viser tydelig at EPJ-systemets viktigst funksjon er å være et arbeidsredskap for helsepersonell. Vi vil derfor peke på at bruken av begrepet forsvarlighet i lov om spesialisthelsetjenestens § 3-2 ikke bare handler om forsvarlighet fra et informasjonssikkerhets-perspektiv slik utkastets §4 kan gi inntrykk av, men også handler om at journalsystemene skal være forsvarlige som arbeidsredskaper for helsepersonell.

DMF vil anføre at de som er ansvarlige for utviklingen av et informasjonssikkerhetsregelverk også burde legge empirisk basert kunnskap om hvordan helsepersonell faktisk bruker helseopplysninger til grunn for sitt arbeide med å utvikle regelverket. Forskning som er utført ved NSEP viser at helsepersonell ofte havner i dilemmaer der de må velge mellom hvilke regelverk de skal følge som i praktisk sammenheng blir stående mot hverandre. Krav til timelighet, kvalitet og effektivitet i helsetjenesteytelsen kan gå på bekostning av krav til dokumentasjon av helsehjelpen og til ivaretakelse av informasjonssikkerheten.

Forskning vi har utført viser f.eks. at alt de rigorøse autoriserings- og autentiseringssystemer som nå er i bruk fører til identitetslån og identitetsdeling i et betydelig omfang. Videre at komplisert tilgang

Postadresse
7489 Trondheim

Org.nr. 974 767 880
E-post:
dmf-post@medisin.ntnu.no
http://www.ntnu.no

Besøksadresse
Medisinsk teknisk forskningssenter, Olav Kyrres gt 9Olav Kyrres gate 9

Telefon
+47 73 59 88 59
Telefaks
+47 73 59 88 65

Saksbehandler
Tone Merete Follum
Tlf: +47 73 59 01 50

til journalsystemene fører til forsinkelser i dokumentasjonen av helsehjelp og undersøkelsesresultater fordi helsepersonell samler opp og venter med å dokumentere for at ikke for mye tid skal gå med til pålogging i daglig travelt klinisk arbeid. Forskningsresultatene vil bli publisert senere denne høsten.

DMF mener at de som har ansvaret for informasjonssikkerheten i de enkelte helseforetak bør ha ansvar for at det etableres lærende arenaer rundt helsepersonells faktiske bruk av helseopplysninger ved egen institusjon. NSEP har erfaring med at systemene for melding av avvik, rutinene rundt behandling av avvik, samt gjennomgang og revisjon av institusjonens rutiner fungerer dårlig. Forvaltningen bør ta initiativ til at det utvikles veiledere som gjør det enklere å etterleve regelverket på dette området.

Det finnes i dag et behov for mer forskning på helsepersonells bruk av informasjonssystemer i skjæringsflaten mellom informasjonssikkerhet (etterlevelse av normer for sikring av opplysninger om pasienten) og pasientsikkerhet (etterlevelse av normer for sikring av pasienten som biologisk system). DMF vil oppfordre til at forvaltningen tar initiativ til et forskningsprogram som skal utvikle ny kunnskap på dette området. Et slikt forskningsprogram kunne også omfatte utvikling og utprøving av nye og mer effektive teknologier for autorisering og autentisering av helsepersonell. Dagens tilgangskontroll og regelverk, inklusive høringsutkastet, bærer preg av å være bedre tilpasset merkantilt stillesittende arbeid med enkeltoppgaver, enn arbeidet i store deler av helsetjenesten som foregår i team, med flere parallelle oppgaver og med mye bevegelse. Forskningsaktivitet på dette feltet vil ha stor nytteverdi for forvaltning, sektoren og EPJ-systemleverandører. Vi mener det her også foreligger et stort potensial for effektivitetsgevinster og kostnadsbesparelser.

Spesifikk tilbakemelding på høringsnotatet

Om opplæring og utdanning av helsepersonell

Som utdanningsinstitusjon er DMF opptatt av å legge til rette for læring også etter at helsepersonell er ferdige med sin grunnutdanning. Lov om helsepersonell slår fast at *"helsepersonell skal utføre sitt arbeid i samsvar med de krav til faglig forsvarlighet og omsorgsfull hjelp som kan forventes ut fra helsepersonellets kvalifikasjoner, arbeidets karakter og situasjonen for øvrig"* (Helsepersonelloven § 4). I spesialisthelsetjenesteloven § 3.8 er opplæring av helsepersonell en av de fire hovedoppgavene som helseforetakene har. Tilsvarende er kommunene pliktig til medvirkning i undervisning og opplæring i følge kommunehelsetjenesteloven § 6.1

