Nasjonalt senter for
samhandling og telemedisin
NST

Helse- og omsorgsdepartementet

Postboks 8011 Dep
0030 OSLO

Nasjonalt senter for samhandling og telemedisin
Postboks 6060
9038 Tromsø
Telefon 07766
Telefaks 77 75 40 98
info@telemed.no

VÅR REF.:

DERES REF.:
201001921-/ASD

Tromsø, 9. september 2010

Høring av forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Innledende bemerkninger

Generelt:
Nasjonalt senter for samhandling og telemedisin (NST) vil innledningsvis si oss glade for at "Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre" nå er sendt ut på høring. Vi har lest utkastet med stor interesse og tror at effektiv og sikker tilgang til pasient-informasjon er én av flere forutsetninger for en god samhandling i helsevesenet rundt den enkelte pasient. NST er opptatt av at gode teknologiske løsninger tas i bruk for å oppnå dette. Vi håper at denne forskriften skal gjøre det mulig å legge til rette for en effektiv og sikker elektronisk tilgang til pasientopplysninger for helsepersonell i samme og ulike virksomheter til beste for den enkelte pasient, samtidig som opplysningene sikres mot uautorisert innsyn. Dette krever avveininger av ulike hensyn som kan synes vanskelig å kombinere i praksis. Vi anser imidlertid dette utkastet så vidt uklart på enkelte punkter at det i noen sammenhenger kan være vanskelig å få tak i og ta stilling til de avveiningene som er foretatt. På bakgrunn av forslaget stiller vi også spørsmål ved om det er lagt opp til et så omstendelig og detaljert system at forskriften i realiteten vil få begrenset betydning for den fremtidige praksis.

Uansett hvordan den endelige utformingen av forskriften blir, vil NST oppfordre Departementet til å følge nøye med hvordan forskriften blir fortolket og hvordan den viser seg å fungere i praksis.

I vår høringsuttalelse har vi i all hovedsak valgt å ikke legge avgjørende vekt på hva som er realistisk og mulig å få til per i dag. Begrunnelsen er at vi anser at denne forskriften har flere siktemål, derunder å tydeliggjøre for leverandører og brukere på alle nivåer hvilke funksjonaliteter som må på plass for å oppfylle myndighetenes krav til gode løsninger. Det har vært fremhevet i ulike sammenhenger at dette vil kunne bidra til at den fremtidige satsningen blir mer samordnet og målrettet. Det tror vi kan medføre riktighet.

Til utkastet:
Generelt sett mener vi at det i utkastet til forskrift ikke i alle sammenhenger er tilstrekkelig klart hva som er generelle regler, uavhengig av om pasientopplysningene behandles elektronisk eller ikke. Det er følgelig heller ikke klart hvilke krav som (bare?) knytter seg spesielt til elektronisk behandling og elektronisk tilgang. Dette bidrar

til at ikke alle deler av forskriften er like lett å forstå. Vi synes også det er en del uklarheter når det gjelder enkelte begreper. Dette kommer vi tilbake til under de enkelte kapitlene.

Vi forstår det slik at denne forskriften bare gjelder *elektronisk* føring av registre og *elektronisk* tilgang til registre. Dette er lagt til grunn i det følgende.

Når det gjelder tittelen på forskriften, foreslår vi: **Forskrift om informasjonssikkerhet og elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre**. Begrunnelsen for dette er for det første at vi anser tilgangsstyring for å være en del av informasjonssikkerheten. For det andre mener vi det er behov for å tydeliggjøre at denne forskriftens fokus er på elektroniske registre og elektronisk tilgang til helseopplysninger.

