

Statusbilag til Regionsrådets drøftelse 2018

Implementering af regionernes politiske linje

Hver eneste dag behandles følsomme personoplysninger af medarbejdere i regionerne. Medarbejdernes adgang til relevante data er helt afgørende for en god og sammenhængende behandling af den enkelte borger, ligesom data er vigtige for, at vi kan have et moderne og effektivt sundhedsvæsen. Men samtidig er regionerne forpligtet til at sikre, at disse fortrolige oplysninger behandles sikkert, korrekt efter lovgivningen og ikke kommer uvedkommende i hænde. Borgere og patienter skal føle, at det er trygt og sikkert at være i kontakt med det offentlige.

Partierne i Folketinget indgik i februar 2017 en politisk aftale om syv centrale principper for brugen af sundhedsdata. Principperne skal sætte retning og ramme for, hvordan sundhedsvæsenet i årene fremover skal arbejde hen imod partiernes fælles mål om at skabe bedre sundhed gennem en moderne og sikker brug af data.

Principperne lægger blandt andet vægt på:

- Datasikkerhed – sundhedsdata skal håndteres sikkert, og patienterne skal kunne forvente, at der bliver passet godt på deres helbredsoplysninger.
- Lovlighed, fortrolighed, saglighed og proportionalitet – sundhedsdata må kun bruges til saglige formål inden for lovens rammer. Og brugen af personhenførbare data skal begrænses i størst muligt omfang.

Regionerne skal derfor kunne dokumentere, at de tager hånd om informationssikkerhed og sætter en proaktiv dagsorden om informationssikkerhed ved at implementere og efterleve dels folketingets syv principper og dels regionernes politiske linje for informationssikkerhed.

En central målsætning i den politiske linje er, at regionerne samarbejder og lærer af hinanden. Regionerne skal arbejde proaktivt med forbedring af sikkerhedsniveauet ved systematisk at undersøge risici og finde muligheder for forbedring. Regionerne skal følge op på både den systemmæssige sikkerhed, den fysiske sikkerhed, lov- og kontraktkrav samt overholdelse af sikkerhed blandt personale og i processer. Regionerne skal samarbejde med hinanden, relevante interessenter, myndigheder, leverandører og sundhedspersonale for at lære mest muligt af fejl og løbende forbedre sikkerheden.

For at kunne realisere implementeringen af den politiske linje for informationssikkerhed er det derfor vigtigt, at regionerne har en fælles tilgang til området. Det skal sikre, at regionerne opretholder et højt fælles niveau af informationssikkerhed samt overholder gældende lovgivning. Dette har afgørende betydning for borgernes tillid til, at regionerne forvalter borgernes data sikkert og forsvarligt.

Varig forankring af det tværregionale samarbejde om informationssikkerhed

Regionerne samarbejdede i årene 2015-2017 i RSI Pejlemærket for informationssikkerhed. Arbejdet med pejlemærkets leverancer har været med til at synliggøre behovet for en fælles-regional koordineret indsats. I forlængelse heraf blev der medio 2017 etableret en permanent tværregional styregruppe under RSI, som skal sikre det fremtidige samarbejde. Dette sker bl.a. gennem tværregionale arbejdsgrupper, der varetager det operationelle samarbejde.

Succeskriterier for det tværregionale samarbejde:

- Regionerne efterlever ISO 27001 som ramme for arbejdet med informationssikkerhed
- Regionerne har en fælles og koordineret tilgang til arbejdet med informationssikkerhed
- Regionerne anvender fælles koncepter, værktøjer, skabeloner og modeller, der kan lette den enkelte regions arbejde med at styrke informationssikkerheden (awareness, risikovurdering, logopfølgning, databehandlertaaler og lignende)
- Øget opmærksomhed på og viden om informationssikkerhed blandt regionernes medarbejdere, ledelse og politikere
- Øget juridisk compliance i regionerne - alle regioner har optimeret arbejdsgange og rutiner i forhold til gældende lovgivning

Under styregruppen er der organiseret fire permanente arbejdsgrupper:

1. It-sikkerhed
2. Jura og kontraktkrav
3. Organisation og ledelse
4. Databeskyttelsesrådgiverfunktionen

Med hvert sit fokusområde dækker de tilsammen alle aspekter af informationssikkerhed. Disse faggrupper er bemandet med faglige eksperter fra de enkelte regioner, som kan hjælpe styregruppen med at løfte dens opgaveportefølje.

EU Persondataforordning

EU har vedtaget en databeskyttelsesforordning, som fik retsvirkning 25. maj 2018. Persondataforordningen indeholder en række krav, der får betydning for arbejdet med persondatasikkerhed og informationssikkerhed i regionerne.

Overordnet set indebærer forordningen et fokus på en risikobaseret tilgang i forhold til informationssikkerhed med et deraf følgende øget krav om dokumentation af regionernes behandling af personoplysninger. Desuden er der stort fokus på at opfylde de registreredes rettigheder på området og et krav om, at offentlige myndigheder har en databeskyttelsesrådgiver.

