DANSKE REGIONER

001000
0000010001000
0001000
00010001000
10001000

Regionernes politiske linje for informationssikkerhed

0100101

10000100001000

Regionernes politiske linje for informationssikkerhed

Danske Regioner 2015
Layout: UHI, Danske Regioner

Forord

Digitalisering er i dag en af de største forandringskræfter i vores samfund.

Det er en udvikling, som drives af nye teknologiske muligheder, hvor vi kan indsamle, opbevare og anvende stadig større mængder data. Borgerne stiller i stigende grad krav om, at virksomheder og den offentlige sektor skal være på forkant med de nye digitale muligheder ved f.eks. at tilbyde borgerne digitale selvbetjeningsløsninger på internettet, som skal kunne betjenes fra både den stationære PC i hjemmet og via apps på mobiltelefonen, når man er på farten.

Den digitale udvikling har allerede sat mærkbare spor i sundhedsvæsenet. Det er en udvikling, som gerne skal fortsætte. I sundhedsvæsenet har vi brug for den hjælpende hånd, som de nye digitale muligheder tilbyder. Det har vi, fordi vi i fremtiden ønsker at blive ved med at levere høj behandlingskvalitet til en aldrende befolkning og samtidig fastholde princippet om, at der i Danmark er fri og lige adgang til sundhedsydelserne.

I regionerne skal vi anvende sundhedsdata til at give patienterne den bedst mulige behandling og understøtte den daglige kliniske ledelse på hospitalerne. Vi skal også bruge sundhedsdata til at udvikle og forbedre sundhedsvæsenet for eksempel gennem planlægning, kvalitetsudvikling og forskning.

Det vil komme vores børn og børnebørn til gode.

Sundhedsdata er personlige. Der følger således et særligt ansvar med, når vi i regionerne anvender sundhedsdata. Derfor skal sikkerheden være i orden, og der skal være åbenhed overfor borgerne om, hvordan sundhedsdata anvendes. Informationssikkerhed er fundament for at anvende data til at give patienterne den bedste behandling – nu og i fremtiden.

I regionerne tager vi denne præmis meget alvorligt. Borgerne skal kunne have tillid til, at regionerne forvalter sundhedsdata sikkert og forsvarligt. Derfor har vi lagt en politisk linje for regionernes arbejde med informationssikkerhed.

Vi ønsker med dette initiativ at sætte informationssikkerhed højt på dagsordenen. Regionernes politiske linje for informationssikkerhed er en del af en samlet politik om sundhedsdata, som regionerne vil lancere senere i foråret 2015.

God læselyst!

Bent Hansen

Carl Holst

Et stærkt digitalt sundhedsvæsen

Digitalisering er et centralt redskab i et moderne og kvalitetsstærkt sundhedsvæsen. De digitale arbejdsredskaber betyder, at borgerne kan føle sig trygge ved, at sundhedspersoner har de relevante informationer, når de skal bruge dem til at behandle patienter.

Den digitale udvikling har også givet nye muligheder for kvalitetsudvikling, forskning i nye behandlingsmuligheder og en bedre udnyttelse af ressourcer. Borgere behandles således på et bedre informationsgrundlag i dag end tidligere, fordi vi kan dele viden over afstand, mellem specialer og på tværs af sektorer.

Digital brug af informationer er således en essentiel del af det gode patientforløb og en effektiv indretning af vores sundhedsvæsen. Det er en udvikling, som fortsat drives af ny teknologi såvel som nye generationers krav om, at det offentlige sundhedsvæsen skal kunne matche en digital livsstil.

Mange af de informationer, som deles digitalt i dag, er også blevet delt på papir før digitaliseringen. Men de digitale muligheder for bredere deling af relevante informationer, rejser spørgsmål om, hvordan man beskytter persondata i et digitaliseret samfund.

Årsager til brud på informationssikkerheden kan skyldes svagheder i it-systemer eller teknisk udstyr, forældede løsninger eller forkert adfærd i organisationen. Det kan også skyldes, at der ikke er klare aftaler om, hvem der har ansvar for hvad eller, at der mangler tilstrækkelig prioritering af indsatsen.

