Sundheds- og Ældreudvalget 2017-18
L 146 endeligt svar på spørgsmål 15
Offentligt

SUNDHEDS- OG ÆLDREMINISTERIET

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Dato: 13-04-2018
Enhed: SPOLD
Sagsbeh.: DEPPADL
Sagsnr.: 1707223
Dok. nr.: 560290

Folketingets Sundheds- og Ældreudvalg har den 26. februar 2018 stillet følgende spørgsmål nr. 15 (L 146 – forslag til lov om ændring af sundhedsloven (Organiseringen i Sundheds- og Ældreministeriet, oprettelse af Nationalt Genom Center m.v.)) til sundhedsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Liselott Blixt (DF).

Spørgsmål nr. 15:
"Ministeren bedes oplyse, om danskeres genetiske oplysninger vil blive sendt til udlandet uden at der informeres om det. I bekræftende fald bedes ministeren oplyse, om der sker inspektion af databehandlerne i udlandet."

Svar:
Det er netop et af formålene med Nationalt Genom Center og opbygningen af en national infrastruktur til Personlig Medicin at nedbringe behovet for fysisk at sende oplysninger eller biologiske prøver til udlandet. Der arbejdes således på en løsning, hvor data ikke kan tages ud af systemet. Der vil blive arbejdet udelukkende med data i dertil dedikerede sikre analysemiljøer, hvorfra data ikke skal kunne downloades eller eksporteres.

Spørgsmålet om datasikkerhed er helt afgørende for Nationalt Genom Center, og det uddybes derfor nedenfor.

For at patientens data håndteres ansvarligt skal der oprettes et lukket system med højest mulig sikkerhed. Det betyder bl.a., at der skal være fuld kontrol over hvilke personer, der har adgang til oplysningerne. Der skal være automatiseret logning for at overvåge brugernes adgange og handlinger og potentielle risici. Der skal arbejdes med kryptering på alle niveauer i systemet. Det inkluderer bl.a. netværk og filsystemer.

Nationalt Genom Center skal, som beskrevet i *National Strategi for Personlig Medicin 2017-2020*, være med til at sikre det overordnede formål med Personlig Medicin, som er at kunne diagnosticere og klassificere sygdomme bedre, så behandlingen kan tilpasses den enkelte patient.

Data opbevares derfor på en måde, så man ikke direkte kan identificere den enkelte patient i databasen. Formålet betyder dog samtidigt, at man skal kunne gennemføre patientspecifikke analyser, hvilket inkluderer, at man skal kunne opbevare data til selve analyseafviklingen, og til eksempelvis patientens fremtidige behandlingsforløb, i en national genomdatabase. Det er derfor nødvendigt at kunne tilbageføre de opbevarede data til den patient, som data omhandler, for at kunne bruge det i behandlingen igen, når det er relevant.

Som anført i lovforslagets afsnit 2.1.5.2, så fremgår kravene til databeskyttelse bl.a. af databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, databeskyttelsesforordningens artikel 32

om behandlingssikkerhed og databeskyttelsesforordningens artikel 35 om konsekvensanalyse vedrørende databeskyttelse. Kravene skal tilpasses risikoen, og når der bl.a. samles store datamængder på dette område er risikoen, og dermed kravene, større.

Der er ikke fastlagt en endelig sikkerhedsmodel for den foreslåede oprettelse af Nationalt Genom Center. Som det fremgår af lovforslaget, vurderer Sundheds- og Ældreministeriet, at Nationalt Genom Center vil skulle foretage en konsekvensanalyse i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 35. Denne skal foretages forud for den endelige tilrettelæggelse af sikkerhedsløsningen. Som det i øvrigt fremgår af lovforslaget, vil sikkerhedsniveauet løbende skulle tilpasses de aktuelle risici.

Indretningen af sikkerhedsløsningen kan derfor ikke ses som en statisk model, men som et område, der løbende skal tilpasses, også for at imødegå nye sikkerhedstrusler. Desuden er det centralt at være opmærksom på, at en af årsagerne til, at der foreslås oprettet et Nationalt Genom Center er, at det giver mulighed for at indrette de nye systemer og sikkerhedsmodeller efter principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Det giver netop mulighed for at sikre, at der findes en løsning, hvor sikkerhed er et bærende element i modsætning til, hvis man alene videreanvender ældre løsninger, hvor sikkerhedsmodellen ikke har haft det primære fokus.

