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.