Fællesregional Informationssikkerhedspolitik

Indhold

1. Formål

Den Fællesregionale Informationssikkerhedspolitik er udarbejdet i et samarbejde mellem Region Hovedstaden, Region Sjælland, Region Syddanmark, Region Midtjylland og Region Nordjylland.

Informationssikkerhed handler grundlæggende om beskyttelse af oplysninger, så fortrolighed, integritet og tilgængelighed bevares.

Hver eneste dag behandles følsomme personoplysninger og andre fortrolige informationer af medarbejdere i de fem regioner. Det er absolut nødvendigt, at data er korrekte, fuldstændige og tilgængelige, da adgang til relevante og tidstro persondata er en forudsætning for god og sammenhængende behandling af den enkelte borger. Det er en forudsætning for, at regionerne fortsat kan tilbyde et moderne og effektivt sundhedsvæsen.

Denne brug af data skal ske på en måde, som sikrer borgernes fortsatte tillid til regionerne. Informationssikkerhed skal af den grund være en integreret del af den ydelse, som regionerne leverer til borgere, patienter, virksomheder, samarbejdsparter m.fl., ligesom det skal være en integreret del af det daglige arbejde for medarbejderne og andre brugere. Regionernes håndtering af informationssikkerhed skal sikre, at patienterne får den bedste behandling samtidig med, at deres oplysninger er i trygge hænder.

Følsomme persondata, herunder sundhedsdata, er personlige, og når regionerne behandler dem har de et særligt ansvar for, at sikkerheden er høj. Derfor har Danske Regioner i 2015 lagt en politisk linje for informationssikkerhed, som denne politik skal udmønte. Den politiske linje lægger vægt på at

- informationssikkerhed bruges som fundament for et stadig bedre sundhedsvæsen
- regionerne sætter et tilstrækkeligt højt niveau for informationssikkerhed
- informationssikkerhed og brugervenlighed går hånd i hånd
- alle medarbejdere forstår, at deres adfærd er fundament for informationssikkerhed
- regionerne samarbejder og lærer af hinanden
- regionerne stiller krav til leverandører

Den politiske linje definerer følgende tre overordnede områder.

1. ***Mennesker, organisation og processer***
   Medarbejdernes adfærd i dagligdagen har stor betydning for informationssikkerheden. Det er centralt, at alle medarbejdere er bevidste om, hvordan deres adfærd påvirker informationssikkerheden. Det handler både om, hvordan medarbejderne håndterer teknik og it-udstyr, og om hvordan de omgås følsomme personoplysninger. Medarbejderne skal derfor have kendskab til lovgivning, regionernes egne politikker, retningslinjer og instrukser - og selvfølgelig også overholde dem. Ledelsens prioritering af området er også vigtig. Derfor bør regionerne sikre en organisation, der prioriterer informationssikkerhed, så medarbejdere og ledelse har gode betingelser for at arbejde med følsomme personoplysninger.

2. ***It-systemer og fysisk sikkerhed***
   Regionernes brug og håndtering af følsomme og fortrolige oplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Det kræver blandt andet, at regionerne håndterer oplysningerne fortroligt, bevarer datas integritet og ikke ændrer oplysningerne uden autorisation. Data skal kun være tilgængelige for dem, som må og skal bruge dem og det skal foregå sikkert. Dette stiller tekniske krav i forbindelse med udvikling, implementering og drift af it-løsninger og krav til den fysiske sikring af hardware og lignende.

3. ***Lovkrav og kontraktkrav***
   Regionerne skal sikre, at relevante lov- og kontraktkrav overholdes i det daglige arbejde. Regionerne må kun behandle borgernes oplysninger i tilfælde, hvor det nødvendige lovgrundlag foreligger. Dette element af informationssikkerhed indebærer også et fokus på, at der indskrives konkrete kontraktkrav til informationssikkerhed i de drifts- og udviklingsaftaler, som regionerne indgår med leverandører.