Vi vil også foreslå at uttrykket "forsvarlig informasjonssikkerhet" brukes konsekvent i forskriften, også der man har valgt uttrykket "god informasjonssikkerhet" (§§ 1, 7). Begrunnelsen for dette synspunktet er blant annet at helsepersonell og andre som jobber i helsevesenet er vant til å forholde seg til kravet om forsvarlig virksomhet i helsepersonelloven § 4. Etter vår mening vil en slik begrepsbruk også tydeliggjøre sammenhengen mellom krav til forsvarlig informasjonssikkerhet og kravet til forsvarlig virksomhet i hlspl § 4. Forsvarlig informasjonssikkerhet er en forutsetning for å oppfylle taushetsplikten, noe som igjen kan anses som en forutsetning for at virksomheten vurderes som forsvarlig.

Våre forslag til endringer i forskriftsteksten er fremhevet i kursiv.

Kap I Innledende bestemmelser

Generelt
Vi mener som nevnt at det er grunn til å tydeliggjøre at forskriften gjelder *elektronisk* tilgang til behandlingsrettede helseregistre, også under de enkelte punkt.

Vi anser det positivt med en innledende avklaring av sentrale begreper i § 3, men tror det ville lette forståelsen og praktiseringen av forskriften dersom enkelte begreper tas med i tillegg til de som står der.

§ 1 Forskriftens formål
Forslag til ny formulering:
§ 1, siste setning: Videre er formålet å bidra til *forsvarlig* informasjonssikkerhet.

§ 2 Forskriftens virkeområde
Forslag til ny formulering:
§ 2: Forskriften gir regler om informasjonssikkerhet og *elektronisk* tilgang til helseopplysninger i behandlingsrettede helseregistre *opprettet* med hjemmel i helseregisterloven § 6 og helsepersonelloven § 46.

§ 3 Definisjoner
Kommentar:
§ 3, pkt 3: Vi anser det uklart hva som ligger i formuleringen i § 3, pkt. 3: "tilgang til helseopplysninger:". Én måte å forstå dette på, er at dette handler om helsepersonells generelle adgang til å gjøre seg kjent med / kunne få se pasientopplysninger som er relevante og nødvendige i pasientbehandlingen, uavhengig av måten dette skjer på. I så fall inkluderer det også det som er kalt direkte tilgang i pkt 4, både fra egen og ekstern virksomhet. Men sett på bakgrunn av kommentaren i høringsnotatet s. 15, kan det se ut til at man her har tenkt på "utlevering". Hvis så er tilfelle, stiller vi oss noe undrende til det. Vi foreslår en klargjøring.

§ 3, pkt 4: Forslag til ny "overskrift": direkte *elektronisk* tilgang til helseopplysninger
Dette er etter vår mening å anse som en "undergruppe/spesialtilfelle" av pkt 3, som er den generelle bestemmelsen. Pasientopplysninger tilgjengeliggjøres for andre på mange ulike måter; blant dem ved å åpne for direkte tilgang elektronisk til elektroniske behandlingsrettede registre.

Kommentar
§ 3, pkt 4: Vi har også problemer med at her synes "direkte tilgang" å være begrenset til pålogging fra ett system til et annet. (Denne forståelsen forsterkes for øvrig av merknadene til bestemmelsen, s. 43). Man kan også ha direkte tilgang inn i et system uten å koble seg videre til et annet, og man kan ha direkte tilgang til et system uten å koble seg til systemet via et annet system. Vi synes i alle fall at det er uklart hvordan man ser dette for seg og mener at det er behov for en tydeliggjøring av hva som menes.

Forslag til tillegg:
§ 3: Vi foreslår at definisjoner av følgende begreper tilføyes, da disse begrepene nok er forholdsvis ukjente for mange.
6. Beslutningsstyrt tilgang:
7. Rollebasert tilgang:
8. Hendelsesregister/logg:
Det kan også være nyttig å presisere hva man legger i begrepet "rolle" slik det er benyttet i denne forskriften, noe vi antar vil bli nødvendig ifm. definisjonen av rollebasert tilgang.

