

Wearables i sundhedssektoren – pas på den danske automatreaktion

*Hanne Marie Motzfeldt, lektor
Juridisk Institut, Aarhus Universitet*



Foto: colourbox

Der er fremragende perspektiver i at bruge wearables i sundhedsvæsenet. De data, der kan indsamles via sådanne kropsbårne devices, har potentiale til både at forbedre forebyggelse af sygdom og undgå forværring af allerede udviklede sygdomme og til egentlig behandling af patienter. En for praktiskere uden tvivl irriterende hindring er, at det er meget usikkert og komplekst, hvilke retlige rammer der gælder for indsamling af data via wearables.

De usikre og komplekse retlige rammer er der imidlertid god grund til. Databeskyttelsesforordningen skal på en gang beskytte privatlivet i den digitale tidsalder og sikre, at der ikke sættes unødigt rigide barrierer op over for brug af nye teknologier og data til menneskets bedste. Denne balancegang er ikke let, da den drejer sig om, hvordan der sikres en civiliseret brug af de enorme mængder data, der kan indsamles via kropsbårne devices, og som kan opsamle endda meget omfattende mængder data om den enkelte og dermed skabe indgående profiler af adfærd og personlighed.

Profilering defineres i forordningens artikel 4, nr. 4, som enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske person, som fx helbred. Det nævnes i forordningens præambel betragtning 30, at fysiske personer kan tilknyttes online identifikatorer, som tilvejebringes af deres enheder, applikationer mv., og dette kan efterlade spor, der kan bruges til at oprette profiler om fysiske personer og identificere dem.

Ønsker man at se lidt nærmere på de retlige aspekter, er et godt udgangspunkt at betragte wearables databeskyttelsesretligt som del af de teknologier, der kaldes **Internet of Things (IoT)**. Dermed er wearables også noget af det, der var medvirkende til, at det var nødvendigt med en reform af de tidligere regler, hvilket fremgår af præambelen til [databeskyttelsesforordningen](#). Her står bl.a., at den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelse af personoplysninger.

Særlige relevante karakteristika for wearables indenfor sundhedssektoren er, at fysiske personer ofte bærer dem over længere perioder. Samtidig afgiver wearables ikke alene information om bevægelsesmønstre, men også om vedkommendes fysiske tilstand. Anvendes wearables i forbindelse med behandling af patienter, vil oplysningerne dermed være at regne som helbredsoplysninger. Wearables indenfor sundhedssektoren er således en særlig indgribende underkategori af IoT.

Helbredsoplysninger er i forordningen defineret som personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelse, og som giver information om vedkommendes helbredstilstand, jf. artikel 4, nr. 15.

Genetiske data er defineret som personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person, jf. artikel 4, nr. 13, og

Biometriske data regnes som personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger, jf. artikel 4, nr. 14.

Ved fastlæggelsen af, hvad der nærmere skal forstås ved helbredsoplysninger indeholder databeskyttelsesforordningens præambelbetragtning nr.

35 fortolkningsbidrag. Herefter bør helbredsoplysninger bør omfatte alle personoplysninger om den registreredes helbredstilstand, som giver oplysninger om den registreredes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Dette omfatter desuden oplysninger indsamlet i løbet af registreringen af denne med henblik på eller under levering af sundhedsydelse. Også et nummer, symbol eller særligt mærke, der tildeles en fysisk person for entydigt at identificere den fysiske person til sundhedsformål er omfattet, ligesom oplysninger, der stammer fra prøver eller undersøgelser af en legemsdel eller legemlig substans, herunder fra genetiske data og biologiske prøver; og enhver oplysning om f.eks. en sygdom, et handicap, en sygdomsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den registreredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil, f.eks. fra en læge eller anden sundhedsperson, et hospital, medicinsk udstyr eller in vitro diagnostik.

Som det fremgår, vil de data der indsamles ved brug af wearables i sundhedssektoren som udgangspunkt være helbredsoplysninger, idet der i det hele er tale om oplysninger indsamlet og anvendt i forbindelse med levering af sundhedsydelser.

