

# Etik og sundheds- data

En udtalelse fra Det Ethiske Råd



**DET  
ETISKE  
RÅD**



En **WEARABLE** er en måler, vi bærer på os, og som registrerer data om os. Mobiltelefoner, skridttællere, smartwatches mm, er eksempler på wearables.

Wearables indsamler data om brugerens **adfærd**: motion, søvn, spisevaner, psykiske velbefindende mm.

Eller om vedkommendes **fysiologi**, dvs. blodtryk, puls, stofskifte mm.

# Det etiske dilemma ved big sundhedsdata

**W**earables og de data, de indsamler, ser ud til at komme til at spille en positiv og nødvendig rolle. Både i forhold til:

- en omstilling og fornyelse af sundhedsvæsenet, og
- forbedre forebyggelse og behandling

Samtidig opsamler wearables store mængder persondata. Data som kan kombineres ved hjælp af kunstig intelligens og danne profiler, som går tæt på den enkelte. Det er derfor vigtigt, at vi som samfund forholder os til, hvordan disse data indsamles og anvendes, således at vores privathed ikke sættes under pres og begrænser vores grundlæggende frihed og selvbestemmelse.

## **Det Etiske Råd har taget stilling til 4 områder, hvor udviklingen rejser etiske dilemmaer:**

**1. Apps og wearables**, som er udviklet af private firmaer, opsamler data om os, og nogle firmaer sælger dem som en vare. Der kan også være problemer med kvaliteten af nogle apps.

*På side 16 tager rådet stilling til, om sundhedsvæsenet bør anvende apps udviklet af private firmaer.*

**2. Når en app er gratis**, er det dig – eller rettere dine data – som er betalingen.

*På side 18 tager rådet stilling til, om der bør eksistere et alternativ til at betale med sine data.*

**3. Hvis wearable-data fra sundhedsvæsenet kan samkøres** med data fra fx socialforvaltningen, skatteforvaltningen, politiet mm, håber man at kunne bruge kunstig intelligens til at forudsige, hvem der risikerer at blive syge i fremtiden.

*På side 20 tager rådet stilling til, om sundhedsvæsenet bør kunne samkøre borgernes data fra forskellige forvaltninger for at advare borgerne, hvis de ser ud til at være ved at udvikle sygdomme.*

**4. Også private firmaer forsøger at bruge persondata** til at forudsige sygdomme. Det er et nyt felt, så forudsigelserne er ofte eksperimentelle. Forsikrings-selskaber og arbejdsgivere er blandt dem, der formentlig gerne ville have adgang til sådanne forudsigelser.

*På side 22 tager rådet stilling til forsikrings-selskabers og arbejdsgiveres anvendelse af den type forudsigelser om sygdomme, når de tilbyder forsikringsbetingelser eller skal ansætte medarbejdere.*



## BIG DATA

Data er "Big" på to måder:

For det første mængden af digitale data, som opsamles om hver enkelt fra hele *The internet of things*, og især fra mobiltelefoner og computere.

For det andet omfanget af analyser, man kan lave med kunstig intelligens. Analyser som kan give detaljerede og meget private informationer om en person.

### Store fordele for sundhedsvæsenet

Wearables gør det muligt at opsamle en mængde data, som kan bruges til at udvikle bedre sygdomsbehandlinger. Behandlingerne kan ofte skræddersys til den enkelte person.

Patienten kan selv registrere data om sin sygdom og sende den til lægen, så han undgår besøg på hospitalet. Og på sigt kan man måske med sammenkøring af forskellige data opdage tidlige tegn på sygdom, så udbrud kan forebygges.

Motionsure, apps på mobiltelefoner og andre devices opsamler en strøm af data. Nogle udbydere lagrer og gemmer alle data – men ikke altid i motionsuret eller på telefonen; de kan gemmes på udbyderens server. Når man downloader en app, accepterer man nogle betingelser – formentlig uden at bruge tid på at læse dem. Men ofte står der, at man giver app-udbyderen ret til at anvende ens data til en hel række formål.

### Hvordan man får meget private oplysninger fra ret uskyldige data

Hver enkelt information, fx fra en motionsapp, siger ikke ret meget om den person, den stammer fra. Det nye er, at digitale persondata fra mængder

af meget forskellige kilder kan sammenkøres; fx data fra motionsapps, data om hvilke sider, man besøger på internettet, hvilke varer man køber, ens likes og venner på sociale medier, de sygdomme, man googler osv, osv. Med kunstig intelligens kan firmaerne finde mønstre i alle de spredte og hver især uskyldige data om os.