DMF mener at bruk av pasientinformasjon i samband med utdanning og opplæring av helsepersonell ikke er blitt gitt tilstrekkelig plass i utkastet til forskrift. Autorisasjon og tilgang til pasientinformasjon er snevert knyttet til en direkte og aktiv behandlingssituasjon – jf § 14 og § 19 i høringsutkastet. I mange sammenhenger er helsepersonell under opplæring observatører og utfører ikke oppgaver direkte overfor pasienter slik for eksempel § 19 siste ledd krever overfor studenter.

Plikt til forsvarlighet innbærer en plikt til å øve inn og deretter opprettholde en god kvalitet på de helsefaglige funksjoner som man blir satt til å utøve. Forskning viser at dokumenter som kan gi opplysninger om utkomme av egne helsehjelphandlinger er en viktig kilde til læring hos helsepersonell. I tråd med dette viser allmenmedisinsk forskning at epikrisene betyr mye for både vedlikehold og tilegnelse av nye kunnskaper for allmennlegene. Dette aspektet ved en institusjon sitt dokumentasjonssystem er ikke godt nok ivaretatt i forslaget.

Forslaget til forskrift vil etter DMFs mening svekke dokumentasjonssystemenes funksjon som verktøy for helsepersonells læring. For eksempel vil en sykehuslege under utdanning på medisinsk avdeling ikke ha lov å lese om, og derved lære noe av sykehushistorien til en pasient som han gav Marevan til for en uke siden og som etterpå ble innlagt på kirurgisk avdeling med spørsmål om blødning. Forskning på området gir grunn til å tro at kvaliteten på den hjelpen som helsepersonell yter er fullstendig av hengig av slike "mikrolæringssituasjoner". Vi mener at det å forby helsepersonell å bruke dokumentasjonssystemene til dette formålet vil ha negative konsekvenser, og at dette aspektet ikke er tilstrekkelig belyst og vurdert i høringsnotatet.

Et annet utdanningsrelatert aspekt er veilederens viktige rolle. En mye brukt metode i veiledning er å inspisere den dokumentasjon som den veiledede produserer når han yter helsehjelp. Det er mulig vi har tolket regelverket feil, men kan det virkelig stemme at en overlege som er tilsatt ved hematologisk avdeling og som veileder en turnuskandidat ikke kan inspisere en innkomstjournal som turnuslegen har skrevet i mottakelsen med mindre pasienten tilfeldigvis havner på den avdelingen overlegen er tilsatt? DMF mener at en svært viktig funksjon ved dokumentasjonssystemene er å være verktøy for læring for helsepersonell. Også på dette området er det behov for mere forskning og utprøvning av ny teknologi.

Logging og dokumentasjon av tilgang

Logging og dokumentasjon av tilgang er omtalt i høringsnotatet punkt 4.9, side 34 til 37 og i utkastet til forskrift under § 33 og § 34. Det blir fremhevet som et viktig tiltak ”for å avdekke uautorisert tilgang til opplysninger i behandlingsrettede helseregistre, eller forsøk på slik tilgang”. Databehandlingsansvarlig blir derfor pålagt jevnlig gjennomgang av tilgangskontrollen. Det sies videre at ”dersom en slik kontroll utløser mistanke om at det har skjedd urettmessig tilgang, skulle virksomhetens ledelse varsles”, som evt. informerer Datatilsynet.

Manuell gjennomgang av loggene og sammenstilling med autorisasjons- eller tilstederegistre blir sett på som en uoverkommelig oppgave pga. av et enormt volum. Man ser for seg at det vil bli utviklet programvare som automatisk kan screene logger for uregelmessigheter. Dette er det gjort forsøk på uten at man så langt har greid å lage tilfredsstillende løsninger. Fagmiljøet ved NSEP stiller seg tvilende til om slike løsninger faktisk er mulig. En slik tilnærming vil dessuten kunne gjøre mer skade enn til gagn for både pasienter og helsepersonell.