Kapittel II Generelle krav til informasjonssikkerhet

Generelt
Vi anser det som positivt og nødvendig at det skal være klart for alle hvem som er ansvarlig for informasjonssikkerheten i virksomheten. Vi tror også det er nødvendig at det lages retningslinjer som tydeliggjør hva dette ansvaret innebærer for ansatte på alle nivåer.

Også i dette kapittelet er det tatt inn regler som følger av den generelle lovgivning/forskrifter. Vi ser at det kan være viktig å påpeke plikten til å planlegge, organisere og kontrollere, men vi er i tvil om det er nødvendig å være så detaljert som her.

I dette kapittelet er vi heller ikke helt sikre på hvor generelle de enkelte bestemmelsene er tenkt å være. Dette gjelder for eksempel § 4. Gjelder den alle typer behandlingsrettede helseregistre, eller snakker vi (bare?) om elektroniske registre. Igjen: Vi er vant til at når det snakkes om forsvarlige systemer og informasjonssikkerhet, relaterer dette seg til elektroniske systemer. Med det siste som forutsetning har vi følgende forslag til endringer:

§ 4 Krav om forsvarlige systemer
Forslag til ny formulering:
§ 4: Virksomheter som tar i bruk *elektroniske* behandlingsrettede helseregistre, skal sørge for at *datasystemene* som *benyttes, oppfyller de til enhver tid gjeldende krav til forsvarlig informasjonssikkerhet for behandling av helseopplysninger.*

§ 5 Krav til planlegging, organisering og rutiner
Forslag til ny formulering:
§ 5, 1. setn.: Virksomhet som tar i bruk *elektroniske* behandlingsrettede helseregistre, ...

§ 6 Krav om internkontroll
Forslag til ny overskrift:
§ 6 overskriften: Krav om internkontroll *av informasjonssikkerheten*

Forslag til ny formulering:
§ 6 tredje ledd, siste strekpunkt:
- forebygging, avdekking og oppretting av overtredelser *av bestemmelsene i denne* forskrift

§ 7 Sikkerhetsledelse
Forslag til ny formulering:
§ 7: *Virksomhetens ledelse* har ansvaret for at informasjonssikkerheten i virksomheten er *forsvarlig* og at *de til enhver tid gjeldende lover og regler på dette området* følges *opp*.

Kapittel III: Krav om system for utstedelse av autorisasjoner og krav til autentisering

§ 9: Krav om system for administrering av autorisasjoner
Forslag til ny formulering
§ 9 første ledd: "Databehandlingsansvarlig skal etablere de organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner *som er nødvendige for at forvaltningen av pasientinformasjonen skal anses forsvarlig."*

§ 10: Krav til tilgangsstyring – forholdet til taushetsplikt
Generelt
Vi stiller spørsmål ved om denne bestemmelsen er for detaljert, og kan mistolkes.

Forslag til ny formulering:
§ 10 første ledd: Vi foreslår å sløyfe 1. ledd andre punktum. Eventuelt kan man henvise til hlspl §§ 25 og 45 (taushetspliktbestemmelsene og unntakene fra dem) for å understreke bakgrunnen for og hensikten med bestemmelsen.

Det kan med fordel tas med et punkt om at autorisasjonen skal være rollebestemt, og ikke bare person- og/eller profesjonsbestemt.

Forslag til ny formulering:
Tillegg til § 10, 2. ledd andre punktum: "Den enkelte tjenesteyters behov for den aktuelle autorisasjonen i tjenesten skal vurderes og oppdateres *i henhold til rutiner beskrevet i virksomhetens internkontrollsystem."*

§ 11: Vilkår for utstedelse av autorisasjon
Forslag til sammenslåing av de to leddene i bestemmelsen:
§ 11: *Ingen kan autoriseres for tilgang til helseopplysninger i videre omfang enn det som følger av taushetspliktbestemmelsene i helsepersonelloven, er nødvendig for tjenesteyters arbeid og begrunnet i tjenstlig behov. Grunnlaget for tilgangen skal dokumenteres.*

Vi synes det er uklart hva som menes med det siste. Dersom det er grunnlaget for autorisasjonen som menes, bør dette begrepet brukes i stedet for "tilgangen".

