

København, den 19. marts 2025

Til Indenrigs- og Sundhedsministeriet

Hørings svar vedr. bekendtgørelse om pilotprojekt om udveksling af oplysninger via MyHealth@EU i Den Europæiske Union

Dansk Selskab for Almen Medicin (DSAM) ønsker hermed at afgive høringssvar vedrørende den foreslåede bekendtgørelse om pilotprojektet for udveksling af sundhedsdata inden for EU.

Visionen er, at en fælles digital infrastruktur i EU kan sikre bedre koordinering af behandling på tværs af grænser, og i tillæg kan danne grundlag for kommerciel sundhedsinnovation i EU, blandt andet på baggrund af kunstig intelligens (AI), men inden Danmark tilslutter sig et projekt af denne størrelse, må det være et krav, at behovet er grundigt dokumenteret.

Hvilke konkrete sundhedsproblemer skal MyHealth@EU løse? Hvor er dokumentationen for, at patientbehandling på tværs af grænser lider under manglende dataadgang? Medmindre disse spørgsmål besvares grundigt, kan man med MyHealth@EU risikere at stå med en løsning på et problem, som ikke findes.

Typer af oplysninger, der må behandles i MyHealth@EU via den fælles digitale infrastruktur, er:

1. Oplysninger om patientforløb, der kan danne et patientresumé, herunder: sundhedshistorik, herunder operationer, diagnoser, nuværende og tidligere helbredsstatus, medicin, allergier, laboratorie- og prøvesvar og resultater heraf, behandlingsplaner m.v.
2. Oplysninger om recepter og udlevering af medicin.

I en tid med krig i Europa og øgede spændinger internt i EU, og hvor visse medlemslande bevæger sig længere væk fra fundamentale borgerrettigheder, er det ekstra afgørende at fastholde et stærkt fokus på patienternes selvbestemmelse, datasikkerhed og gennemsigtighed.

Overførsel af helbredsdata mellem lande inden for EU, hvor der aktuelt findes stater, hvor retsstaten og beskyttelsen af borgernes privatliv er under pres, indebærer betydelige risici. Dette stiller ekstra høje krav til, at patienterne bevarer fuld kontrol over selve datadelingen, og hvem der kan tilgå deres helbredsoplysninger, samt at der indføres mekanismer, der beskytter mod misbrug. Sundhedsdata er blandt de mest følsomme oplysninger, og uden klare juridiske garantier kan de misbruges både politisk og økonomisk.

- **Ministeren bør sikre, at der foreligger en grundig analyse, som kan godtgøre, at MyHealth@EU er en gavnlig og rentabel løsning uden store risici for de registrerede.**

Datadelingsformål og risici ved EHDS

Det primære formål med delingen af sundhedsdata i EHDS er at understøtte patientbehandlingen på tværs af landegrænser inden for EU. Sekundært er formålet at samle sundhedsdata, så de kan bruges til forskningsmål, herunder også for kommercielle aktører. Særligt er tanken, at samlingen af data skal kunne bruges af virksomheder og forskere til, på pseudonymiserede data (altså ikke reelt anonyme data), at afprøve og træne værktøjer baseret på AI. Der er altså tale om databehandling med høj risiko, jævnfør Artikel 29-Gruppen vedrørende databeskyttelse¹.

Det er i realiteten det sekundære formål, som vil give anledning til størstedelen af databehandlingen, idet kun en mindre del af EU-borgere har behov for, at deres sundhedsdata kan tilgås i andre lande i forbindelse med sygdomsbehandling. Det er derfor afgørende, at offentligheden og politikere fuldt ud forstår de konsekvenser, som en implementering af EHDS vil have – ikke kun for patientbehandling, men også for langsigtet anvendelse af sundhedsdata i kommerciel og forskningsmæssig sammenhæng.

Problemer ved brug af sundhedsdata til AI i MyHealth@EU

Et af de centrale argumenter for MyHealth@EU er, at sundhedsdata kan anvendes til udvikling af kunstig intelligens (AI) til klinisk beslutningsstøtte og personaliseret medicin². Imidlertid er der alvorlige problemer med denne vision. AI-modeller er ikke afhængige af store mængder uspecifikke journaldata, men kræver høj kvalitets, strukturerede data – primært parakliniske data som blodprøver, genetiske analyser og billeddiagnostik. Journaldata, som ofte indeholder vitalparametre, medicinlister og sygdomshistorik, er derimod mindre velegnede til AI-træning, da de ofte er fejlbehæftede, upræcise og inkonsistente³. AI-træning i sundhedsvæsenet primært bør baseres på standardiserede og præcise datasæt, snarere end uensartede patientjournaler^{3,4}.