Algoritmerne kan forvandle ret ligegyldige informationer til meget private og personfølsomme informationer. Firmaer som Google, Facebook, Apple, Amazon og en række andre firmaer laver profiler om os, ofte uden at vi er klar over det. Men formentlig accepterede vi, at de gør det, da vi sagde 'ja' til de lange betingelser, vi ikke lige fik læst, da vi downloadede programmet eller købte app'en.

### **Ingenting er gratis**

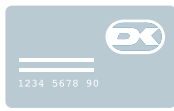
Siden internettets barndom har vi vænnet os til, at tjenester på nettet er gratis, fordi udvikleren kan tjene penge ved at sælge annoncer. Ved at bearbejde de digitale data, firmaer får adgang til om deres brugere, kan de opdele brugerne i livsstilsgrupper. Dermed kan de tilbyde annoncørerne at målrette deres markedsføring til præcis de forbrugere, som kunne være interesserede i deres produkt.



## **PROFILERING**

**Med de rigtige algoritmer kan spredte informationer tilsammen give et endda meget præcist billede af, hvem vi er:** hvilken type personlighed, om man har nogen sygdomme – eller måske er i fare for at udvikle sygdomme i fremtiden, ens seksuelle orientering, etnicitet, politiske synspunkter, religion, personlighed, intelligens, køn, alder, hvor mange venner man har mm.





## I PERSONPROFILER INDGÅR:

- **Oplyste data:** som personen har oplyst – fx motionsdata, kontonummer, adresse mmm
- **Observerede data:** som er registreret ved at følge personens aktiviteter både on-line og off-line. Det kan fx være data om søgninger efter bestemte sygdomme på nettet, antal venner på facebook, indkøb på nettet – og i butikker mmm
- **Udledte data:** fremkommet ved at analysere forskellige data om personen og nå frem til antagelser eller forudsigelser om vedkommende (fx at vedkommende er ved at udvikle en sygdom, er homoseksuel, hvad vedkommende interesserer sig for mmm)

Personprofiler, som fx siger noget om en persons interesser, er værdifulde for annoncører, som gerne vil betale firmaet for oplysningerne, så de kan rette deres bannerannoncer mod dem, der kunne være interesserede i dem. Mange kunne være interesserede i at købe oplysninger om en persons risiko for sygdom – fx forsikringsselskaber, arbejdsgivere, banker, kreditforeninger mm.

### Behov for bedre beskyttelse af sundhedsdata

Sundhedsdata er følsomme personoplysninger, derfor har sundhedsvæsenet bygget sikkerhedssystemer omkring den elektroniske patientjournal, som begrænser, hvem der har adgang til patientens data. Patienten har normalt ret til at få udleveret en kopi af sine data.

Anderledes med IT-verdenen. Her er data om personer – fx deres sundhedsdata – en vare, som kan købes og sælges.

Når firmaerne opsamler sundhedsdata om personer, eller laver personprofiler, som knytter sygdom eller risiko for sygdom til personer, kan vores sundhedsoplysninger fremover blive spredt på måder, som vi ikke selv har mulighed for at kontrollere eller følge med i.

Er det etisk problematisk, hvis andre kan få adgang til vores sundhedsdata?

Eller hvis vi må opgive tanken om at kunne holde nogle informationer om os selv private i det hele taget?

Og hvorfor er det egentlig et problem?



## DATA KAN SAGTENS VÆRE FORKERTE

Der er mange muligheder for fejl, både i de af vores data, som opsamles, og i dem der udregnes af kunstig intelligens. Kilder til fejl kan fx være:

- Mange apps måler ikke nøjagtigt nok, fx måler forskellige skridttællere forskellige antal skridt på samme afstand
- Der kan være tale om snyd – patienten kan få hunden til at gå rundt med skridttælleren og selv slappe af
- Der kan være fejl i algoritmerne – fx at de inddrager data fra en forkert patient
- Der kan være såkaldt bias hos den, der lavede algoritmen, så vedkommendes fordomme eller uvidenhed ubevidst er bygget ind i algoritmen

# Hvor og hvordan opsamles data?

Firmaer får deres betaling gennem salg af data som opsamles fra wearables, mobiltelefon-apps (som enten selv registrerer – eller brugeren indtaster – data om kost, motion, søvn, tanker, bevægelser (gps)), computere (sociale media posts, søgninger, browserhistorie, mails, internethandel, hastighed af tastning, ordvalg), dankortkøb, elforbrug, data fra the internet of things (biler, tv, køleskabe osv) mmm.