Brug af wearables i sundhedsvæsenet til indsamling af helbredsoplysninger rejser en række retlige spørgsmål, herunder om klarlæggelse af relationen mellem den virksomhed der har udviklet og drifter teknologien og den sundhedsperson eller organisation, der anvender det pågældende device. Herudover er der udfordringer i forhold til de databeskyttelsesretlige principper, især kravene til fair og transparent behandling samt kravet om data-minimering. Også i forhold til kravene i forordningens artikel 25 om databeskyttelse via design og via indstillinger vil der uden tvivl vise sig praktiske udfordringer.

Her fokuseres i det følgende imidlertid på *et* særligt udfordrende punkt; nemlig udfordringerne med at finde det rette databeskyttelsesretlige grundlag for at behandle oplysninger via wearables i sundhedssektoren. Anderledes udtrykt; hvilken behandlingsbetingelse er relevant? Grunden til, at dette er særligt udfordrende, er, at den danske automatreaktion vil være at vende sig mod samtykke, men det er langt fra sikkert, at denne rygmarvsreaktion er klog.

I databeskyttelsesforordningen skelnes bl.a. mellem ordinære personoplysninger og følsomme personoplysninger. Hertil kommer oplysninger om strafbare forhold og CPR-numre, der dog formentlig kun sjældent har betydning i forbindelse med sundhedsvæsenets brug af wearables.

Behandling af følsomme personoplysninger som f.eks. helbredsoplysninger og genetiske data er som udgangspunkt ikke tilladt efter forordningens artikel 9, stk. 1. Generelle undtagelser til dette udgangspunkt er ifølge artikel 9, stk. 2:

- Ifølge litra a kan behandling ske, hvis den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål (se nærmere om samtykke neden for i del II, afsnit 3)
- Ifølge litra h kan behandling ske, hvis behandling foretages af en person underlagt tavshedspligt og er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til ... medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson.
- Hvis behandling er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Som det fremgår, er behandling af helbredsoplysninger når den registrerede har givet *udtrykkeligt* samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål (artikel 9, stk. 2, litra a). Anvendes samtykke som behandlingsgrundlag, skal det samtidig sikres, at den registrerede kan trække dette tilbage – og at tilbagetrækning kan ske lige så let som afgivelse, jf. databeskyttelsesforordningens artikel 7, stk. 3. Sundhedsmyndigheden skal desuden sikre sig at kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger, jf. artikel 7, stk. 1.

Hvad der nærmere ligger i samtykke, uddybes dels i definitionen af samtykke i forordningens artikel 4, nr. 11, dels i databeskyttelsesforordningens præambels betragtning nr. 32, hvorefter:

“samtykke bør gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved vedkommende accepterer, at personoplysninger om vedkommende behandles. Tavshed, forud afkrydsede felter eller inaktivitet bør ikke udgøre samtykke. Samtykke bør dække alle behandlingsaktiviteter, der udføres til det eller de samme formål. Når behandling tjener flere formål, bør der gives samtykke til dem alle. Hvis den registreredes samtykke skal gives efter en elektronisk anmodning, skal anmodningen være klar, kortfattet og ikke unødigt forstyrre brugen af den tjeneste, som samtykke gives til.”

Hertil kommer, at der i databeskyttelsesforordningens artikel 7 stilles en række betingelser, for at et samtykke er gyldigt, dvs. kan anvendes som grundlag for behandling af personoplysninger omfattet af forordningen.

Samtykke fra den registrerede defineres i forordningen som: “enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling”, jf. artikel 4, nr. 11.

De forskellige krav til samtykke er tæt forbundne og til dels overlappende. I kravet om, at et samtykke skal være *specifikt*, ligger, at samtykket skal være konkretiseret, således at det klart og utvetydigt fremgår, hvad der meddeles samtykke til, herunder hvilke oplysninger der må behandles på baggrund af samtykket, af hvem og til hvilke formål, jf. Datatilsynets journalnummer 2007-321-0047.