./. Den samlede løsning vil blive underlagt et meget højt sikkerhedsniveau. Sikkerheden for Nationalt Genom Center vil skulle opretholdes gennem en lang række initiativer. Løsningen vil blive baseret på internationale og nationale erfaringer på området. Løsningen kommer til at bygge på de nyeste teknologier og sikkerhedsparadigmer. Løsningen bliver således underlagt et allerede stærkt reguleret område. Det inkluderer fra maj 2018 EU's databeskyttelsesforordning, forslag til databeskyttelsesloven samt sundhedsloven. Derudover vil Nationalt Genom Center skulle følge internationale sikkerhedsstandarder. Desuden vil Nationalt Genom Center i samarbejde med Sundhedsdatastyrelsen løbende skulle følge udviklingen af forskellige sikkerhedsmodeller Ud over privatlivsbeskyttelse skal realiserbarhed i forhold til brugsscenarier, teknologimodenhed og leverandørafhængighed også vurderes. Endelig undersøges muligheden for at se på sikkerhedsmodeller fællesoffentligt. Der henvises i øvrigt til det uddybende notat i bilag om sikkerhed i forbindelse med etablering og drift af den fælles nationale teknologiske infrastruktur for Personlig Medicin.

Fsva. datastrømsanalyse skal det bemærkes, at det fremgår af betænkning nr. 1565 om databeskyttelsesforordningen, at forordningens artikel 30 om fortegnelser ikke i sig selv medfører et krav om større analyser af datastrømme m.v. Men Nationalt Genom Center vil som dataansvarlig naturligvis skulle føre en fortegnelse over behandlingsaktiviteter i centeret, jf. databeskyttelsesforordningens artikel 30.

Hvad angår spørgsmålet om overførsel af personoplysninger til udlandet kan følgende oplyses:

Nationalt Genom Center kan kun overføre personoplysninger til et land uden for EU – et såkaldt tredjeland – hvis Nationalt Genom Center har et lovligt grundlag for at behandle, herunder videregive, oplysningerne. Herudover skal Nationalt Genom Center sikre, at de særlige regler om overførsel af personoplysninger til tredjelande, dvs. lande uden for EU, i databeskyttelsesforordningens kapitel V iagttages.

Systemet vil dog teknisk betyde, at data ikke fysisk overføres til det andet land, men i stedet betyde, at det vil være muligt fra EU-lande og tredjelande at få kontrolleret adgang til data til fx forskning eller patientbehandling. Det vil ske på en måde, hvor data ikke tages ud af systemet og dermed ikke fysisk forlader Danmark.

Det skal dog bemærkes at begrebet "overførsel" juridisk også kan bestå af en såkaldt "se adgang". Det betyder, at selvom oplysningerne ikke fysisk forlader Danmark, så kan situationen være omfattet af reglerne om overførsel til tredjelande og kravene, der knytter sig hertil.

Med venlig hilsen

Ellen Trane Nørby / Anne-Sofie Duelund Lassesen

SUNDHEDS- OG ÆLDREMINISTERIET

NOTAT

Sikkerhed i forbindelse med etablering og drift af den fælles nationale teknologiske infrastruktur for Personlig Medicin

Personlig Medicin omfatter bl.a. brugen af genomdata til behandling af patienter og til forskningsformål. Disse data indeholder helbredsoplysninger og tilhører derfor følsomme personhenførbare sundhedsdata. Der kræves derfor et højt sikkerhedsniveau. Den fælles nationale teknologiske infrastruktur for Personlig Medicin, der skal understøtte genomsekventering og sikker anvendelse af disse data, skal derfor etableres og drives i overensstemmelse med de krav og retningslinjer, der er for håndtering af følsomme personhenførbare sundhedsdata.

Den fælles nationale teknologiske infrastruktur for Personlig Medicin indeholder bl.a. Den Nationale Genomdatabase, High Performance Computing-faciliteter (HPC-faciliteter), genomsekventeringsfaciliteter samt en tværgående teknisk infrastruktur på tværs af disse elementer.

Informationssikkerhed og fysisk sikkerhed skal leve op til gældende love og regler, herunder for nuværende Persondataloven og Sikkerhedsbekendtgørelsen og EU's databeskyttelsesdirektiv. Efter maj 2018 gælder databeskyttelsesforordningen fra EU og i tillæg hertil relevant national lovgivning samt nationale og regionale retningslinjer, vejledninger m.v.