En gjennomgang av logger/hendelsesregistre (manuell eller automatisk) må baseres på kriterier for utvelgelse av hendelser som kan representere urettmessig tilegnelse av taushetsbelagte opplysninger. Vi vet imidlertid at det foreligger stor variasjon i behovet antall og typer helsepersonell som involveres i pasientbehandling, hvor lenge de bør ha tilgang og rimelig antall påloggінger i forhold til oppgavene. I tillegg kommer variasjon i individuelle forhold både hos pasienten (for eksempel alvorlighetsgrad og komplikasjoner), og helsepersonell (hvordan de velger å gjennomføre oppgavene) og tilleggsbehov knyttet til undervisning og kvalitetssikringsrutiner. Dette medfører at man må operere med kriterier som er grenseverdier for hva som skal være tillatt før det reageres. Settes det vide grenseverdier vil en del potensielle uregelmessigheter ikke bli fanget opp (lav sensitivitet og mange falsk negative). Blir grenseverdiene for stramme vil en del helt legitim bruk av pasientjournalen bli varslet (lav spesifisitet og mange falsk positive).

Falsk positive og falsk negative inntreffer også pga. feil enten ved forbytting av pasienter og helsepersonell eller feil føring i registrene, samt av tekniske feil i programvare eller ved integrasjon av disse og informasjonssystemene. Det siste kan være vanskelig å oppspore og inntreffe bare i blant.

Tabell 1. Omfanget av potensielt falsk positive ved regelmessig kontroll av logger/hendelsesregistre for overvåkning av urettmessig tilegnelse av taushetsbelagte opplysninger i et middels stort sykehus med om lag 30 000 innleggelser per år avhengig av virkelig forekomst (kolonne til venstre) og kontrollens sensitivitet og spesifisitet.

Antall innleggelser per år		30000							
Sensivitet		90	%		90	%		90	%
Spesifisitet		95	%		99	%		99,9	%
Antall ulovlig oppslag i journal per 1000 innleggelser	Ekte positive per år	Antall falsk positive per år	% falsk positive av alle positive	Ekte positive per år	Antall falsk positive per år	% falsk positive av alle positive	Ekte positive per år	Antall falsk positive per år	% falsk positive av alle positive
1	27	1499	98,2	27	300	91,7	27	30	52,6
5	135	1493	91,7	135	299	68,9	135	30	18,1
10	270	1485	84,6	270	297	52,4	270	30	9,9
50	1350	1425	51,4	1350	285	17,4	1350	28	2,1
100	2700	1350	33,3	2700	270	9,1	2700	27	1,0
500	13500	750	5,3	13500	150	1,1	13500	15	0,1

Det er et inverst forhold mellom sensitivitet og spesifisitet. Ønsker man et system som fanger de fleste uregelmessighetene (høy sensitivitet), blir det mange falske positive (lav spesifisitet), og vice versa. Høy sensitivitet ønsker man for å være sikre på å kunne fange de alvorligste tilfellene, virke effektivt preventivt og at ulovligheter skal bli behandlet likt. Det som erfaringsmessig er vanskeligst er derimot å oppnå høy spesifisitet når det er kompliserte og mange forhold som kan spille inn.

Hvordan dette vil kunne virke er lett å beregne. I tabell 1 har vi satt opp noen eksempler for et middels stort sykehus der vi horisontalt oppgir ulike kombinasjoner av sensitivitet og spesifisitet og hvor man under kan lese av hvor mange falske positive det gir avhengig av hvor ofte urettmessig tilegnelse av taushetsbelagte opplysninger forekommer (kolonne til venstre). Vi vet ikke nøyaktig hvor ofte dette skjer, men om man mangedobler det som blir rapportert av pasienter i intervjuundersøkelser ligger det likevel godt under 100 per 1000 innleggelser. Vi har i tabellen eksempler med en spesifisitet som er 95 % eller høyere. Vi tror det kan bli vanskelig å få til endog en så høy spesifisitet som 95 % ved overvåkning av logger knyttet til EPJ i sykehus. Ved 95 % spesifisitet er andelen falsk positive så høy at kontrollen blir meningsløs. Først med kontroller som kan oppvise en spesifisitet på 99 % vil andelen ekte positive bli høyere enn andelen falske hvis den reelle forekomsten av urettmessige oppslag er over 50 per 1000 innleggelser.

Hensikten med regelmessig overvåkning av hendelsesregistre er at det skal virke preventivt og øke tilliten hos pasienter ved at uregelmessig tilgang til pasientjournaler blir nøye overvåket. Hvis sykehus får flere hundre saker som må etterforskes, kanskje over 1000 i året, så mener vi at effekten kan bli den motsatte, alternativt at pasientene mister tilliten til systemet og regelverket når nesten alle saker eventuelt ”blir henlagt”. Vi ser for oss at et så lite effektivt system også kan få en alvorlig ødeleggende effekt på helsepersonellet som arbeider ved sykehusene og blir hyppig urettmessig mistenkt.