Vi trykker accept, accept, accept...







Firmaer lokaliserer personers identiteter via e-mailadresser, telefonnumre, ID'er fra smartphones, computere og brugerkonti, og følger dem på tværs af forskellige tjenester, platforme og devices.





## PROFILERING INC.

Der skal forbavsende få informationer til, før man kan give et vældigt præcist billede af en person. Kun fem egenskaber kan udlede, hvor personen er placeret på de fleste kendte karaktertræk (Fem-faktor modellen). Disse egenskaber kan udledes ud fra Facebook-likes, men også fra andre tilgængelige data som web-søgninger, browserhistorie, kreditkortkøb mm.



Ved hjælp af algoritmer udleder aktører personfølsomme oplysninger som:

- Sygdomsdispositioner
- Seksuel orientering
- Etnicitet
- Politiske synspunkter
- Religion
- Personlighed
- Intelligens
- Køn
- Alder
- Antal venner  
mmm.



Mange aktører køber og sælger data om personer, helt overvejende uden at personen selv er klar over, at deres data handles og behandles.

# Hvordan laves person- profiler og hvordan videregives og sælges de?

Der er allerede firmaer, som sælger data om folk, de har analyseret sig frem til har – eller er i risiko for at få – sygdomme.



## Jens Jensen

Køn: Mand

Alder: 37 år

Status: Gift

Børn: 2

Uddannelse: Mellemlang

Beskæftigelse: Mekaniker

Etnicitet: Nordisk

Religion: Protestant  
(ikke udøvende)

Sexualpreference: Bisexuel

Interesser: Fodbold,  
bøger, biler

Sygdomme: Astma, tinitus,  
disposition for diabetes,  
depression.

# Hvorfor er privathed værdifuldt?

En persons seksuelle præferencer kan udledes af deres indkøbsmønster. Hastigheden af klik med computermusen kan afsløre, at en person er ved at udvikle Alzheimer's sygdom eller depression.

Med tech-firmaernes salg af personprofiler om os alle må vi indse, at vores privathed er under pres.

– Er det et etisk problem?

For at kunne svare på det, er det nødvendigt at se på, hvorfor vi betragter det at have et privatliv som så vigtigt, at det er skrevet ind i Menneskerettighedskonventionen og mange andre traktater.

Et bud er, at privatliv i virkeligheden er vigtigt, fordi det beskytter noget meget grundlæggende: Det beskytter vores frihed til at kunne leve i overensstemmelse med vores egne ønsker til et godt liv uden at blive diskrimineret eller set skævt til.

## **Privatlivet beskytter mod misbilligelse og diskrimination**

Nogle oplysninger om os ønsker vi ikke at dele med alle, fordi ikke alle vil billige dem, og nogen vil måske decideret bruge dem til at skade eller diskriminere os.

En person kunne fx frygte, at kollegerne på arbejdspladsen ville se skævt til ham, hvis de kendte hans politiske overbevisning.

Fordi homoseksuelle gennem historien er blevet diskrimineret mod, kan de i nogle sammenhænge ønske at holde den information for sig selv.

Og i nogle tilfælde kan oplysninger om, at man har en risiko for at udvikle en sygdom, gøre, at man bliver diskrimineret og fravalgt på arbejdsmarkedet.

Nogle informationer ønsker vi derfor at holde private for at være fri til at vælge, hvordan vi vil leve, uden at udsættes for andres misbilligelse eller diskrimination.

Retten til privatliv beskytter muligheden for selv at kontrollere, hvem der skal vide hvad om mig. Til at vurdere, om nogen kunne finde på at bruge en information til at skade mig, så jeg derfor ikke vil lade dem få informationen.

## **Overvågning**

Dataindsamlingen bliver ofte sammenlignet med overvågning, fordi nogen følger med i vores handlinger ved at registrere vores digitale fodspor.

På den måde får de informationer om os, som de i værste fald kan bruge til at styre, kontrollere eller skade os.

Alene muligheden for, at man bliver overvåget, kan gøre, at man ændrer adfærd. Måske tør man ikke længere google en sygdom af frygt for, at den information havner i en personprofil og bliver tolket som en oplysning om, at man har eller er ved at udvikle sygdommen. Frygten kan gøre, at man ikke længere er fri til at gøre ting, man ikke ønsker, at andre skal se. Dermed kan alene frygten for overvågning gøre, at man mister en del af sin frihed.