En række af databeskyttelsesforordningens nye krav gav et behov for, at regionerne iværksatte tiltag, der skulle bidrage til, at den enkelte region kunne blive parat til at imødekomme kravene. Med den tværregionale styregruppes etablering satte regionerne derfor et fælles arbejde i gang omkring udvalgte emner i forhold til databeskyttelsesforordningen inden for følgende tre hovedoverskrifter:

- Den registreredes rettigheder
- Organisation og politik
- Kortlægning og konsekvensvurdering

At regionerne i fællesskab adresserer en række af de nye krav, som følger af databeskyttelsesforordningen, er med til at optimere regionernes samlede ressourceforbrug i implementeringsarbejdet med forordningen. Dette er eksempelvis sket i form af at udarbejde en række værktøjer, rammer og vejledninger samt sikre, at der sker en tværregional vidensdeling og sparing.

National strategi for cyber- og informationssikkerhed

I forlængelse af Forsvarsforliget 2018-2023 har regeringen og forligspartierne udformet en ny national strategi for cyber- og informationssikkerhed. Regeringen igangsætter initiativer og målrettede strategier for de mest kritiske sektorer – herunder sundhedssektorens - arbejde med cyber- og informationssikkerhed, der skal øge den tekniske robusthed i den digitale infrastruktur, øge viden og kompetencer hos borgere, virksomheder og myndigheder og styrke den nationale koordinering og samarbejdet på området.

Strategi for sundhedssektoren

Sundhedssektoren er kendetegnet ved, at der ved behandling og pleje af patienter registreres et stort antal personhenførbare oplysninger. Det gør sektoren til et muligt mål for cyberkriminalitet. Det udbredte samarbejde om patientbehandlingen i sundhedssektoren med dertilhørende deling af patientoplysninger parterne imellem indebærer desuden en risiko for, at potentielle cyberkriminelle vil gå efter "det svageste led", hvis ikke alle aktører i tilstrækkelig grad lever op til nødvendige og ensartede krav til sikkerhed. Delstrategien skal på den baggrund styrke og ensrette arbejdet med cyber- og informationssikkerhed på tværs af sundhedssektoren med henblik på at forudsige, forebygge, opdage og håndtere cyberangreb samt videreføre arbejdet i strategi for digital sundhed 2018-2022. Sundheds- og Ældreministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationsikkerheden i sundhedssektoren. Regionerne er repræsenteret i arbejdet med delstrategien.

Trusselsvurdering fra Center For Cybersikkerhed (CFCS)

Center For Cybersikkerhed vurderede i maj 2018, at truslen fra cyberspionage og cyberkriminalitet mod danske myndigheder er meget høj.

Truslen fra cyberspionage er især rettet mod danske myndigheder, som har oplysninger, der er strategisk, politisk eller økonomisk værdifulde for fremmede stater. Der er tale om en særdeles aktiv trussel fra enkelte stater, der løbende forsøger at stjæle informationer fra danske myndigheder og virksomheder. Truslen mod danske myndigheder vil gælde på langt sigt og er dermed et grundvilkår for myndighederne.

Truslen fra cyberkriminalitet er et globalt fænomen, der også rammer danske myndigheder, virksomheder og borgere. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra myndigheder, virksomheder og borgere. Nogle cyberkriminelle grupper kan udføre målrettede og avancerede cyberangreb, hvor de f.eks. stjæler fra myndig-

heder og virksomheder eller afpresser dem for meget høje pengebeløb. De mere målrettede og avancerede angreb har på verdensplan især ramt finanssektoren og sundhedssektoren.

CFCS understreger alvoren i truslen og har konkrete eksempler på hackere, som har forsøgt at få fat på dansk offentlig forskning efter at have scannet danske myndigheder og virksomheder for it-sårbarheder.

Center For Cybersikkerhed anbefaler, at danske myndigheder har fokus på logning og mulighederne for at opdage og analysere cyberangreb. Desuden fremhæves basale sikkerhedsforanstaltninger som systematisk sikkerhedskopiering, awareness kampagner, opdatering af programmer og systemer og lignende som vigtige elementer i adressering af cybertrusler.

Konklusion

Informationssikkerhed spiller en vigtig rolle i regionernes dagligdag. Medarbejdernes brug af informationer er en stor del af det gode patientforløb, og informationssikkerhed er en forudsætning for at anvende data til at give patienterne en tryk behandling.

I takt med digitaliseringen øges imidlertid risikoen for brud på informationssikkerheden og for it-kriminalitet. Det aktuelle trusselsbillede afslører, at blandt andet statsstøttede hackergrupper, der går efter danske myndigheder og virksomheder, er en alvorlig cybertrussel mod Danmark.

Regionerne har derfor fortsat fokus på arbejdet med informationssikkerhed. Dels fortsætter arbejde med databeskyttelsesforordningen og dels er der øget opmærksomhed på cyber- og informationssikkerhed. I det tværregionale samarbejde skal indsatserne på det it-tekniske, juridiske og organisatoriske område spille sammen, da de er indbyrdes afhængige af hinanden.

Samarbejdet i regionerne har øget regionernes niveau for informationssikkerhed og muligheden for stå samlet på området. For at fastholde den positive udvikling er der derfor skabt en organisering, der også fremadrettet sikrer en tværregional opmærksomhed og indsats på området.