Informationssikkerhed er en forudsætning for at udnytte det fulde potentiale for at skabe et stadig bedre sundhedsvæsen gennem digitalisering. Deling af informationer skal foregå på en måde, som er tryg for borgeren. Informationer må ikke blive misbrugt eller komme i uvedkommendes hænder. Lovgivningen skal overholdes og sikkerhedsbrud, cyberkriminalitet og hacking skal minimeres og sikkerhedsbrud håndteres.

Ingen kæde er stærkere end det svageste led.

Regionerne har allerede et stort fokus på sikker brug af persondata og arbejder med informationssikkerhed på flere niveauer. Men den digitale udvikling går stærkt, og der er behov for hele tiden at have øjet på bolden. Derfor lancerer regionerne denne publikation om informationssikkerhed, som indeholder fællesregionale målsætninger og initiativer om informationssikkerhed. Formålet er at sætte et fælles niveau for, hvordan regionerne værner om borgernes privatliv ved brug af persondata.

Informationssikkerhed er mere end it

Informationssikkerhed omhandler grundlæggende beskyttelse af information med udgangspunkt i bevarelse af fortrolighed, integritet og tilgængelighed.

Fortrolighed indebærer, at information er sikret mod adgang eller eksponering for uvedkommende. Det betyder grundlæggende, at man som borger skal kunne stole på, at ens personfølsomme informationer ikke vises til personer, som ikke har rettighed til og et konkret formål med at se informationerne.

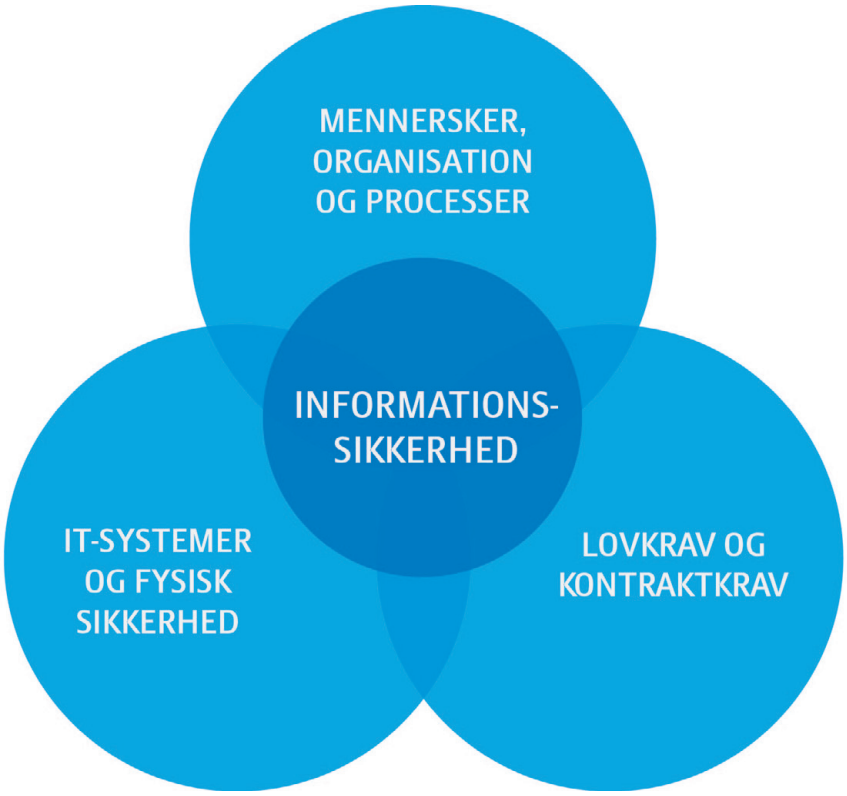
Integritet indebærer, at informationer ikke må ændres uden autorisation. Det betyder, at man som borger skal kunne stole på, at de data som sundhedspersonale har adgang til er nøjagtige og fuldstændige, og at behandling således igangsættes på et korrekt grundlag.

Tilgængelighed indebærer, at informationer er tilgængelige for autoriserede personer, når det er relevant. Det handler om, at borgerne skal kunne være trygge ved, at sundhedspersonale har de informationer, som de skal bruge for at behandle på et så oplyst grundlag som muligt.

Informationssikkerhed er mere end it-sikkerhed. Det handler om, hvordan organisationer og medarbejdere omgås informationer og de tiltag, som iværksættes for at sikre sikker behandling af personfølsomme informationer.