Af kravet om, at samtykket skal være *informeret* følger, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til – dvs. kan vurdere, om vedkommende vil give samtykke. Af præambelens betragtning 42 fremgår om information, at den registrerede som minimum skal gøres bekendt med den dataansvarliges identitet og formålene med den behandling, som personoplysningerne skal bruges til. Forordningens artikel 7, stk. 2, supplerer her ved at stille krav til den måde, der informeres på. F.eks. skal der anvendes et egnet sprog, så de registrerede forstår, hvad de samtykker i, herunder til hvilke formål. Anvendelse af en kompliceret retlig eller teknisk jargon lever ikke op til kravene. Dertil kommer, at de informationer, der meddeles de registrerede, skal være adskilt fra andre tekster og dermed være klare og tilstrækkeligt synlige, så de registrerede ikke overser dem.

I kravet om *utvetydighed* ligger, at den registrerede skal give et aktivt signal, som er tilstrækkeligt klart til, at det markerer den registreredes vilje, og er forståeligt for den dataansvarlige. Et eksempel herpå kan være, at der forudgående gives information, hvorefter ibrugtagelse af en teknologi betragtes som samtykket, saml. fx Datatilsynets journalnummer 2007-212-0042 (FDB og Coop) om ibrugtagelse af medlemskort. En sådan konstruktion vil dog ikke kunne anvendes ved brug af wearables, idet behandling af helbredsoplysninger kræver et udtrykkeligt, ikke blot utvetydigt, samtykke. Et *udtrykkeligt* samtykke forudsætter et aktivt svar – mundtligt eller skriftligt – hvorved den pågældende udtrykker ønske om, at hans/hendes oplysninger behandles med henblik på bestemte formål.

Databeskyttelsesforordningen indeholder flere fortolkningsbidrag til forståelsen af *frivillighed*. Af præambelens betragtning nr. 42 fremgår, at:

“Samtykke bør ikke anses for at være givet frivilligt, hvis den registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende.”

I den efterfølgende betragtning 43 står følgende:

“Med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgøre et gyldigt retsgrundlag for behandling af personoplysninger i et specifikt tilfælde, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, og det derfor er usandsynligt, at samtykket er givet frivilligt under hensyntagen til alle de omstændigheder, der kendetegner den specifikke situation. Samtykke formodes ikke at være givet frivilligt, hvis det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter vedrørende personoplysninger, selv om det er hensigtsmæssigt i det enkelte tilfælde, eller hvis opfyldelsen af en kontrakt, herunder ydelsen af en tjeneste, gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse.”

Datatilsynet har sammen med en række andre [myndigheder](#) udsendt en vejledning om databeskyttelsesforordningens samtykkekrav i november 2017. Også denne vejledning kommer ind på skævhed mellem den dataansvarlige og den registrerede som en faktor, der kan udfordre samtykkes gyldighed som behandlingsbetingelse. Under pkt. 3.3.1, står bl.a.:

“Det kan f.eks. være tilfældet, hvis den dataansvarlige er en offentlig myndighed og den registrerede ansøger om en offentlig ydelse hos myndigheden. Den registrerede vil i dette tilfælde oftest ikke have andre alternativer end at give samtykke til behandlingen, hvis borgeren vil have ydelsen. Offentlige myndigheder bør derfor overveje anvendelsen af samtykke som behandlingshjemmel.”

Også Artikel 29-gruppen, der ved forordningens virkningstidspunkt omdannes til Databeskyttelsesrådet, har flere gange udtalt sig om, hvornår der opstår udfordringer med at sikre, at samtykke er reelt frivilligt. [I WP 187 s. 38 ff](#) står f.eks., at:

“For at et samtykke er gyldigt, skal det være frivilligt. Det betyder, at der ikke må være nogen risiko for vildledning, intimidering eller væsentlige negative konsekvenser for den registrerede, hvis han/hun ikke samtykker. Databehandling i en ansættelsessammenhæng, hvor der er et underordningsforhold, og i forbindelse med offentlige tjenester, f.eks. inden for sundheds-

området, kan kræve en nøje vurdering af, om der er tale om et frivilligt samtykke fra de ansattes/borgernes side.”