MyHealth@EU vil dog samle data fra lande med vidt forskellige kliniske standarder, kodingspraksisser og behandlingsprotokoller, hvilket skaber betydelige metodiske problemer. Selv inden for Danmark er sundhedsdata inkonsistente og fejlbehæftede. Når nationale fejl flyttes over i en fælles europæisk database, bliver problemet kun større.

¹ Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679 <https://www.datatilsynet.dk/media/7826/konsekvens-analyser-vedroerende-databeskyttelse-dpia-wp248.pdf>

² https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en

³ Kristiansen TB, Kristensen K, Uffelman J, Brandslund I. Erroneous data: The Achilles' heel of AI and personalized medicine. *Front Digit Health*. 2022 Jul 22;4:862095. doi: 10.3389/fdgth.2022.862095. PMID: 35937419; PMCID: PMC9355416.

⁴ Jawad BN, Altintas I, Eugen-Olsen J, Niazi S, Mansouri A, Rasmussen LJH, Schultz M, Iversen K, Normann Holm N, Kallmose T, Andersen O, Nehlin JO. Prospective and External Validation of Machine Learning Models for Short- and Long-Term Mortality in Acutely Admitted Patients Using Blood Tests. *J Clin Med*. 2024 Oct 27;13(21):6437. doi: 10.3390/jcm13216437. PMID: 39518575; PMCID: PMC11546962.

Sammenfattende er der betydelig usikkerhed omkring, hvorvidt de data, der samles gennem MyHealth@EU, overhovedet vil være anvendelige til AI. Fejlbehæftede og uensartede data vil føre til forkerte AI-modeller, som kan skade patienterne og føre til systematiske fejl i beslutningsstøtteværktøjer. Samtidig risikerer det at resultere i spild af ressourcer og økonomiske midler på initiativer med sparsom værdi. Selv den bedste AI-model kan ikke rette op på fejlbehæftede data.

Manglende hjemmel i sundhedsloven

DSAM vurderer, at den lovhjemmel, som bekendtgørelsen angiveligt skulle hvile på (§ 157, stk. 14, og § 193 b, stk. 3, i sundhedsloven), ikke danner et tilstrækkeligt grundlag for at tillade denne form for international dataudveksling. Disse paragraffer regulerer udveksling af data inden for Danmarks grænser, og vi finder det problematisk at anvende dem som basis for en ordning, der eksplicit indebærer deling af helbredsoplysninger uden for landets grænser. Dette kræver en grundlæggende lovændring og ikke blot en bekendtgørelse.

Europa-Parlamentets og Rådets direktiv 2011/24/EU⁵ fastlægger patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse. Direktivet slår fast, at medlemsstater selv har ansvaret for at beskytte patienters rettigheder og datasikkerhed, hvilket understøtter argumentet for, at en bekendtgørelse ikke er tilstrækkelig – der kræves en egentlig lovændring for at sikre, at de nødvendige retsgarantier er på plads.

- ***Ministeren bør sikre et korrekt juridisk fundament gennem en lovændring, der grundigt belyses i en åben, demokratisk proces, frem for at presse dette igennem via en bekendtgørelse uden en reel debat.***

Patienterne har ingen reel kontrol over egne oplysninger

Det fremgår af bekendtgørelsen, at patienter kan fravælge, at sundhedspersoner i andre EU-lande slår deres oplysninger op. Men patienter har ikke mulighed for at forhindre, at deres oplysninger registreres i MyHealth@EU i første omgang. Data overføres automatisk fra de nationale kildesystemer uden patientens samtykke eller anden mekanisme til at fravælge registrering.

DSAM mener, at dette er en væsentlig mangel og i strid med princippet om dataminimering og selvbestemmelse over egne helbredsoplysninger. Danske patienter har i dag en vis kontrol over egne helbredsdata gennem eksisterende mekanismer såsom Fælles Medicinkort, men denne bekendtgørelse fjerner patienternes kontrol ved at overføre data uden deres aktive medbestemmelse.

