Direktoratet for forvaltning og IKT

Vår dato	Vår referanse
10.09.2010	2010/3818
Deres dato	Deres referanse
10.05.2010	201001921-/ASD

Helse- og omsorgsdepartementet
Postboks 8011 DEP
0030 Oslo

Høringsuttalelse: Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Difi viser til høringsbrev av 10. mai, med frist for uttalelse 10. september. Direktoratet er ikke oppført blant høringsinstansene, men finner det likevel naturlig å avgi uttalelse.

Difi vil innledningsvis gi uttrykk for at det er positivt til forskriftsregulering av dette kompliserte feltet, og tiltrer i all hovedsak forslaget.

For Difi er det sentralt at det i regelverket benyttes en enhetlig begrepsbruk og systematikk, slik at krav og metode har overføringsverdi og er gjenkjennbart for brukeren. Vi har i dag flere lover og forskrifter som omhandler informasjonssikkerhet. Disse er dessverre ikke samordnet på en optimal måte. Det hadde derfor fremstått som positivt om departementets forslag i større grad hadde bidratt i et slikt samordningsperspektiv.

Til § 3 pkt. 4 hvor direkte tilgang til helseopplysninger defineres. Begrepet benyttes ”bare” i to bestemmelser. Difi er usikker på om definisjonen har noen merverdi, og om begrepet i seg selv gir tilstrekkelig informasjon. Eventuelt kan definisjonen endres til noe i retning av *”mulighet til direkte innlogging i virksomhetsinterne eller eksterne behandlingsrettede helseregistersystemer”.*

Til § 4 om krav om forsvarlige systemer. Etter forslaget skal virksomheten sørge for at ”*systemene som tas i bruk sikrer forsvarlig informasjonssikkerhet”*. Sikring av informasjonssikkerhet i et behandlingsrettet helseregister er komplisert, omfattende og et samspill av flere ulike elementer og tiltak. Et system i seg selv kan bare sikre elementer av dette. Ivaretakelse av tilfredsstillende informasjonssikkerhet i et behandlingsrettet helseregister forutsetter øvrige rutiner og tiltak, samtidig som alle tekniske berøringsflater til enhver tid også oppfyller kravet. Et systems sikkerhetsnivå er heller ikke en statisk størrelse. Muligheten til å ivareta kravet preges av den raske utviklingen, og forutsetter en dynamisk utvikling for å begrense konsekvensene av de til enhver tid identifiserte farer. Etter Difis oppfatningen bør bestemmelsens ordlyd endres til noe i retning av *”Virksomheter som tar i bruk behandlingsrettede helseregistre, skal sørge for at de elektroniske løsningene og tilknyttede tiltak til enhver tid er egnet til å ivareta og sikre forsvarlig informasjonssikkerhet.”*

For øvrig vil Difi anbefale at det i forskriften gjennomgående benyttes *”god informasjonssikkerhet”* (§ 1), *”forsvarlig informasjonssikkerhet”* (§ 4) eller det tradisjonelle begrepet ”*tilfredsstillende informasjonssikkerhet”*. Forslaget skaper enkelte uklarheter for denne del.

Direktoratet for Forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00

Besøksadresse Oslo:
Sandakerveien 24C,
inngang D 9, 4. etasje
Telefaks Oslo: 22 45 10 01

Besøksadresse Leikanger:
Skrivarvegen 2
Telefaks Leikanger: 57 65 50 55

postmottak@difi.no
Org.nr.: NO 991 825 827
www.difi.no

Til §§ 22 og 24 omtaler strukturerte helseopplysninger og strukturert og forhåndsvurdert klinisk informasjon. I merknadene til § 24 er det presisert ved at journalføringen skal kan struktureres og er strukturert på en slik måte at det er mulig bare å gi tilgang til et avgrenset sett av informasjon. Difi er av den oppfatning at det bør fremgå tydeligere i merknadene hva som ligger i dette. Vil en begrenset journal, uten de mange støttesystemer og tilknyttede informasjonssamlinger, være å anse som strukturert? Tilsvarende spørsmål kan reises for røntgeninformasjonsystemet.