### **Fortrolighedsrum**

I nogle sammenhænge kan mennesker have brug for at vide, at data ikke bliver videregivet, og måske brugt mod vedkommende eller blot læst i et andet lys. Det kan fx være relationen til lægen eller andre sundhedspersoner, hvor patienten kan frygte, at kommunens kontrolgruppe for socialt bedrageri vil læse oplysningerne fra wearables anderledes end de sundhedsprofessionelle. Men også de apps, der fx giver mulighed for at dele oplysninger på Facebook om ens måltider (i håb om vennernes likes og kommentarer), kan miste deres motiverende effekt,

hvis de fx anvendes af et forsikringselskab til at sætte prisen på forsikringen op.

### **Hvornår opstår et etisk problem?**

Hvis man siger, at retten til privatliv er vigtig for at beskytte én mod diskrimination eller skade fra omgivelserne, så er det jo ikke alle sundhedsinformationer, det vil være et etisk problem at dele. Hvis man fx går rundt på krykker med benet i gips, er det ikke et problem, at folk på gaden får den sundhedsoplysning, at man har brækket benet. Det er svært at se, at det skulle skade én, at alle får den information.

**Det etiske problem opstår der, hvor data om en person kan anvendes til skade for personen. Det vil sige hvis myndigheder eller virksomheder kan få adgang til data om personer, der gør dem i stand til gribe ind i disse personers liv på begrænsende måder.**

I anbefalingerne tager rådet 4 områder op, hvor adgang til personers sundhedsdata kan give etiske problemer.

# Hvilken beskyttelse giver loven?

**E**U's databeskyttelsesforordning (GDPR) fra maj 2018 er verdens mest ambitiøse forsøg på at beskytte personers data. Men hvorfor forhindrer den så ikke, at vores data opsamles og bruges til profilering?

Svaret er i høj grad de samtykker, vi giver, når vi downloader en app eller tager et digitalt redskab, som en mobiltelefon eller et el-løbehjul, i brug.

**Når firmaer opsamler data**, beder de oftest først om samtykke til at gøre det. Men det er almindeligt anerkendt, at de allerfærreste faktisk tager sig tid til at læse de betingelser, man samtykker til. Hvis man gjorde, ville man formentlig opdage, at man meget ofte siger ja til, at firmaet høster, bearbejder og deler virkeligt mange data om én. Der er næppe nogen tvivl om, at opsamling af data har et uendeligt meget større omfang, end den enkelte kan forestille sig.

Data-forordningen har nogle grundprincipper, som er:

- Det skal være klart, hvilke formål indsamlede data bruges til; fx opsamler en motionsapp data om, hvor meget man motionerer

- Anvendelsen må ikke være uforenelig med det oprindelige formål; fx bør data fra en motionsapp ikke altid anvendes til at regne på, hvilke sygdomme man vil få senere i livet
- Der må ikke indsamles flere oplysninger end nødvendigt til formålet; fx bør motionsapp'en ikke få adgang til ens facebook-kontakter
- Oplysninger skal slettes eller anonymiseres, når de ikke længere er nødvendige; de skal ikke gemmes og kombineres med andre data mhp. senere, endnu ikke planlagt, profilering

Firmaet har altså mulighed for at kræve samtykke til nogle betingelser for at give lov til at bruge deres app eller device. Her kan de til tider formulere deres formål med databehandling så bredt, at de får samtykke til en meget bred indsamling af information om brugerens adfærd og præferencer.

Brugeren kan naturligvis sige nej til alle disse samtykkekrav, men i realiteten vil det være svært at fungere i det moderne samfund, hvis man gør dette særligt ofte. Vi er meget afhængige af digitale tjenester, og ofte er der ikke et alternativ, som synes acceptabelt.

Spørgsmålet er, om forordningen skal fortolkes sådan, at det forsat skal være muligt at bede brugeren acceptere sådanne brede samtykker? Dette vil vi først få fuld klarhed over, når der er ført nogle retssager, som fastlægger den endelige fortolkning af reguleringen.