- ***Ministeren bør sikre, at patienter får mulighed for at fravælge registrering i MyHealth@EU – ikke blot at begrænse adgangen til automatisk overførte oplysninger efterfølgende. DSAM anbefaler en opt-in-model, hvor patienter aktivt giver samtykke til dataoverførsel.***

⁵ Europa-Parlamentets og Rådets direktiv nr. 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelse, EU-Tidende 2011, nr. L 88, side 45-65. <https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32011L0024&from=PT>

Tavshedspligt, datasikkerhed og behov for uafhængigt tilsyn

Bekendtgørelsen skitserer, at helbredsoplysninger kan gøres tilgængelige for sundhedsprofessionelle i andre EU-lande. Det er dog ganske utilstrækkeligt belyst, hvordan datasikkerheden sikres samt hvordan patienters ret til at blokere for læsning af oplysninger kan administreres effektivt.

Kritiske perspektiver på MyHealth@EU:

1. Det er uklart, hvilke konkrete problemer denne omfattende deling af sundhedsdata på tværs af EU egentlig skal løse. I praksis oplever vi sjældent en mangel på data i mødet med udenlandske patienter, men snarere, at udenlandske journaler ofte er uforståelige eller ubrugelige, da behandlingspraksis varierer betydeligt mellem lande.
2. Bureaukratiet ved at etablere tilstrækkelige sikkerhedsforanstaltninger til at beskytte data i MyHealth@EU vil være enormt, og risikoen for datafejl, uautoriseret adgang eller fejlagtige opslag vil være markant.
3. Det er uforståeligt, hvorfor Danmark deltager i dette pilotprojekt, når der ikke er en klar og veldokumenteret gevinst for patienterne, mens risikoen for misbrug og fejlhåndtering er betydelig.

Kritiske ubesvarede spørgsmål om datasikkerhed:

1. Hvordan sikres det, at lande med varierende datasikkerhedsstandarder ikke får adgang til danske patienters data?
2. Hvordan vil ministeriet sikre, at danske patienters data ikke kan tilgås af myndigheder i andre EU-lande til andre formål end sundhedsbehandling?
3. Hvordan sikres gennemsigtighed i logning af opslag i patienters data på tværs af lande?
4. Hvordan håndteres sikkerhedsbrud og uautoriseret adgang til patientdata?
5. Vil danske myndigheder kunne tilbagekalde data, hvis nye sikkerhedsrisici opstår?

Derudover er det afgørende, at der skabes en garanti for, at patienters oplysninger ikke tilgås af uvedkommende sundhedspersoner i andre lande. Det bør ligeledes sikres, at der findes en effektiv, national kontrolinstans, der kan gribe ind ved eventuelle brud på tavshedspligten.

- ***For at sikre transparens anbefaler vi et uafhængigt tilsyn, som kan føre løbende kontrol med dataadgangen og sikre, at patientrettigheder respekteres i praksis i alle lande.***

Entydig identifikation af sundhedspersonale

DSAM ser behov for, at sundhedspersonale, der tilgår oplysninger via MyHealth@EU, identificeres med en entydig autorisationskode frem for blot navn. Dette vil kunne styrke sikkerheden og audit-trails betydeligt.

- **Ministeren bør forpligte sig til at implementere en entydig autorisationskode for sundhedspersonale i alle lande, så patientdata ikke utilsigtet kan tilgås eller misbruges uden siden at kunne identificeres sikkert.**

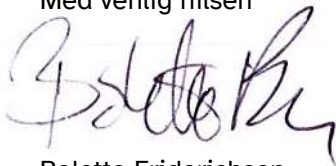
Konklusion

Det er essentielt, at danske patienters rettigheder ikke udvandes i en forhastet EU-integration uden et sikkert demokratisk mandat fra Folketinget via en lovændring. Særligt fordi de økonomiske og administrative byrder risikerer at blive enorme, uden at gevinsterne ved MyHealth@EU er oplagte.

Derudover kan MyHealth@EU føre til diskrimination af danske borgere. I Danmark indsamles og registreres flere sundhedsdata end i flertallet af EU-landene, og samtidig er den danske digitale infrastruktur for deling af data langt mere udbygget og standardiseret end i mange andre medlemslande. Dette betyder, at MyHealth@EU vil medføre mere omfattende datadeling for danske borgere end for flertallet af borgere i resten af EU. En sådan ubalance er problematisk og understreger behovet for en opt-out-mulighed for MyHealth@EU, som nævnt tidligere.

Vi opfordrer kraftigt til, at bekendtgørelsen revurderes, og at ministeriet sikrer, at ingen danske patienter mister retten til at bestemme over deres egne sundhedsdata. Udveksling af sundhedsdata på tværs af grænser kræver et langt stærkere lovgrundlag, langt større datasikkerhed og, vigtigst af alt, en garanti for, at patienternes ret til selvbestemmelse ikke kompromitteres.

Med venlig hilsen



Bolette Friderichsen
Formand for DSAM