§ 12: Krav om opplæring
Kommentar:
I kommentaren vises det til at helsepersonell nødvendigvis autoriseres til videre tilgang enn de strengt tatt har tjenstlig behov for. Dette begrunnes i behovet for tilgjengelighet og problemer med å avgrense på forhånd hva behovet er. Derfor blir den enkeltes holdninger også viktig.
Vi synes dette er bra og i tråd med det vi har hevdet i mange sammenhenger: nemlig at man må ta i bruk flere virkemidler som til sammen gir en effektiv beskyttelse av pasientens rettigheter. Videre synes vi det er positivt at det her kommer et krav om opplæring relatert til informasjonssikkerhet.

§ 14 Autorisasjon for ytelse av helsehjelp
Forslag til tillegg i teksten:
§ 14 andre ledd, i.f.: "... i ekstern virksomhet *via direkte oppslag i den eksterne virksomhetens systemer.*" Dette for å presisere at det dreier seg om direkte oppslag, og ikke den generelle retten til å forespørre pasientinformasjon fra annen virksomhet.

Forslag til tillegg:
§ 14 tredje 3. ledd: *"Medhjelper har også et selvstendig ansvar for å følge reglene om taushetsplikt."*

Kap IV Tilgang til helseopplysninger i behandlingsrettet helseregister

Generelt
Nasjonalt senter for samhandling og telemedisin (NST) slutter seg til vurderingen om at det er tjenelig å samle bestemmelsene om tilgang til helseopplysninger i et eget kapittel i forskriften. Etter vår mening bør overskriften til kapittelet være *"Elektronisk* tilgang til helseopplysninger i behandlingsrettet helseregister".

Kommentarer
Forslagets § 18 bør komme til sist i kapittel IV. Det er mer naturlig at kapittelet starter med bestemmelsene i § 19.

Til § 19 Tilgang til helseopplysninger for ytelse av helsehjelp
Forslag til ny overskrift:
§ 19: *"Elektronisk* tilgang til helseopplysninger for ytelse av helsehjelp".

Kommentar:
Departementet bes vurdere om det i bestemmelsen eller annet sted i kap IV bør fremgå mer direkte at elektronisk tilgang har samme rettslige grunnlag som annen tilgang og at tilgangen og begrensninger i denne er hjemlet i helsepersonelloven §§ 25 og 45. Dette er nevnt i kommentarene til de enkelte bestemmelser men kommer ikke frem i forskriftsteksten.

§ 19, første ledd: Kravet om at tilgang er betinget av at det skal foreligge konkret beslutning om å yte helsehjelp til pasienten kan komme i konflikt med ønsker om tidlig kontakt mellom for eksempel sykehus og kommunehelsetjeneste i forbindelse med behandling av pasient. I prosjektet "Elin-k" er det blant annet utviklet såkalte tidligmeldinger der det kan meldes om pasient som *kanskje* må legges inn eller ha annen behandling. I forbindelse med disse meldingene kan det være behov for (elektronisk) tilgang til helseopplysninger også før (og etter) at det er "foretatt en konkret beslutning om å yte helsehjelp til pasienten".

Forslag til ny formulering:
§ 19 første ledd, andre setning: "Tilgangen skal følge av *at det vurderes å yte helsehjelp til en pasient eller at det er fattet en konkret beslutning om å yte slik hjelp."*

Kap V Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

Generelt
Bestemmelsene i dette kapittelet blir imøtesett med stor forventning. I telemedisin- og e-helsemiljøet i Norge har lovregulering av "tilgang på tvers" vært et tema i mange år. NST er glad for at lovendringene og denne forskriften nå gjør det mulig å etablere elektronisk tilgang mellom virksomheter.