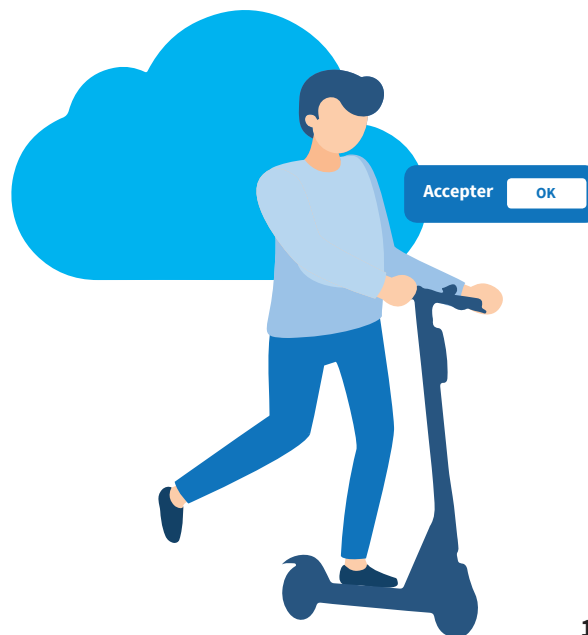
**I sundhedsvæsenet** opsamles data, fx blodprøver, røntgenbilleder mm, med det formål at behandle patienten, og det kræver ikke specifikt samtykke. Data kan kun gives videre til andre formål, hvis de ikke er uforenelige med det oprindelige – altså behandling af patienten.

Alle data om patienten samles i den elektroniske journal, som er beskyttet mod adgang fra andre end patienten og vedkommendes behandlere. Patienten har ret til at se de data, der findes om ham i den elektroniske patientjournal. Nogle systemer giver desuden mulighed for at følge med i, hvordan ens data anvendes.

Forordningen tillader sundhedsvæsenet at give data videre til andre offentlige myndigheder, fx en kommune der ønsker at bruge data til at levere genoptræning til en borger. Hvis det sker, har kommunen som udgangspunkt pligt til at oplyse

patienten om, at man nu behandler vedkommendes data.

Hvis sundhedsvæsenet eller kommunen senere vil bruge disse data til at forudse fremtidig sygdom, kan de som udgangspunkt gøre det. Som hovedregel skal borgeren dog gøres opmærksom på, at det vil ske. Der er dog undtagelser. Bla giver den danske databeskyttelseslov myndighederne lov til at udstede en bekendtgørelse, som giver tilladelse til at bruge dataene til de nye formål uden at orientere borgeren om det.



# Anbefalinger

Det Etiske Råd peger på 4 områder, hvor der er behov for at stramme op på beskyttelse og anvendelse af sundhedsdata.

## 1 Bør sundhedsvæsenet anvende apps udviklet af kommercielle udbydere?

Data fra wearables, fx motions- og sundhedsapps, som måler motion, søvn, kost- og medicinindtag, stressniveau, psykiske tilstande mmm, vil kunne anvendes i sundhedsvæsenet. De kan supplere de data, lægen allerede har fra diverse test og samtaler med os, og tilsammen kan de give et mere komplet billede af os, så vi kan få en bedre og mere personrettet behandling. De kan også anvendes til at få større viden om sygdomme og udvikle bedre behandlinger.

Men apps er kostbare at udvikle, så lægen vil i mange tilfælde kunne anbefale patienten at bruge en app, som er udviklet af et privat firma. Firmaet vil så ofte gemme patientens data på deres egne servere.

Hvis der er tale om en gratis app, som kræver samtykke til, at udbyderen må bruge éns data til profilering og salg, opstår der et problem. For på den måde medvirker sundhedsvæsenet til, at

endnu flere data om patienten opsamles og vil kunne anvendes til helt andre formål end sygdomsbehandling.

Desuden er der spørgsmålet om app'ens kvalitet; der er mange apps på markedet, og en meget stor del er ikke lavet af fagfolk og ikke godkendt til medicinsk brug eller kvalitetstestede.

Så bør sundhedsvæsenet kun bruge apps, de selv har udviklet?

**Flertallet i Det Etiske Råd anbefaler**, at sundhedsvæsenet også bør kunne anbefale wearables fra kommercielle firmaer til patienterne og tage imod data, som patienten selv indsamler på dem. Det vil ikke være muligt for sundhedsvæsenet at finde ressourcer til selv at udvikle særligt mange apps, og man vil også ofte mangle medarbejdere med de relevante kompetencer i forhold til at udvikle apps. Derfor vil et forbud mod at bruge apps udviklet af andre gå ud over behandlingen. Apps fra private firmaer bør dog kun anvendes på betingelse af, at:

- Det er muligt at lagre de data, app'en indsamler, i den elektroniske patientjournal udover på firmaets server