De centrale elementer i informationssikkerhed berører således tre overordnede områder:

1. Mennesker, organisation og processer
2. Lovkrav og kontraktkrav
3. It-systemer og fysisk sikkerhed



1. Mennesker, organisation og processer

Et kerneelement i informationssikkerhed er ledelsens prioritering af området og medarbejdernes adfærd i dagligdagen. Få tænker over, at det kan udgøre en alvorlig sikkerhedsrisiko selv at downloade programmer. Det samme gælder eget indkøb og tilkobling af medico-teknisk udstyr. Det giver risiko for hacking. Tilsvarende kan det også udgøre en risiko at gemme personfølsomme informationer på en USB-nøgle, der kan blive væk.

Derfor er det centralt, at medarbejderne er bevidste om, hvor vigtig deres adfærd er for informationssikkerheden. Det handler både om, hvordan medarbejderne håndterer teknik og it-udstyr, og om hvordan de omgås personfølsomme informationer. Det er vigtigt, at dette understøttes af ledelsesstrukturer og processer, som prioriterer informationssikkerhed.

2. It-systemer og fysisk sikkerhed

Bevidst og ubevidst misbrug af informationer og hackerangreb udgør væsentlige trusler mod informationssikkerheden. Der skal derfor være fokus på at sikre, at uvedkommende ikke har adgang til data, og der skal være planer for håndtering ved sikkerhedsbrud.

Dette element af informationssikkerhed indebærer også kryptering af data, så de sendes og opbevares sikkert, opdatering af operativsystemer samt tekniske muligheder for opfølgning af menneskelig adfærd, eksempelvis gennem log-funktioner i it-systemerne.

Medico-teknisk udstyr kan også indeholde personfølsomme data og være forbundet til it-systemer, som kræver etablering af sikkerhedsforanstaltninger. Endelig omhandler det de fysiske elementer af informationssikkerhed som for eksempel sikring af serverrum mod brand, indbrud, strømudfald, oversvømmelse eller andre trusler.

3. Lovkrav og kontraktkrav

Krav om tavshedspligt, fortrolighed og sikker behandling af helbredsinformationer er reguleret i blandt andet sundhedsloven, persondataloven, forvaltningsloven og straffeloven. Lovene er komplekse og det kræver fokus at sikre, at lovene overholdes både, når det omhandler it-drift og udvikling af nye digitale initiativer.

Dette element af informationssikkerhed indebærer også et fokus på, at der indskrives konkrete kontraktkrav til it-sikkerhed i de drifts- og udviklingsaftaler, som regionerne indgår med leverandører.

En samlet prioritering af informationssikkerhed kræver fokus på alle tre områder. Indsatserne på de tre områder skal understøtte hinanden og tilsammen styrke informationssikkerheden.

Regionernes målsætninger om informationssikkerhed

Borgere skal kunne føle sig trygge ved, at persondata bruges sikkert og forsvarligt ligegyldigt hvor i Danmark, man modtager behandling. Disse målsætninger sætter et fællesregionalt niveau for indsatsen omkring informationssikkerhed. Målsætningerne skal understøtte medarbejdere og ledelse i en løbende og vedvarende prioritering af sikker omgang med personinformationer.

1. **Informationssikkerhed bruges som fundament for et stadig bedre sundhedsvæsen**
   Sikker og ansvarlig brug af sundhedsinformationer er en forudsætning for at tilbyde borgerne behandling på det bedste grundlag. Topledelsen anskuer derfor informationssikkerhed som et fundament for udviklingen af det danske sundhedsvæsen. Regionerne tager ansvar for, at sikkerheden for personfølsomme informationer er understøttet af de nødvendige tiltag.

2. **Regionerne sætter et tilstrækkeligt højt niveau for informationssikkerhed**
   Det anvendte sikkerhedsniveau skal være afstemt efter sårbarheder og risici, så kræfterne bruges de rette steder. Sikkerhedsniveauet skal være tilstrækkeligt højt og ensartet både i og på tværs af regionerne vel vidende, at ingen kæde er stærkere end det svageste led. Nye muligheder for sikring af persondata skal afsøges.