Til § 25 om krav til autentisering. Difi er positiv til at det stilles tydelige krav til autentisering. Krav til verifisering av at brukeren er den vedkommende gir seg ut for å være, er viktig. Forskriften legger opp til at det skal kreves autentisering med kvalifisert sertifikat. Vi anbefaler at bestemmelsen gis en annen utforming, som opprettholder kravet til sikkerhet, men uten å kreve at sertifikatet er angitt som ”kvalifisert”.

Vi vil her vise til at annet regelverk henviser til forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere, som igjen peker på Kravspesifikasjon for PKI i offentlig sektor. Kravspesifikasjonen er en overordnet, funksjonell kravspesifikasjon for selvdeklarering og anskaffelse av PKI-basert eID som skal benyttes med og i offentlig sektor. Den er hjemlet i eForvaltningsforskriftens § 27. Formålet med kravspesifikasjonen er å bidra til enklere anskaffelser og felles krav til sikre og standardiserte PKI-tjenester i forvaltningen. For personlige sertifikater er det definert to sertifikatklasser som har forskjellig sikkerhetsnivå: Person-Høyt og Person-Standard. I kommende versjon 2.0 (som per d.d. er på EØS-høring med høringsfrist den 23. september), stilles det krav om at sertifikater som inneholder bruksområdet signering skal være kvalifiserte og merkes som dette, se Kravspesifikasjon for PKI v 2.0 pkt 4.1.4. Sertifikater som ikke inneholder bruksområdet signering, og for eksempel kun skal benyttes til autentisering eller kryptering, *kan* merkes som kvalifiserte men må ikke. Det stilles imidlertid like strenge sikkerhetskrav som til kvalifisert sertifikat, og en sertifikatutsteder som leverer sertifikater for autentisering skal også tilby sertifikat for signering. Det er imidlertid uheldig dersom sertifikater som oppfyller Kravspesifikasjonen for offentlig sektor ikke skal kunne benyttes for tilgang til helseopplysninger.

Lovtekniske hensyn taler også for at det benyttes en lik henvisning i alle lover og forskrifter hvor det stilles krav om bruk av en eID med høy sikkerhet med og i forvaltningen, og det bør henvises til forskrift om frivillig selvdeklarasjonsordninger § 3. Dersom kravet senere skulle endre seg vil det være tilstrekkelig med lov-/forskriftsendring kun ett sted.

Difi foreslår følgelig at det i forskriften benyttes samme henvisning som er gjort i hvitvaskingsforskriften:

> **FOR 2009-03-13 nr 302: Forskrift om tiltak mot hvitvasking og terrorfinansiering mv.**
>
> **§ 6.** *Elektronisk legitimasjon for fysiske personer*
>
> Gyldig legitimasjon for fysiske personer er elektronisk signatur som oppfyller kravene i forskrift 21. november 2005 nr. 1296 om frivillig selvdeklarasjonsordninger for sertifikatutstedere § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift.

Difi antar at det vil kunne være et behov for at utenlandske leger på kortere arbeidsoppdrag skal ha tilgang til registrene, og at disse skal kunne benytte den eID de skulle inneha fra eget land. Vi kan ikke se at denne problemstillingen er vurdert i høringsnotatet. I flere land i Europa merkes ikke autentiseringssertifikat som kvalifisert. I for eksempel Italia er det kun signeringssertifikat som tillates merket kvalifisert.

Til § 26 om krav til forespørselen m.m. Bestemmelsen setter et krav om at tilgang til annen virksomhet skal skje via ”autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet”. (vår kursivering).

Motivene drøfter ikke muligheten for bruk av fellesløsninger for autentisering og autorisasjon. Forskriftens krav om at slike tjenester må være i egen regi kan tyde på at dette ikke skal være mulig. Vi antar utgangspunktet må være at felleskomponenter skal kunne benyttes, jf. målsetningene for statlig ikt-politikk, som bl.a. kommer til uttrykk i St.meld. nr 17 (2006-2007). Som kjent tilbyr Difi i dag en felleskomponent på autentiseringsområdet, og denne vil også støtte autentisering på høyt sikkerhetsnivå.
HOD oppfordres derfor til å klargjøre at kravet om "egen regi" ikke er til hinder for at tilgang kan gis ved hjelp av fellestjenester, så lenge den databehandlingsansvarlige finner dette sikkerhetsmessig forsvarlig.

Vennlig hilsen
for Difi

Tone Bringedal
Avdelingsdirektør

Ingvild Høvik Kiland
Seniorrådgiver