

Ministeriet for Sundhed og Forebyggelse
Center for Primær Sundhed og Forebyggelse
Til: primsund@sum.dk
Kopi: seb@sum.dk

Høringssvar om udkast til forslag til lov om ændring af sundhedsloven og lov om klage- og erstatningsadgang inden for sundhedsvæsenet

Rådet for Digital Sikkerhed (RfDS) finder anledning til at fremkomme med en kommentar til det fremsatte lovforslag, idet det vil få betydning for borgernes oplevelse af tillid til den offentlige digitalisering og til sikringen af en tryk 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.

RfDS kommentar knytter sig til lovforslagets § 195, stk. 2 og § 231 e i Sundhedslovens kap. 70 b om obligatoriske opgaver m.v. for alment praktiserende læger.

1. Informationssikkerhed og privatlivsbeskyttelse

RfDS er enig i, at en generel sundhedsplanlægning, herunder tilrettelæggelse og kvalitetsudvikling af sammenhængende patientforløb, må tilrettelægges på en måde, der sikrer effektiv ressourceudnyttelse og undgår overlappende funktioner.

Fra et borgersynspunkt er det imidlertid afgørende for oplevelsen af tillid og tryghed i sundhedssystemet, at digitaliseringen og anvendelsen af personoplysninger sker i systemer, der sikrer effektiv informationssikkerhed og beskyttelse af personlige sundhedsdata.

RfDS finder det nødvendigt, at disse principper skrives ind i sundhedsloven. Det bør således sikres, at videregivelse af personhenførbare sundhedsoplysninger fra alment praktiserende læger til regionerne, herunder kliniske data på den enkelte patient, sker gennem it-løsninger med et højt sikkerhedsniveau, og med en indbygget høj beskyttelse af borgernes grundlæggende ret til persondatabeskyttelse, herunder til beskyttelse af følsomme sundhedsoplysninger.

Sammenfatning:

RfDS opfordrer til, at det indføres i bemærkningerne til lovforslaget, at regionrådene alene kan kræve patientoplysninger indberettet, når det er nødvendigt og proportionalt i forhold til at forbedre effekten af sundhedsydelser.

2. Sikkerhedsniveauet ved videregivelse af sundhedsoplysninger

Efter forslaget skal praktiserende sundhedspersoner, herunder alment praktiserende læger, indberette oplysninger til regionsrådene til brug for planlægning, kvalitetssikring, kontrol af udbetalte tilskud og honorarer m.v. Af forslaget fremgår også, at alment praktiserende læger skal foretage kodning af henvendelser til almen praksis og anvende datafangst, og at data, som er tilvejebragt på baggrund af kodning og datafangst, skal stilles til rådighed for regionerne, jf. § 231 e.

Regionerne er også tiltænkt adgang til at kunne rekvirere kliniske data om patientbehandlingen i almen praksis, som omfatter behandlingsresultater, der kan belyse patientens sundhedstilstand.

Af forslaget fremgår, at de omhandlede oplysninger skal *beskyttes i videst muligt omfang* og at det forudsættes, at regionerne behandler og anvender patientoplysninger i krypteret form. Dog kan der ske kortvarig dekryptering, i det omfang berigelse af oplysningerne med oplysninger fra andre kilder, kræver dette.

RfDS finder at kryptering er et udmærket middel til at begrænse adgangen til oplysningerne, under forudsætning af at der anvendes krypteringsmetoder, der følger almindeligt anerkendte standarder. Heraf følger bl.a. at såkaldt 128 bits sikkerhed på nuværende tidspunkt er et mindstekrav. Men det er vigtigt at understrege, at kryptering naturligvis ikke forhindrer misbrug foretaget af personer, der har adgang til at dekryptere data.

Sammenfatning:

RfDS opfordrer til, at der udarbejdes klare retningslinjer for krav til den kryptering der anvendes, hvem i regionernes organisation, der kan få adgang til data, og hvem der kan autorisere, at oplysningerne dekrypteres.

3. Beskyttelse af følsomme sundhedsoplysninger

RfDS er enig i, at tilrettelæggelsen af fremtidens sundhedsydelse må ske på en måde der sikrer omkostningseffektivitet og kvalitet. Indsigt i sygdomsmønstre, behandlingseffekt og erfaringer med forebyggelse er også legitime hensyn.

For RfDS er det imidlertid helt centralt, at hensynet til borgernes ret til integritet, selvbestemmelsesret og beskyttelse af personlige sundhedsdata integreres i tænkningen og anvendes som argument for at opnå løsninger, der er i borgernes interesse. Persondatabeskyttelse bør således være en integreret del i såvel de specifikationskrav, der stilles til nye løsninger, som i selve designet af de it-arkitekturer, der bærer løsningerne. Ved den efterfølgende anvendelse af indhentet sundhedsdata, må det også ske på en måde, der opfylder forpligtelsen til at beskytte borgerens rettigheder.

Kravet om respekt for borgernes rettigheder og integritet udspringer af EU traktatens charter om grundrettigheder og er senest gentaget i forslaget til EU Forordning om Persondatabeskyttelse. Det er også en grundlæggende forudsætning for livet i et demokratisk samfund, at staten ikke har uhindret indsigt i borgernes private forhold, herunder i sundhedsforhold.

Hvis persondata skal indberettes til regionerne i flere omgange, og hvis det er nødvendigt at kunne genkende oplysninger, der hører til samme person, kan det virke naturligt at indberetningerne ledsages af f.eks. navn eller CPR nummer. Men det er ikke nødvendigt. Identifikationen af en person kan erstattes af pseudonymer eller såkaldt énvejskryptering af CPR numre.

Sammenfatning:

RfDS opfordrer til, at patienternes personlige sundhedsoplysninger kun overføres fra de alment

praktiserende læger til regionerne i et omfang og på en måde, der sikrer, at oplysningerne ikke kan henføres til den enkelte borger.

Med venlig hilsen

Rådet for Digital Sikkerhed

Birgitte Kofod Olsen
Formand

Shehzad Ahmad
Næstformand

Om Rådet for Digital Sikkerhed

Med cirka 50 medlemsorganisationer arbejder Rådet for Digital Sikkerhed med fokus på tryk 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:
www.digitalsikkerhed.dk

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

Shehzad Ahmad, næstformand
Mobil: 20 93 88 22
Mail: shehzad.ahmad@digitalsikkerhed.dk

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