3. **Informationssikkerhed og brugervenlighed skal gå hånd i hånd**
   Brugeres adfærd er afgørende for sikkerhedsniveauet. Derfor skal brugervenlighed og sikkerhed gå hånd i hånd. Sikkerhed skal tænkes ind i nye projekter og tiltag fra start og betragtes som et bærende element for udvikling af gode løsninger. Sikkerhedsindsatsen skal tage udgangspunkt i dagligdagen, og løsningerne skal være tilpasset arbejdsgange og brugere.

4. **Alle medarbejdere forstår, at deres adfærd er fundament for informationssikkerhed**
   Alle medarbejdere i regionerne skal se det som deres ansvar at værne om borgernes privatliv, når de omgås personfølsomme informationer. Medarbejderne skal være opmærksomme på risici og forstå og følge retningslinjer for informationssikkerhed, når de omgås personfølsomme informationer, uanset hvordan disse opbevares.

5. **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.

6. **Regionerne stiller krav til leverandører**
   Regionerne skal forpligte sine leverandører til at have et tilstrækkeligt og forsvarligt informationssikkerhedsniveau og leve op til regionernes informationssikkerhedspolitikker. Regionerne skal samarbejde proaktivt med leverandører om at udvikle og modne sikkerhedsarbejdet i samarbejde med andre parter.

Initiativer for bedre informationssikkerhed

Udgangspunktet for den fællesregionale indsats for informationssikkerhed er, at regionerne skal følge ISO 27001 standarden. Denne standard er lagt an på en risikobaseret tilgang til tilrettelæggelse af informationssikkerhed, hvor beskyttelsesniveau er afstemt efter risiko og væsentlighed.

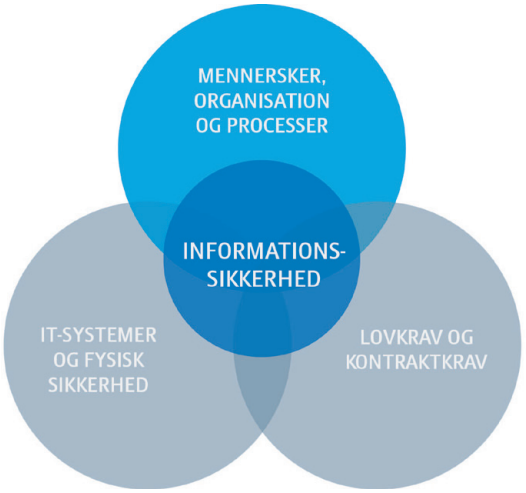
Den risikobaserede tilgang tager udgangspunkt i en erkendelse af, at alt ikke kan beskyttes fuldstændigt. Ressourcer og indsatser skal derfor prioriteres bedst muligt i forhold til opgavevaretagelsen. Fokus skal hele tiden være på både at understøtte et kvalitetsstærkt sundhedsvæsen for borgerne samtidigt med, at der værnes om borgernes privatliv gennem beskyttelse af persondata.

Den risikobaserede tilgang til informationssikkerhed udmøntes gennem strukturerede risikovurderinger af digitale arbejdsredskaber. Gennem risikovurderingen får organisationen overblik over sine it-systemer, og hvor vigtige de er for forretningen. På baggrund heraf kan ledelsen træffe beslutning om, i hvilken grad it-systemerne skal beskyttes, og hvor indsatsen skal prioriteres. Det accepterede risikoniveau og den heraf følgende handlingsplan skal godkendes på topledelsesniveau.

Indenfor hvert af de tre ovenstående områder, som er skitseret i figuren, er der beskrevet en række initiativer, som hver region skal gennemføre. Formålet med disse initiativer er at skabe et ensartet niveau for arbejdet med informationssikkerhed på tværs af regionerne.

Der skal følges op på det fællesregionale niveau for informationssikkerhed primo 2017.

Initiativer:
Mennesker, organisation og processer



1. **Entydigt ledelsesansvar og struktureret opfølgning**
   Regionerne vil have et entydigt og nedfældet ledelsesansvar for informationssikkerhed, som afspejler en struktureret tilgang til informationssikkerhed i organisationen. Det vil dække hele den organisatoriske kæde fra topledelsesniveau til afdelingsniveau. Det er topledelsen, som vil træffe de endelige beslutninger om et tilstrækkeligt og acceptabelt sikkerhedsniveau gennem afvejning af hensyn til sandsynlighed og konsekvens.