- Alle apps og enheder, der anvendes i sundhedsvæsenet, bør sikkerhedsgodkendes. Der bør udvikles en europæisk certificeringsordning, og indtil den er klar, kan man anvende standarder fra den amerikanske lægemiddelmyndighed, FDA

Certificeringen bør også angive, om app'en opsamler flere informationer om personen end nødvendigt. Samt om de sletter oplysningerne efter brug, eller om de tværtimod sælger dem videre til andre firmaer

**Et mindretal i rådet** anbefaler dog, at sundhedsvæsenet kun bør anvende egne apps til opsamling af sundhedsdata om patienterne. På den måde kan man både sikre kvaliteten af de apps, man opfordrer patienterne til at bruge, og forhindre at patientens data havner på kommercielle firmaers servere og bruges på måder, som senere kan skade patienten.

Sundhedsvæsenet bør dog også kunne gå i partnerskab med kommercielle firmaer, som kan udvikle apps til dem. Men firmaet skal dokumentere, at deres apps er sikre og pålidelige, og de data, som indsamles, må kun lagres i på sundhedsvæsenet sikre servere.



## 2 Der bør eksistere et alternativ til at betale med sine data

Når en sundhedsapp eller andre digitale tjenester er gratis at downloade, skyldes det som nævnt, at vi betaler med vores data. Der er skabt en kultur, hvor vi automatisk siger 'accept' til nogle betingelser, vi ikke har tid til at læse – og dermed giver lov til en langt mere omfattende brug af vores data, end vi gør os klart.

**Et stort flertal i Det Ethiske Råd anbefaler**, at der bør tages et opgør med gratis-princippet, som betyder, at apps og andre tjenester stilles gratis til rådighed mod, at udbyderen får adgang til brugerens data. Det bør som minimum altid være muligt at vælge at betale et beløb for at få adgang til en app, i stedet for at udbyderen får ret til at anvende vores data til profilering og salg.

Det må aldrig være en betingelse for at få adgang til en app eller en webtjeneste, at man accepterer, at udbyderen opsamler og anvender ens data. Man må ikke nægtes adgang til en app eller en hjemmeside pga manglende samtykke, og brugeren skal oplyses om, at samtykke ikke er en betingelse for at få adgang.

Samtidig bør der sættes massivt ind på at informere befolkningen om den omfattende profilering, som foregår, og om de reelle omkostninger ved at afgive samtykker til opsamling af personlige data.

Den nuværende opsamling og profilering af personer kan bla anvendes til at fremanalysere mere eller mindre korrekte data om vores helbred og sygdomsdispositioner.

Profileringen kan gøre os gennemsigtige og underminere vores ret til privatliv. Men respekten for privatlivet er afgørende for friheden til at leve efter egne værdier. Den er en beskyttelse mod misbilligelse, diskrimination og overvågning fra andre mennesker, myndigheder og firmaer. Derfor udgør traditionen for at betale med sine data for at få adgang til en wearable eller anden digital tjeneste et alvorligt problem, som det er nødvendigt at tage et opgør med.

**Et medlem** mener ikke, det er *opsamlingen* af data i sig selv, som begrænser personers frihed. Derfor er det ikke *opsamlingen*, man bør sætte ind overfor. Det er de *anvendelser* af data, som faktisk tillader virksomheder og offentlige myndigheder at gribe ind i personernes liv på kontrollerende måder.

Hvis der ikke er tale om personfølsomme oplysninger, er der ikke noget galt i, at personer samtykker til brug af deres data. Hvis et firma får data om fx en persons motionsvaner og anvender dem til at sørge for, at personen ser bannerreklamer for løbeudstyr, er det ikke et problem. Motionsvaner er ikke personfølsomme data, og reklamen begrænser ikke personens frihed.

Derfor skal man sætte ind i de tilfælde, hvor nogen bruger sundhedsdata på måder, der skader den, de kommer fra, så de udsættes for misbilligelse, diskrimination eller overvågning. Hvis myndigheder eller firmaer anvender data på denne måde, bør der sættes ind, som de næste anbefalinger peger på.



### 3 Sundhedsvæsenet og andre myndigheder bør kun kunne bruge data til at forudsige sygdomme på visse betingelser

Data opsamlet med wearables kan anvendes til såkaldt *predictive medicine*, hvor målet er at finde tidlige tegn på sygdom, så man kan forebygge, at den bryder ud.