Tallene for falsk positive/falsk negative kan bli noe annerledes hvis det blir pasienten som selv regelmessig undersøker hendelsesregistre fordi de sitter med annen informasjon i tillegg, men problematikken er den samme. Faren for at det i hovedsak blir falsk positive er stor, og det bør

undersøkes før ideen forskriftfestes. Vi vet av erfaring at pasienter blir skadelidende og at det skaper uro omkring dem når oppstår mistanke om uregelmessig tilgang til opplysninger, og at dette nødvendigvis ikke går over om de får tilbakemelding om at det var uriktig. Vi mener derfor at man må alvorlig overveie om pasientene skal få tilgang til hendelsesregistre før det er dokumentert at registrene har en kvalitet hvor hovedandelen av oppdagelsene av uregelmessigheter som pasientene gjør, er ekte positive. Man bør vurdere det som et krav i forskriften på linje med hvilke opplysninger som skal være med. Dette handler om å ivareta pasientsikkerhet.

Vi mener ikke med dette at det ikke skal opprettes hendelsesregistre. De vil kunne være et viktig hjelpemiddel når det blir fremmet påstander om uregelmessig tilgang til opplysninger og dette må etterforskes. Dette kan man faktisk også indirekte lese av tabell 1. I saker hvor pasienter hevder at helsepersonell har tilegnet seg opplysninger urettmessig vil forekomsten ulovlig tilgang reelt være langt høyere enn ved regelmessig overvåkning av hendelsesregistret. Antallet 500 per 1000 (kolonnen til venstre) illustrerer dette. Om hendelsesregistre ikke regelmessig overvåkes, vil de likevel ha en preventiv effekt. En logg er også viktig for rettsikkerheten til helsepersonell.

Oppsummert mener vi at følgende krav må settes til et system for regelmessig søking i logger:

- Den normale anvendelsen av tilgangen til pasientinformasjonen må være definert og/eller forstått i forhold til
    - kontekst (organisasjon, tjeneste) og problem (diagnose, allment aksepterte prosedyrer og målsetting)
    - legitim variasjon i forløp (pasientenes alder, multi- og co-morbiditet, utilsiktede hendelser, variasjon i pasientpreferanser og behov/tilgjengelige tjenester i videre forløp)
- Logganalysens positive prediktive verdi må være kjent
    - analysens sensitivitet og spesifisitet i den sammenheng den skal anvendes
    - forekomsten av ulovlig anvendelse av tilgang til pasientinformasjon
- Analysen må være akseptert av dem den skal anvendes på, likeledes tiltak/reaksjoner
    - all aktivitet og informasjon må være transparent for alle parter, evt. representanter for disse
    - gjennomføring må være forutsigbar og være en kontinuerlig virksomhet
- Analysen må kunne gi avkastning som må kunne forsvares ressursmessig
    - økonomisk og personellmessig i forhold en samlet politikk på området og andre tiltak som kan redusere brudd på taushetsplikten
    - ikke gå på bekostning av samlet pasientsikkerhet og nødvendig pasientbehandling

Problematikken beskrevet i dette avsnittet henger nøye sammen med kompleksiteten i EPJ-systemene og variasjoner i bruken. En regelmessig overvåkning av hendelsesregistre i enklere systemer vil kunne fungere bedre. Et eksempel vil være en kjernejournal med sterkt begrenset informasjon med anvendelse og formål som foreslått av Nasjonal IKT.

Andre kommentarer

Utkastet til forskrift § 2 om virkeområde kan synes å inkludere alle behandlingsrettede helseregistre. Det er etter vår mening svært omfattende da det finnes en mengde medisinsk tilleggsutstyr med helt spesielle funksjoner. Mange av disse har bare små elementer av pasientinformasjon som ofte knapt kan sies å være sensitiv stående alene uten noen meningsbærende sammenheng.

Det virker for oss uklart om det er et skille, evt. hva det skal være, mellom punkt 3. Tilgang til helseopplysninger og punkt 4. Direkte tilgang til helseopplysninger i § 3 Definisjoner.

I §§9-12 og 17 blir innført et tydelig skille mellom autorisering og tilgang. Det ser vi som positivt. Vi vil imidlertid peke på at for helsepersonell er begrepet autorisert sterkt knyttet til og brukt i sammenheng med yrkesutdanningen. Vi ser for oss at teksten kan bli misforstått.

