SIEMENS **Healthcare**

Helse- og Omsorgsdepartementet
Postboks 8011 Dep
0030 Oslo

Navn	Sigbjørn Skjervold
Avdeling/seksjon	HS
Divisjon	Med
Tlf.	22 63 48 16
Faks	22 63 48 80
Mobil	922 39 948
E-post	sigbjoern.skjervold@siemens.com

Kopi:

Deres referanse	201001921-/ASD
Vår referanse	SISK100910
Dato	10. september 2010

Høringsuttalelse

Vi har mottatt "Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre", og vil gjerne komme med enkelte kommentarer til forslaget.

Overordnet mener vi forslaget er meget godt, og at forskriften vil bidra til en klar styrking av pasientsikkerheten i IT-systemer som omfatter pasientrettede registre – herunder spesielt elektroniske journalsystemer (EPJ).

Vi tillater oss å bemerke at vårt pasientjournalsystem DocuLive EPJ i det alt vesentlige allerede imøtekommer kravene i forskriften – forutsatt at foretakene / databehandlingsansvarlig konfigurerer installasjonen korrekt. Vi tar utfordringene rundt tilgangsstyring og –kontroll svært alvorlig, og gjør vårt ytterste for å tilpasse våre systemer slik at de er i overensstemmelse med gjeldende (og foreslåtte!) lover og forskrifter.

Våre konkrete kommentarer er som følger:

§ 10 Krav til tilgangsstyringen – forholdet til taushetsplikt
Den databehandlingsansvarlige skal sørge for at virksomhetens tilgangsstyring sikrer og begrenser tilgangen til de helseopplysninger som er relevante og nødvendige for formålet med tilgangen. Tilgangen skal vurderes og konfigureres med hensyn til:
a) antall registrerte det gis tilgang til
b) mengde informasjon om den enkelte det gis tilgang til og
c) varighet av tilgangen.

Enhver autorisasjon skal være tidsbegrenset og bare omfatte slik behandling av helseopplysninger som er relevant og nødvendig for å nå det angitte formålet med tilgangen. Den enkelte tjenesteyters behov for den aktuelle autorisasjonen i tjenesten skal vurderes og oppdateres jevnlig.
Virksomheten skal dokumentere vurderingene etter andre ledd. Dokumentasjonen skal inngå i virksomhetens internkontrollsystem.

Vi tror det vil bli vanskelig å finne operative regler vi som systemleverandør kan implementere i vårt EPJ for å tilfredsstille spesielt pkt. b i forslaget. Det kan også virke som om formuleringene i denne paragraf vil være komplisert eller uhensiktsmessig for foratakene / databehandlingsansvarlig å kunne følge opp – uansett støtte fra EPJ-systemet.

§ 25 Krav til autentisering
Enhver som gis tilgang til helseopplysninger i et behandlingsrettet helseregister ved en ekstern virksomhet, skal autentisere seg ved bruk av kvalifisert sertifikat.

Vi er usikre på hvor hensiktsmessig eller nødvendig det er i forskrifts form å binde autentiseringsmetoden fast opp mot kvalifisert (personlig) sertifikat. Vi vet at mange av helseforetakene av økonomiske og andre årsaker antakelig vil vente i lang tid med å innføre slike sertifikater til alle ansatte / brukere. Det vil derfor kunne by på praktiske vansker å komme i gang med utprøving eller bredding av "tilgang på tvers" dersom dette kravet blir gjort gjeldende. Poenget bør vel heller være å kreve *tilstrekkelig sikker* autentisering – uten å gå inn på nøyaktig hvilke tekniske mekanismer som benyttes.

Dersom det for eksempel benyttes virksomhetssertifikater mellom institusjonene, og systemene hver for seg gir tilstrekkelig høy grad av autentiseringssikkerhet for brukerpålogging (passordstyrke, evt. biometrisk pålogging og lignende) bør sikkerheten rundt autentisering kunne ivaretas forsvarlig.

§ 26 Krav til forespørselen m.m.
En forespørsel om og direkte tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Forespørselen og tilgangen til helseopplysninger kan bare omfatte en person om gangen. Forespørselen samt beslutningen om å etterkomme den, eller ikke, skal registreres. Ved behov for gjentatt tilgang til helseopplysninger om samme pasient skal det gjøres en ny forespørsel.

Vi er usikre på hvor hensiktsmessig siste setning i avsnitttet er. Vi antar at hensikten er å hindre en "åpen" adgang for all framtid etter at en konkret forespørsel er akseptert, men det vil vel være mer regelen enn unntaket at helsepersonell har behov for flere påfølgende "oppslag" i pasientens helseopplysninger i en gitt behandlingssituasjon. Vil det ikke da være bedre å begrense varigheten av en akseptert forespørsel til "angjeldende behandlingsbehov" eller liknende – evt. også med en konfigurerbar øvre tidsgrense?

§ 29 Sperring av helseopplysninger
Dersom den registrerte har motsatt seg eller motsetter seg at andre får tilgang til helseopplysninger, jf. helsepersonelloven §§ 25 og 45, skal opplysningene sperres.
Den registrerte kan bestemme om sperringen kun skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for den eller de den registrerte selv bestemmer, eller om de bare skal være tilgjenglig etter samtykke.
Dersom de opplysninger den registrerte krever sperret antas å være påtrengende nødvendig for å yte forsvarlig helsehjelp i en akutt situasjon, skal det fremgå av journalen at det er registrert opplysninger som er sperret.

Vår kommentar til dette punktet gjelder siste setning. Hvordan kan man a priori vite hvilke opplysninger som vil kunne være "påtrengende nødvendige"? Er det ikke da bedre å kreve at det skal være mulig i journalen å se at det finnes sperrede opplysninger, evt. at denne informasjonen kun er tilgjengelig for brukere / brukerroller med spesifikk rettighet til å se om slike opplysninger er registrert?

Med vennlig hilsen

Vedlegg

Sigbjørn Skjervold