Indeværende notat opsummerer de væsentligste elementer, som arbejdet med sikkerhed i forbindelse med etablering og drift af den fælles nationale teknologiske infrastruktur for Personlig Medicin baseres på:

1. Sundhedsloven og Vejledning om informationssikkerhed
2. EU's Databeskyttelsesforordningen (GDPR)
3. Privacy by Design (Data Protection by Design)
4. International standard til styring af informationssikkerhed
5. Internationale retningslinjer for fysisk sikkerhed

1. Sundhedsloven og Vejledning om informationssikkerhed i sundhedsvæsenet
Arbejdet med at etablere og efterfølgende drive den fælles nationale teknologiske infrastruktur for Personlig Medicin, skal ske inden for rammerne af de principper og retningslinjer vedr. håndtering af følsomme personhenførbare sundhedsdata, der er fastlagt i Sundhedsloven.

Sundhedsdatastyrelsens Vejledning om informationssikkerhed i sundhedsvæsenet (2016) konkretiserer derudover, hvordan dansk lovgivning – herunder Sundhedsloven – skal fortolkes, og kommer med forslag til, hvordan gældende krav og regler samt best practise kan implementeres og efterleves i dette regi.

En central del af arbejdet med sikkerhed omkring den fælles nationale teknologiske infrastruktur for Personlig Medicin baseres derfor både på Sundhedsloven og på yderligere detaljer i Vejledningen om informationssikkerhed i sundhedsvæsenet.

2. EU's Databeskyttelsesforordning (GDPR) samt persondataloven og sikkerhedsbekendtgørelsen og anden relevant lovgivning
På nuværende tidspunkt er det især Persondataloven og tilhørende sikkerhedsbekendtgørelse, der regulerer spørgsmålet om databeskyttelse af personoplysninger i Danmark.

Fra maj 2018 vil det være EU's Databeskyttelsesforordning og tilhørende implementering i dansk lovgivning, herunder det fremsatte forslag til databeskyttelseslov og evt. yderligere relevant dansk lovgivning, der gælder på området.

Alle tekniske komponenter og aktører i samarbejdet om den fælles nationale teknologiske infrastruktur for Personlig Medicin udarbejdes i regi af, og er fremadrettet underlagt Databeskyttelsesforordningen.

Fra Justitsministerens side er der som fortolkningsbidrag udarbejdet en betænkning, der gennemgår konsekvenserne af Databeskyttelsesforordningen i forhold til den gældende retstilstand efter Persondataloven og Databeskyttelsesdirektivet. Krav og retningslinjer i Databeskyttelsesforordningen er endnu ikke indarbejdet i Vejledning om informationssikkerhed i sundhedsvæsenet og vil derfor skulle iagttages særskilt.

En række aktører vil på forskellig vis være involveret i den fælles nationale teknologiske infrastruktur for Personlig Medicin, for at arbejdet med at genomsekventere, analysere og fortolke resultater kan realiseres, og de vil tilsvarende på forskellig vis skulle anvende relateret data. Dette kan både inkludere leverandører af software, hardware og lign., klinikere der fortolker resultaterne, teknisk personale ansat af universiteterne, der vedligeholder HPC-faciliteterne (af GDPR benævnt 'controllers' og 'processors', og i dansk regi eksisterende retningslinjer for arbejdet omkring dataansvarlige og databehandlere).

Ved inddragelse af tredjepart vil arbejdet baseres på en struktureret tilgang til at minimere de risici der er forbundet med at inddrage en tredjepart. Som minimum skal tredjeparter overholde de samme retningslinjer og principper, som er opstillet i indeværende notat, men der kan være tilfælde, hvor kravene skærpes yderligere.

3. Databeskyttelse gennem design (Privacy/Data Protection by Design)
Princippet i Databeskyttelsesforordningen om 'Privacy by Design' er nyt i forhold til i dag. Det vil være dog være centralt for designet af den fælles nationale teknologiske infrastruktur for Personlig Medicin.

Som en del af den vedtagne Databeskyttelsesforordning (GDPR) arbejdes der under princippet 'Privacy by Design', som alle nuværende og fremadrettede løsninger og relaterede teknisk infrastruktur skal designes under. Det gælder derfor også for etablering og drift af den fælles nationale teknologiske infrastruktur for Personlig Medicin til varetagelse af området inden for genomsekventering og Personlig Medicin.