Man forsker i at bruge kunstig intelligens til at analysere data om patienten fra sundhedsvæsenet – både data fra wearables og andre sundhedsdata – sammen med data fra andre myndigheder som socialforvaltning, politi, skat, forsyningsvirksomheder mm.

Forventningen er, at når man kombinerer disse forskellige data, vil man finde mønstre, som kan sige noget om personens risiko for at blive indlagt akut eller for at udvikle sygdomme i fremtiden. Tanken er, at man på den måde kan spare borgeren for at blive syg, fordi man kan opsøge ham med råd om, hvordan han kan undgå at udvikle en truende sygdom. Desuden kan man spare udgifter i sundhedsvæsenet, hvis man kan forhindre folk i at blive syge.

Skeptikere peger på, at man i mange tilfælde ikke kan forebygge sygdomme ved at ændre levevis. Desuden

er det ofte miljøet – der hvor man bor eller hvor man arbejder – som gør én syg, og de forhold kan være svære at ændre.

Der opstår flere etiske overvejelser, som rådet har taget stilling til:

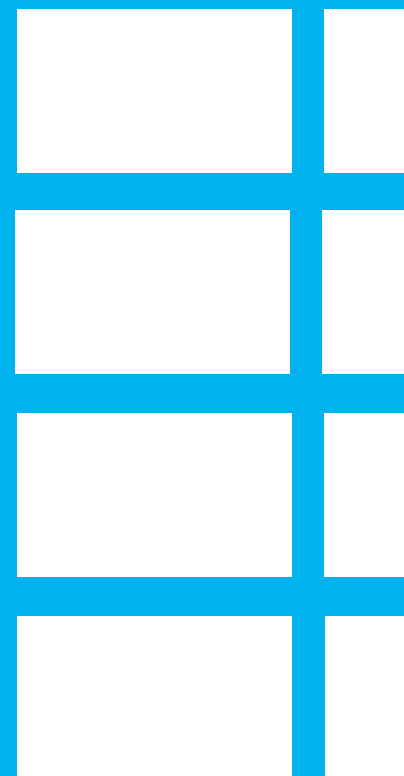
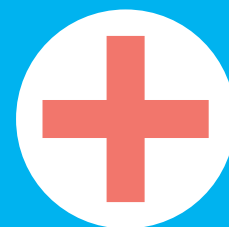
#### **Det Etiske Råd anbefaler, at en række betingelser skal være opfyldt, før data fra wearables kan samkøres med data fra andre myndigheder mhp sygdomsforebyggelse:**

- Borgeren skal altid **informeres** om, at deres data vil blive sammenkørt og analyseret, og man skal have mulighed for at sige 'nej tak' til at deltage
  - Nogle af medlemmerne mener ikke, det er nok at få lejlighed til at sige nej – myndighederne må ikke starte på at sammenkøre data, hvis de ikke har fået samtykke fra borgeren til at gøre det
- Alle data om borgeren skal **opbevares sikkert** ligesom andre sundhedsdata. Borgeren skal have adgang til de data, man analyserer sig frem til om ham, samme sted, som han har adgang til sine sundhedsoplysninger

- Der skal tages højde for det **dilemma**, at nogle mennesker foretrækker at leve i uvidenhed om fremtidige sygdomsdispositioner, og de har en **ret til ikke-viden** om dem. Andre vil gerne have oplysningen, især hvis der er mulighed for at forebygge, at sygdommen opstår, og disse borgere har **ret til at til at kende alle oplysninger**, som er indsamlet om deres helbred

For at imødekomme begge grupper, bør borgeren på forhånd have mulighed for at til- eller framelde sig at modtage henvendelser, hvis dataanalyser viser, at de har en risiko for at udvikle sygdom i fremtiden

- **Respekt for borgerens frihed til at vælge sin egen livsstil:** Gode råd til borgeren om at ændre livsstil for at nedsætte risikoen for at blive syg bør udelukkende have karakter af tilbud. Hvis det giver borgeren stor livskvalitet her og nu at leve, som man plejer, bør man have sin frihed til at gøre det, uden at man fx bliver sat bagud i behandlingsskøen af den grund.



## 4 Forsikring og arbejdsgivere bør ikke anvende sundhedsdata, som er blevet til ved sammenkøring af data

Personprofiler kan bla give – mere eller mindre pålidelige – data om, hvilke sygdomme vi har, og hvilke vi er i risiko for at få i fremtiden. Nogle forsikrings-selskaber og arbejdsgivere kunne være interesserede i at få adgang til den type sundhedsoplysninger, så de kan bruge dem til at skræddersy forsikringstilbud eller vælge de sundeste medarbejdere.