I en række andre udtalelser om mere specifikke temaer har gruppen undersøgt samtykkets begrænsninger, herunder i udtalelsen om elektroniske patientjournaler (WP 131), i udtalelsen om behandling af personoplysninger ved ansættelsesforhold (WP 48) og i udtalelsen om Det Internationale Antidopingagenturs behandling af oplysninger (WP 162). Gruppen anførte i [WP 131 om elektroniske patientjournaler](#), at ved “frivilligt” samtykke menes en viljesbeslutning, som en person, der er ved sine evners fulde brug, har truffet uden nogen form for tvang af social, økonomisk, psykologisk eller anden art. Ethvert samtykke, der er afgivet under trussel om, at den pågældende ikke vil blive behandlet eller få en dårligere behandling, kan ikke anses for at være “frivillig”. Gruppen anførte videre:

“... det er vildledende, hvis en erhvervsudøvende i sundhedssektoren, der er nødt til at behandle personoplysninger i et EPJ-system ... forsøger at begrunde dette under henvisning til patientens samtykke. Anvendelsen af samtykke skal begrænses til de tilfælde, hvor patienten har et reelt valg og som følge heraf uden at lide skade kan trække sit samtykke tilbage.”

I den danske betænkning om databeskyttelsesforordningen kobles frivillighed, betragtning 42 og 43 og artikel 7, stk. 4 til hinanden. Af artikel 7, stk. 4, fremgår, at der ved vurdering af, om samtykke er givet frit, tages der størst muligt hensyn til, bl.a. om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af denne kontrakt. I betænkningen anføres herom:

“Netop det faktum, at artikel 7, stk. 4, indeholder ordet bl.a. vil bevirke, at bestemmelsen i praksis vil kunne få betydning i en række forskellige situationer, hvor der kan siges at være en klar skævhed mellem den registrerede og den dataansvarlige. Det er vanskeligt at fastlægge rækkevidden af denne bestemmelse på forhånd, og bestemmelsen vil utvivlsomt blive udviklet gennem praksis i de kommende år. Det fremgår som nævnt af artikel 7, stk. 4, at der skal tages størst muligt hensyn. Der ses derfor ikke at være tale om en absolut bestemmelse, som ikke vil kunne fraviges. Bestemmelsen må fastlægge et fortolkningsprincip om størst mulig hensyntagen til “skævheder” ved vurderingen af samtykkets gyldighed.”

EU-Domstolen har vurderet spørgsmålet om frivillighed i Michael Schwarts, [Sag C-291/12](#), om afgivelse af fingeraftryk til pas. Præmis 31-32 lyder som følger:

“31. Det fremgår af chartrets artikel 8, stk. 2, at personoplysninger kun kan behandles på grundlag af den berørte persons samtykke eller på et andet berettiget ved lov fastsat grundlag.

32. Hvad dernæst angår betingelsen om pasansøgeres samtykke til optagelse af deres fingeraftryk bemærkes, at det generelt er nødvendigt for EU-borgere at besidde et pas, bl.a. for at kunne rejse til tredjelande, og at dette dokument skal indeholde fingeraftryk, jf. artikel 1, stk. 2, i forordning nr. 2252/2004. EU-borgere, der ønsker at foretage sådanne rejser, kan derfor ikke frit modsætte sig behandlingen af deres fingeraftryk. Under disse omstændigheder kan pasansøgere ikke anses for at have samtykket til en sådan behandling.”

Opsummerende kan man roligt konkludere, at der skal udfoldes ikke-ubetydelige anstrengelser for at sikre, at et samtykke til behandling af personoplysninger ved brug af wearables faktisk er gyldigt som databeskyttelsesretligt behandlingsgrundlag efter databeskyttelsesforordningens artikel 9, stk. 1, litra a. Anbefalingen herfra lyder derfor, at samtykke alene betragtes som en proportionalitetsforanstaltning – og det dermed sikres, at en anden behandlingsbetingelse er opfyldt.

Mest relevant er her artikel 9, stk. 2, litra h. Som beskrevet ovenfor, giver denne bestemmelse mulighed for, at behandling foretages af en person underlagt tavshedspligt og er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til ... medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson. Det giver en rimelig ramme for at bruge wearables – selvom sundhedsinstanser naturligvis skal være opmærksomme på de øvrige udfordringer, der er påpeget ovenfor, herunder kravet om dataminimering.