13. september 2013

Til:
Ministeriet for Sundhed og Forebyggelse
Att:Dorthe Rodian
Mail: dra@sum.dk

Høringssvar om udkast til Bekendtgørelse om medicin- og vaccinationsoplysninger

Rådet for Digital Sikkerhed (RfDS) finder anledning til at fremkomme med en kommentar til det fremsatte forslag til bekendtgørelse, idet det vil få betydning for borgernes oplevelse af tillid til den offentlige digitalisering og til sikringen af en tryg it-anvendelse i Danmark.

RfDS er ikke optaget på listen over høringsparter og fremsender derfor nærværende høringssvar uopfordret. Rådet for Digital Sikkerhed, der blev etableret i 2012, anmoder om fremover at blive adviseret om relevante høringer.

Tryg it-anvendelse
RfDS har som mål at fremme effektiv it-sikkerhed og persondatabeskyttelse og fremsætter i det følgende forslag til, hvordan adgang til medicin- og vaccinationsoplysninger kan sikres på en måde, der tilgodeser hensynet til høj sikkerhed om borgernes sundhedsoplysninger og samtidig imødekommer et behov for et effektivt sundhedsvæsen, der giver borgerne adgang til behandling og services af højest opnåelige kvalitet.

RfDS er således som udgangspunkt positiv overfor at gøre adgangen til medicin- og vaccinationsoplysninger lettere for det behandlende sundhedspersonale ved at integrere oplysningerne i lokale journalsystemer.

Samtidig finder vi, at etablering af såvel adgang til som integration af sundhedsoplysningerne kræver en såkaldt Privacy Impact Assessment (PIA). Det vil sikre at mulige risici for uberettiget adgang til borgernes sundhedsoplysninger og misbrug af oplysninger bliver afdækket, samtidig med en den vil give en vurdering af relevansen og nødvendigheden af adgangen til medicin- og vaccinationsoplysninger i forhold til de sundhedsopgaver, der udføres af det personale, der er nævnt i bekendtgørelsens kap. 3.

RfDS anbefaler, at en PIA følges op af kravspecifikationer vedrørende integration med de lokale journalsystemer, der integrerer effektiv it-sikkerhed og beskyttelse af de følsomme sundhedsoplysninger, der behandles og anvendes om borgerne, i systemets arkitektur og design. Et sådant systemtiltag kan med fordel baseres på den eksisterende ISO standard 27002.

RfDS finder endvidere at der i bekendtgørelsen genrelt bør skelnes mellem læse- og opdateringsadgang, så opdateringsadgang kun tildeles, når der er et konkret behov.

Krav om nødvendighed og relevans
Ved at tage udgangspunkt i borgerens behov for relevant behandling af høj kvalitet, vil typen af behandlingspersonale efter RfDS' opfattelse ikke kunne afgrænses generelt eller ved at overlade skønnet om nødvendighed i den konkrete situation til den enkelte behandler, således som bestemmelserne i kap. 3 i udkastet foreslår.

For at fremme sikkerheden og styrke borgernes tillid til sundhedspersonalets korrekte anvendelse af deres sundhedsdata, finder RfDS, at der bør foretages en konkret vurdering af, hvornår det er nødvendigt for sundhedspersonalet i en konkret organisation og situation at tilgå sundhedsoplysninger, og hvornår det er tilstrækkeligt at kende personens fødselsdato, adresse og rette adkomst til behandling eller medicin. Fx forekommer det ikke relevant, at apotekspersonale som udgangspunkt har adgang til en persons samlede medicinoplysninger; det må være tilstrækkeligt at borgeren kan verificere, at han eller hun er den rette indehaver af recepten, og at borgeren selv kan ved sin accept kan give apotekspersonale adgang til at se de samlede medicinoplysninger.

RfDS anbefaler derfor, at der foretages en lokal vurdering af, om der er et reelt arbejdsmæssigt behov for, at den enkelte sundhedsfaglige person skal kunne tilgå medicin- og vaccinationsoplysninger. Dette behov bør være dokumenteret, og en ledelsesmæssig godkendelse bør være et kriterium for at blive godkendt som bruger af systemet.

Krav om decentral dataklassifikation m.m.
I forhold til implementering af ovenstående foreslår RfDS, at bekendtgørelsen udvides med krav om, at der centralt eller lokalt i organisationerne foretages klassificering af personoplysningerne i hhv. almindelige og personfølsomme oplysninger, samt i relevante og ikke-relevante oplysninger for de forskellige personaletypers og lokationers sundhedsbehandling. Yderligere bør der etableres retningslinjer for lokale vejledninger og retningslinjer for anvendelse, logopfølgning, tildeling af adgange m.v.

Rådet er opmærksomt på, at medicin- og vaccinationsoplysninger er personfølsomme oplysninger, og at de på nuværende tidspunkt er vanskelige at adskille fra personers stamdata. Vi mener imidlertid at en sådan adskillelse er ønskelig i fremtiden, og derfor bør der allerede nu påbegyndes en klassificering af oplysningerne, da dette vil gøre det nemmere fremover at etablere nye systemer hvor privatlivsbeskyttelsen er integreret fra start (Privacy by Design).

RfDS anbefaler at systemer etableres, så der lokalt registreres fortegnelse over tildelte brugeradgange samt logning af datatilgang og anvendelse, svarende til bestemmelsen i forslagets kap. 5. Dette bør omfatte specifikation af automatiserede loganalyser, der bl.a. kan afdække uautoriserede søgemønstre i medicin- og vaccinationsoplysninger. Der bør i denne forbindelse også specificeres, hvordan og hvornår der rapporteres til ansvarlige ledelse om uautoriserede opslag.

Til udførelse af de lokalt forankrede opgaver, kan der med fordel udpeges en lokal dataansvarlig eller sikkerhedskoordinator, der tilrettelægger opgaven efter internationale standarder for it-sikkerhed, fx ISO 27002*: Information technology – Security techniques – Code of practice for information security management,* og udmønter disse i lokale vejledninger for anvendelse af SSI's systemer indeholdende medicin- og vaccinationsoplysninger.

Med venlig hilsen

Rådet for Digital Sikkerhed

Birgitte Kofod Olsen
Formand

Lars Stig Jørgensen
Næstformand

Om Rådet for Digital Sikkerhed
Med mere end 40 medlemsorganisationer og et antal forskermedlemmer arbejder Rådet for Digital Sikkerhed for at skabe fokus på tryg digitalisering. Vi bidrager med viden og analyser, som kan være med til at sætte retningen for fremtidens digitale velfærdssamfund. Rådet arbejder for at it-sikkerhed og privatlivsbeskyttelse bliver naturligt integreret i systemer og samfund. Rådet vil understøtte læring og sund adfærd i den digitale verden samt innovativ udnyttelse af teknologiens muligheder.

Læs mere:
digitalsikkerhed.dk

Rådets medlemmer:
digitalsikkerhed.dk/om-raadet/organisation/raadets-medlemmer

Yderligere oplysninger:
Birgitte Kofod Olsen, formand
Mobil: 41 42 83 81
Mail: birgitte.kofod.olsen@digitalsikkerhed.dk

Lars Stig Jørgensen, næstformand
Mobil: 30 56 53 52
Mail: lars.stig.jorgensen@digitalsikkerhed.dk

Bjørn Kassøe Andersen, pressekontakt/sekretariat
Mobil: 42 44 03 30
Mail: bjorn.kassoe.andersen@digitalsikkerhed.dk