**Et stort flertal i Det Ethiske Råd anbefaler**, at hverken forsikringsselskaber eller arbejdsgivere bør kunne anvende sundhedsdata, som er analyseret frem ved at sammenkøre data fra wearables med andre digitale data.

For det første er der indtil videre tale om **meget usikre data**. Men selv hvis man bliver bedre til at lave forudsigelser om fremtidig sygdom, vil der næsten altid kun være tale om, at man har en større *sandsynlighed* for at udvikle en sygdom, end andre har. Men det er ikke sikkert, at man får sygdommen, derfor vil det være uretfærdigt, hvis man får afslag på et job eller skal betale mere for sin forsikring, selvom sygdommen måske aldrig kommer til at bryde ud.

Hvis man lader forsikringspræmier eller ansættelser være påvirket af analyser, som hævder at kunne vise en persons risiko for at få en sygdom i fremtiden, ville det på mange måder **ramme de svagest stillede**.

- Hvis man er i risiko for at udvikle en sygdom, er man allerede dårligere stillet end andre. Derfor bør man ikke straffes yderligere ved at få en dyrere forsikring eller blive forbigået til de job, man søger
- Måske er det ens levevis, som har fået algoritmen til at anse én for at være i risiko for at få en sygdom. Her kan man se, at der er flere blandt de dårligst stillede, som har en mindre sund levevis. Men det kan være svært at bryde med fx de spise- og motionsvaner, man er vokset op med. Hvis man lader forsikringspræmier eller ansættelser afhænge af sund levevis, vil man derfor også ende med at straffe de dårligst stillede hårdest

Endelig finder disse medlemmer grundlæggende, at vi bør værne om **friheden** til selv at vælge, hvordan vi vil leve. Det skal være muligt at vælge at leve lidt mindre sundt, hvis det giver én stor livskvalitet, vel vidende at det kan koste nogle leveår i den anden ende. Forsikringspræmier eller jobmuligheder bør

ikke anvendes til at presse alle til at leve på samme måde, selv om det er mere sundt.

**Et medlem ønsker ikke at komme med anbefalinger på nuværende tidspunkt.** Det skyldes, at hun grundlæggende ikke synes, det er problematisk, hvis forsikringsselskaber og arbejdsgivere – med borgerens tilladelse – anvender data fra en persons wearables eller anvender sundhedsdata, som algoritmer har analyseret sig frem til, ved at kombinere en mængde data om personen. Den type data kan jo nogle gange anvendes til den enkeltes fordel – hvis det er pålidelige data.

På nuværende tidspunkt er der dog grund til bekymring for kvaliteten af de sundhedsdata, som kommer ved at sammenkøre data fra wearables med data fra mange andre kilder. Mange af forudsigelserne må på nuværende tidspunkt anses for at være eksperimentelle og ikke baserer sig på forskning, som viser deres pålidelighed.

Det kan derfor give anledning til bekymring, hvis forsikringsselskaber og arbejdsgivere anvender sundhedsdata, som er blevet til ved datasamkøring, før der er langt bedre erfaring for, at man faktisk er i stand til at levere pålidelige forudsigelser.

## **Etik og sundhedsdata**

### **En udtalelse fra Det Ethiske Råd**

© Det Ethiske Råd 2019

ISBN: 978-87-92915-20-7

Tekst: Anne Lykkeskov

Grafisk design og illustrationer: Peter Waldorph

Tryk: Rosendahls

## **DET ETISKE RÅD**

[kontakt@etiskraad.dk](mailto:kontakt@etiskraad.dk)

Tel: +45 72 21 68 70

[etiskraad.dk](http://etiskraad.dk)

**Er det etisk problematisk, hvis andre kan få adgang til vores digitale sundhedsdata?**

**Eller hvis vi må opgive tanken om at kunne holde nogle informationer om os selv private i det hele taget?**

**Det Ethiske Råd finder, at big data kan bidrage til bedre behandling og forebyggelse, hvis vi opsætter regler for de situationer, hvor etiske problemer kan opstå.**

**Det kan de, hvis data om en person anvendes til skade for personen. Det vil sige hvis myndigheder eller virksomheder kan få adgang til data om personer, der gør dem i stand til gribe ind i disse personers liv på begrænsende måder.**



**DET  
ETISKE  
RÅD**