Slik bestemmelsene nå er utformet gis det svært begrensede muligheter for tilgang på tvers. Vi håper departementet i samarbeid med brukerne fortløpende vil vurdere om ordningene som etableres viser seg hensiktsmessige og tjenelige for brukerne.

Vi vil foreslå at dette kapittelet i utkastet gjennomgås med tanke på en mulig omstrukturering av innholdet. Slik teksten nå står, kan det være vanskelig å skaffe seg oversikt. For eksempel er det nødvendig å se § 26 i sammenheng med § 22. Det er et spørsmål om ikke disse to bestemmelsene burde slås sammen, eller at § 26 flyttes frem.

Vi tror det kan være hensiktsmessig å vurdere å utarbeide retningslinjer og/eller maler for avtaler om lese- og skrivetilgang som skal inngås mellom virksomheter.

Forslag til ny overskrift kap V: "Tilleggsbestemmelser for direkte *elektronisk* tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter".

Til § 22 Avtale om direkte lesetilgang til helseopplysninger på tvers av virksomheter
Bestemmelsen bør gjøre det klart at det er ledelsen i virksomhetene som skal inngå avtaler som nevnt.

Til § 25 Krav til autentisering
Kommentar:
NST mener at det som hovedregel bør være krav om autentisering ved bruk av kvalifisert sertifikat for å få tilgang til helseopplysninger i et behandlingsrettet helseregister ved en ekstern virksomhet. Vi mener imidlertid at det bør åpnes for unntak fra dette kravet der virksomhetene som inngår avtale om tilgang på tvers har god tilgangsstyring og et høyt sikkerhetsnivå, har felles drift av autorisasjonssystem og/eller brukerdatabase, og dersom det gjennom risikoanalyse kan dokumenters at sikkerheten er forsvarlig.

Til § 26 Krav til forespørselen m.m.
Kommentar:
Vi forutsetter at det i siste punktum ligger at den som forespør informasjon om en pasient i en annen virksomhet må autentisere seg på nytt i henhold til kravet i § 25 hver gang det forespørres om slik informasjon, og at det helsepersonell som forespør ikke må gjennom ny autorisasjon til å få gjøre oppslag i ekstern virksomhet dersom vedkommende allerede er autorisert for dette. I praksis begrenser dette seg da til krav om ny innlogging hver gang man skal ha tilgang til informasjon fra systemet i annen virksomhet, og at det ikke er krav om at man må autoriseres på nytt for hvert oppslag.

Til § 27 Krav om samtykke
Kommentar:
Bestemmelsen bør presisere hvem det er som skal innhente og dokumentere samtykke fra den registrerte.

Det bør videre klargjøres på hvilket tidspunkt det skal innhentes samtykke. Av kommentaren til bestemmelsen framgår at samtykket må innhentes fra pasienten "i den aktuelle behandlingssituasjonen det er behov for

opplysningene". Det er noe uklart hva som ligger i dette. Skal samtykke foreligge på det tidspunkt den registrerte er pasient ved ett foretak og det blir aktuelt å gjøre oppslag i pasientens journal i en annen virksomhet? Skal det kunne innhentes et mer generelt samtykke når opplysninger føres i journal første gang med spørsmål til pasienten om disse opplysningene skal kunne gjøres tilgjengelig for tilgang fra eksterne virksomheter? Eller er tanken at det skal være opp til den enkelte virksomhet å bestemme dette, eventuelt i samarbeid med andre virksomheter det inngås avtale om "tilgang på tvers" med? Dette bør etter vår oppfatning klargjøres i forskriften.