§ 10 om tilgangsstyringen er svært detaljert med krav som til dels er overlappende og kan komme i konflikt med hverandre. Slik vi har gjort rede for vedrørende kontroll av logger, er medisinsk virksomhet så kompleks at anvendelse av regler på denne måten kan få virkninger som kan bli uheldige og i seg selv true pasientsikkerheten i noen sammenhenger. Vi har også tvil til om arbeidsmengden står i forhold til nytte om det skal foregå en kontinuerlig oppdatering av den enkelte tjenesteyters tilgang medfører kan forsvares i sammenheng med andre oppgaver som helsepersonell og helsetjenesten har i forhold til sine hovedoppgaver. Det er i merknadene til denne paragrafen ikke gjort noen vurdering av disse kravene i forhold til effekten på å ivareta pasientbehandlingen.

§19 stiller krav om at man dokumenterer at tilgangen var nødvendig. Beslutningen kan helsepersonell selv gjøre. Vi mener paragrafen ikke er tydelig nok eller tatt tilstrekkelig hensyn til noen helt vanlige situasjoner, som for eksempel behov for å sjekke ut opplysninger (sikre negativt utfall) og tilgang til opplysninger ved henvendelser, uten at der ytes direkte helsehjelp.

Eksempler:

1. Lege på legevakt blir kontaktet av sykehus med spørsmål om opplysninger om pasient som tidligere på dagen er sendt til sykehus av en annen lege ved legesenteret i kommunen hvor det er felles EPJ-system. Det er ikke legens pasient, og har ikke behandlet pasienten (dvs. ingen behandlingsrelasjon) og kan ikke selv innhente samtykke. Slike henvendelser handler uten unntak om behov for viktige opplysninger (legemidler, cave, prøvesvar).
2. Sykepleier ved LV-sentral får henvendelse direkte fra pasient som er på ferie. Pasienten hadde fått tabletter for en blærekatarr og nå blitt kvalm. Pasienten ville vite om det kunne være tablettene og om hun trengte å oppsøke lege. Hun husket ikke navnet på tablettene. Hun hadde tatt siste dose i morges. Hun brukte også andre legemidler. Ved tilgang på kjernejournal med legemiddelopplysninger ville sykepleieren raskt kunne gitt gode råd og avklart behovet for legetilsyn.

Vi mener det er viktig at rådgivning/veiledning både dirkete av pasient og indirekte via annet helsepersonell skal gi grunnlag for tilgang til helseopplysninger som er nødvendig og relevante. I høringsutkastet av oktober 2008, omfattet § 13 tilgang for å besvare henvendelser og § 15 tilgang for andre formål. Vi ser ikke at det er gitt en begrunnelse for at disse er fjernet.

Til slutt vil DMF gi uttrykk for at vi mener at departementet har gjort et klokt valg når man vil legge opp til en gradvis innføring av denne forskriften. Det gir ikke bare anledning til en god tilpasning, men også til muligheten til å skaffe til veie bedre dokumentasjon på potensielle effekter av det som man innfører av regler.

Det vil også være vårt råd til departementet at man i forskriften tilstreber seg å bli mest mulig uavhengig av teknologien. Utkastet til forskrift er detaljert på krav til bruk av tekniske løsninger. Det er legitimt for løsninger hvor sikkerheten er velprøvd og dokumentert. Det er imidlertid ikke tilfelle vedrørende alle forhold som forskriften tar for seg, spesielt ikke overvåkning av hendelsesregistre i EPJ. Vi er også i tvil om det her er mulig å lage en forsvarlig løsning.

Det største problemet knyttet til å ivareta personvernet i helsetjenesten er dessuten lekkasje fra helsepersonell av informasjon som de får gjennom det som de hører, ser og får lese helt lovlig i arbeidet. Til å forebygge dette finnes det ikke noen teknisk løsning. Det er derfor viktig at forskriften

ikke gir et bilde som tar ressurser og fokus bort fra denne delen av sikkerhetsarbeidet, men heller bidrar til at det får oppmerksomhet og blir prioritert. Vi mener at bedre utdanning her kan være et viktig bidrag.

Med hilsen

Stig A. Slørdahl
Dekan

Arild Skaug Hansen
administrasjonskoordinator

Kopi:
Norsk senter for elektronisk pasientjournal