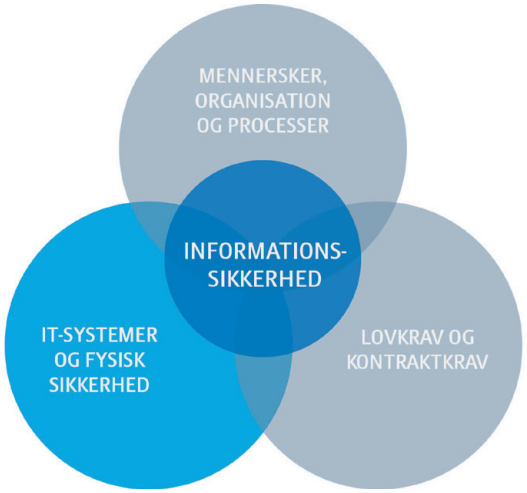
2. **Udarbejdelse af en fællesregional informationssikkerhedspolitik**
   Regionerne vil udarbejde en fællesregional informationssikkerhedspolitik baseret på ISO 27001 standarden. Denne skal konkretisere, hvad regionerne skal leve op til. Hvordan regionerne lever op til politikken, er som udgangspunkt de enkelte regioners valg. Med udgangspunkt i sikkerhedspolitikken, det fællesregionale trusselsbillede, anbefalinger fra Center for Cybersikkerhed samt gennemførte risikovurderinger i de enkelte regioner, vil hver region udarbejde en handlingsplan for implementering af de prioriterede kontroller.

3. **Medarbejdernes viden**
   En stærk bevidsthed om hvordan man omgås personfølsomme informationer er afgørende. Regionerne vil derfor udføre initiativer omkring kompetenceudvikling, awareness-kampagner samt løbende dialog om informationssikkerhed understøttet af en stærk ledelsesforankring. Dette arbejde vil tage afsæt i konkrete informationssikkerhedsprocedurer og informationssikkerhedsinstrukser. Regionerne vil følge systematisk op på, om procedurer og instrukser efterleves, og dette vil have ledelsens bevågenhed. Brud på sikkerhedsprocedurerne kan have ansættelsesretslige konsekvenser.

4. **Sikkerhed skal tænkes ind i nye it-løsninger fra start**
   Det er afgørende, at sikkerhed tænkes ind fra starten i udviklingen af nye løsninger for at sikre, at brugervenlighed og sikkerhed kan forstærke hinanden. Derfor vil regionerne etablere metoder og processer for at sikre dette. Da medico-teknisk udstyr kan indeholde personfølsomme data og ofte er forbundet med it-systemer, vil der også være processer for sikring af informationssikkerhed ved erhvervelse af nyt medico-teknisk udstyr. Muligheder for anvendelse af anonymisering og pseudonymisering til at sikre, at data ikke er personhenførbare samt større anvendelse af kryptering som beskyttelse af data mod utilsigtet adgang vil blive afsøgt.

5. **Regionsråd skal drøfte informationssikkerhed årligt**
   Regionsrådene vil årligt drøfte regionens trusselsbillede og sikkerhedstiltag med udgangspunkt i en statusrapportering fra regionerne.

Initiativer:
It-systemer og fysisk sikkerhed



1. **Strukturerede risikovurderinger af it-systemer og medico-teknisk udstyr**
   Regionerne vil gennemføre jævnlige strukturerede risikovurderinger af de forretningskritiske systemer og medico-teknisk udstyr. Risikovurderingerne vil blive fulgt op af handlingsplaner for håndtering af kritiske risici. Vurderingerne vil forholde sig til sårbarhed og trusler samt sandsynlighed for at sikkerhedsbrud opstår og konsekvenser heraf. På baggrund heraf sættes der mål for informationssikkerheden, og der laves en handlingsplan for håndtering af risici.