Målet er at sikre, at personfølsomme data ikke i sig selv kan henføres direkte til en identificeret eller identificerbar fysisk person. Hermed er koblingen mellem eksempelvis rådata og analyseresultater fra en genomsekventering og personen, disse data vedrører,

beskyttet med en nøgle, som sikrer, at alene den der kontrollerer nøglerne, kan identificere den registrerede. Målet er kritisk i både forventede anvendelsesscenarier, men også, og især, ved eventuelle utilsigtede brug af data, ved generelle brud på datasikkerhed eller mulige cyberangreb.

Ved 'Privacy by Design' forstås, at beskyttelsen af følsomme personhenførbare data kan forbedres ved som udgangspunkt at designe sin teknologi således, at den reducerer graden af indgriben i de registreredes privatliv. Dette sker typisk ved dels at begrænse både adgangs- og anvendelsesmulighederne for behandling af følsomme personhenførbare data, og dels at sikre en tidlig pseudonymisering af følsomme personhenførbare data.

Pseudonymisering betyder, at data der kan identificere en given person holdes adskilt fra de følsomme data om samme person på en sådan måde, at de ikke længere kan henføres til personen uden brug af supplerende oplysninger og sikkerhed. De supplerende oplysninger skal derfor opbevares separat og skal være underlagt tydelige og gennemsigtige snitflader ift. selve løsningen og den relaterede teknisk infrastruktur samt tilhørende governancestruktur. Disse tiltag er derfor yderst kritiske for beskyttelsen af især følsomme personhenførebare sundhedsdata for området for Personlig Medicin.

Justitsministeriets vejledning om sikkerhed gennem design og standardindstillinger forventes i december 2017.

I tillæg til ovenstående lovgivning vil sundhedsområdet også fra maj 2018 være reguleret af EU's NIS-direktiv, der vedrører beskyttelsen af cybersikkerheden for kritisk infrastruktur. Dette kan også blive relevant for den fælles nationale teknologiske infrastruktur for Personlig Medicin.

4. International standard til styring af informationssikkerhed

Arbejdet med at etablere og drive den fælles nationale teknologiske infrastruktur for Personlig Medicin, skal følge de principper og retningslinjer, der er fastlagt i standarden ISO27001 (international standard til styring af informationssikkerhed). Det inkluderer de særlige forhold, der gælder i relation til følsomheden af personhenførbare sundhedsdata. Der lægges særlig vægt på standardens fokus på afvejning af de indgående parters risikoprofil versus rette sikkerhedsforanstaltninger og kontrolprocedurer, standardens strenge krav til kontroller versus muligheden for løbende tilpasning i takt med ændringer i organisationen, teknologi og trusselsbilledet, og sidst, at standarden har en fleksibilitet i forhold til, at den kan anvendes sammen med andre rammeværk for informationssikkerhed.

Alle parter, der indgår i den fælles nationale teknologiske infrastruktur for Personlig Medicin, skal således kunne leve op til ISO27001, og dette skal dokumenteres gennem løbende auditeringer.

ISO27001 understøtter et højt niveau for sikkerhed, hvor risikotolerancen for etablering og drift af den fælles nationale teknologiske infrastruktur for Personlig Medicin er 0 og sikkerheds- og databrud ikke kan accepteres. Dette indebærer eksempelvis, at alle sikkerhedskontroller dokumenteres, og skal kunne fremskaffes ved forespørgsel således, at al historik vedr. håndtering af drift og vedligehold ift. blandt andet informationssikkerhed til alle tider kan revideres.

5. Internationale retningslinjer for fysisk sikkerhed

I relation til den fysiske sikkerhed omkring den fælles nationale teknologiske infrastruktur for Personlig Medicin baseres arbejdet på alle ISO27001-sikkerhedskontroller, der vedrører fysisk sikkerhed. Den gælder i særdeleshed de steder, hvor de enkelte involverede HPC-faciliteter og Den National Genomdatabase huses.

Derudover baseres arbejdet på at anvende yderligere sikkerhedskontroller fra NIST-standard (amerikansk standardiseringsorganisation National Institute of Standards and Technology). Kombinationen af ISO27001 og NIST giver en fordel ved beskyttelse af højrisikodata og indebærer blandt andet minimering af adgange, dokumenteret vedligeholdelse af udstyr, kontroller mod katastrofer m.v.