Kapittel VI: Sperring av helseopplysninger

Effektive måter å sperre for opplysninger i elektroniske behandlingsrettede helseregistre er utvilsomt en forutsetning for en forsvarlig informasjonssikkerhet/ forsvarlige informasjonssystemer. Vi er imidlertid i tvil om disse generelle reglene om adgangen til å sperre helseopplysninger når pasienten motsetter seg at opplysninger deles, hører hjemme i denne forskriften.

Vi stiller oss også noe spørrende til bestemmelsens 3. ledd og adgangen til å forskriftsregulere at det skal fremgå av journalen at den inneholder opplysninger som er sperret "...dersom det antas å være påtrengende nødvendig for å yte forsvarlig helsehjelp i en akutt situasjon,..". Hvis en slik ordning skal innføres, bør i så fall dette baseres på et informert samtykke fra pasienten.

Kapittel VII: Logging

Generelt
Loggføring og kontroll av logger er utvilsomt et viktig verktøy for å sikre en forsvarlig behandling av pasientopplysninger. Det forutsetter imidlertid at alle i systemet har kjennskap til at det blir gjort. Vi vil imidlertid understreke at logging og kontroll av logg begrenser seg til etterfølgende kontroll og avdekking av lovbrudd som allerede er begått, og derfor er av begrenset verdi som informasjonssikkerhetsverktøy. Når opplysninger er på avveier, er allerede skaden skjedd. Logging og kontroll av logg er derfor tiltak som må ses i nær sammenheng med andre virkemidler som tas i bruk for å hindre uberettiget innsyn og at opplysninger havner på avveier.

Vi foreslår at de generelle bestemmelsene om hendelsesregistrering innleder kapittelet (§§32 og 33).

§ 31 Krav om dokumentasjon av tilgang
Forslag til endring av overskrift:
§ 31: Krav om dokumentasjon av *elektronisk* tilgang *til behandlingsrettet helseregister*

Kommentar/spørsmål:
§ 31 første ledd: Vi er usikre på hva som menes med "tidsrom" i pkt c). Er det tidsangivelse for hver enkelt tilgang? Det kan i så fall bli mange i løpet av en innleggelse. Eller er det en samlet tidsangivelse for en "episode" eller innleggelse, for eksempel NN har hatt tilgang 14 ganger i perioden 13.03.10-22.03.10, første gang (dato) og siste gang (dato)?

§ 32 Krav om hendelsesregistrering/logg
Kommentar/spørsmål:
§ 32 andre ledd: Vi er heller ikke helt sikre på hva som ligger i "stedet" hvor vedkommende har vært pålogget fra (§ 32pkt b)).

§ 33 Oppfølging og kontroll av elektronisk tilgang
Kommentar/spørsmål:
§ 33: Det er noe uklart for oss hva "jevnlig kontrollere" er tenkt å skulle innebære i praksis. Skal loggen kontrolleres rutinemessig hele tiden, eller er stikkprøver tilstrekkelig?

Slik vi ser det ville målsettingen med logging og kontroll av logger oppfylles ved at all aktivitet logges og at kontroll for eksempel foretas etter følgende mønster:

- Gjennomgang på forespørsel fra pasient
- Gjennomgang av logger knyttet til journaler det er grunn til å tro at det er stor interesse for ("kjendiser")
- Rutinemessige stikkprøver (random)
- Regelmessig gjennomgang av tilgangslogg for ansatte i virksomheten med vid tilgang og liten eller ingen pasientkontakt
- Stikkprøver av ev. andre grupper ansatte med vide fullmakter

Rutiner for slik kontroll skal nedfelles i virksomhetens internkontrollsystem/sikkerhetspolicy.

§ 34 Innsynsrett i logg og annen dokumentasjon av tilgang
Forslag til endring av overskrift:
§ 34 Innsynsrett i logg/*hendelsesregistre* og annen dokumentasjon av tilgang

Med vennlig hilsen

for Kirsti Laurents

Toralf Hasvold
Leder for Nasjonalt senter for samhandling og telemedisin

Ellen K. Christiansen
Seniorrådgiver