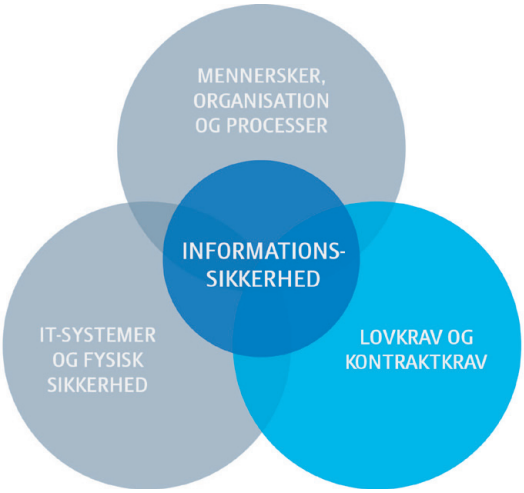
2. **Sikring mod hackerangreb**
   Man kan ikke sikre sig fuldstændigt mod hackerangreb, men regionerne vil etablere kontroller for at formindske risici. Det skal kunne opdages, når systemer er blevet hacket, og der skal være planer for re-etablering af kritiske systemers data. Regionerne vil yderligere gennemføre regelmæssige penetrationstest på udvalgte systemer, hvor en uafhængig tredje part tester sikkerheden med henblik på identifikation af sårbarheder.

3. **Bruger-rollestyring**
   Regionerne vil sikre, at der er adgangsbegrænsning på, hvem der kan tilgå hvilke data med personfølsomme informationer. Tiltag til at understøtte dette kan være procedurer for brugeradministration, teknisk understøttelse af bruger-rollestyring, tilpassede arbejdsgange eller advarselsfunktioner. Dette vil understøtte hensynet mellem tilgængelighed af data for sundhedspersonale og beskyttelse af personfølsomme data.

4. **Log og opfølgning**
   Regionerne vil sikre, at der er logning af brugernes adgang til it-systemer, der håndterer personfølsomme informationer. Regionerne vil gennemgå loggen systematisk. Ledelsen vil følge op på det og tage hånd om det, når det opdages, at nogle har slået patientdata op uden en behandlermæssig grund. Dette kan understøttes ved installation af værktøjer, der løbende og systematisk gennemgår opslag for, om der er en aktuel behandlerrelation mellem sundhedsfagligt personale og borger.

5. **It-beredskabsplaner**
   Regionerne vil udarbejde It-beredskabsplaner. Beredskabsplanerne skal som en del af det samlede forretningsberedskab sikre organisationens kritiske forretningsprocesser og informationsaktiver i tilfælde af alvorlige hændelser, der påvirker organisationens muligheder for at operere. It-beredskabsplanerne skal løbende vedligeholdes og testes.

Initiativer:
Lovkrav og kontraktkrav



1. **Krav til leverandører**
   Regionerne vil stille krav til leverandører om anvendelse af ISO 27001 standarden. Leverandørerne skal forpligtes til at arbejde proaktivt med informationssikkerhed, opdage og rette fejl samt indgå aktivt i udvikling af et bedre sikkerhedsniveau. Kontrollen af eksterne leverandører sker gennem revisionserklæringer og struktureret opfølgning.

2. **Juridisk compliance**
   Regionerne vil styrke den juridiske vurdering af brug af sundhedsdata, når der iværksættes nye initiativer og projekter. Der vil således blive etableret klare og nedfældede procedurer for sikring af hjemmelgrundlaget ved nye digitaliseringsinitiativer. Dette indebærer også sikring af korrekte og opdaterede anmeldelser til de relevante myndigheder. Brug af data uden hjemmel kan have strafferetslige konsekvenser.

3. **Databehandleraftaler**
   Databehandleraftaler er et juridisk bindende dokument, som fastlægger ansvarsfordelingen mellem den dataansvarlige og den databehandlende instans, herunder hvordan du må opbevare, videreformidle og behandle data til understøttelse af opgavevaretagelsen. Regionerne vil sikre, at der er databehandleraftaler med alle de instanser, der behandler personfølsomme data på regionernes vegne.

4. **Modernisering af lovgivningsmæssige rammer**
   Både nationale love og EU sætter rammer for, hvordan sundhedsdata kan bruges. Regionerne skal spille en aktiv rolle i at sikre, at lovgivningen følger med udviklingen. Regionerne skal kunne anvende data til udvikling af et stærkt og moderne sundhedsvæsen og samtidigt sikre den nødvendige beskyttelse af borgernes privatliv.

DANSKE
REGIONER