Der er vigtigt, at borgere, patienter, virksomheder, samarbejdsparter og andre interessenter kan have tillid til, at regionerne har etableret nødvendige tiltag til at sikre borgernes oplysninger, og at regionerne forvalter deres følsomme personoplysninger sikkert og forsvarligt.

Den politiske linje for informationssikkerhed stiller desuden krav til, at regionerne efterlever ISO 27001-standarden som rammeværktøj for arbejdet med informationssikkerhed i regionerne. Den fællesregionale politik skal sammen med den enkelte regions egen informationssikkerhedspolitik understøtte og sikre et ensartet sikkerhedsniveau. Det skal ske ved, at den enkelte region etablerer, implementerer, vedligeholder og løbende forbedrer et ledelsessystem for informationssikkerhed inden for rammerne af informationssikkerhedsstandarden ISO 27001.[1]

2. Organisation

[1] Et ledelsessystem, også kaldet et InformationsSikkerhedsManagementSystem (ISMS), er i denne sammenhæng et udtryk for de politikker, procedurer, processer, organisatoriske beslutningsgange og aktiviteter, som tilsammen udgør regionernes styring af informationssikkerhed. Den enkelte region har fastlagt en struktur samt rammer og arbejdsgange for informationssikkerhedsarbejdet.

For at sikre at behandling og opbevaring af følsomme personoplysninger lever op til lovens krav er det vigtigt at indrette sin organisation på en måde, der gør det naturligt i praksis at efterleve informationssikkerhedsreglerne. Dette arbejde starter med en forankring i topledelsen.

Hver region skal have et entydigt og nedskrevet ledelsesansvar for informationssikkerhed, som afspejler en struktureret tilgang til informationssikkerhed i organisationen. Det skal dække hele det organisatoriske niveau.

Det er **topledelsens** ansvar at træffe den endelige beslutning om et sikkerhedsniveau, der er afstemt efter risiko og væsentlighed og offentlighedens interesser. Niveauet skal overholde relevante lov- og kontraktkrav.

Topledelsen har ansvar for at understøtte politikker, retningslinjer og instrukser samt allokere nødvendige ressourcer til at gennemføre arbejdet med informationssikkerhed i regionen. Den skal sikre, at regionens medarbejdere har den fornødne viden om informationssikkerhed.

Linjeledelsen har med udgangspunkt i topledelsens udstukne politikker, retningslinjer og instrukser ansvar for, at disse efterleves i egen enhed.

Ledelsen skal arbejde for en kultur hvor ansvarlighed i forhold til informationsbehandling falder naturligt for alle. Alle **medarbejdere** har et ansvar for at bidrage til, at regionernes oplysninger ikke kommer i de forkerte hænder. Det er ledelsens ansvar at sikre, at alle medarbejdere har den fornødne viden om informationssikkerhed, og at der i relevant omfang sker en løbende uddannelse i informationssikkerhed. Tilsvarende er medarbejderne forpligtede til at gøre sig bekendt med den information om informationssikkerhed, der stilles til rådighed.

3. Gyldighedsområde

Den Fællesregionale Informationssikkerhedspolitik og hver regions egen informationssikkerhedspolitik gælder, hvor regionens oplysninger og særligt regionens følsomme personoplysninger opbevares eller behandles. Det har ingen betydning for gyldighedsområdet, hvor og hvordan de opbevares eller behandles. Behandling af regionens oplysninger må kun finde sted efter aftale med den pågældende region. Informationssikkerhedspolitikken gælder således for:

- **Alle brugere**. Ved en bruger forstås fx medarbejdere, forskere, konsulenter, regionsrådsmedlemmer, elever, studerende og andre, der midlertidigt eller for en længere periode har adgang til regionens personoplysninger.
- **Samarbejdspartnere** der opbevarer eller har adgang til, anvender eller behandler biomateriale, papirbaserede eller elektroniske følsomme personoplysninger efter aftale med regionen. Det har i denne sammenhæng ingen betydning, om samarbejdspartnerne befinder sig i eller uden for Danmark.
- **Fællesregionale samarbejdspartnere**. Hvor flere regioner anvender samme samarbejdspartner eller leverandør til fælles løsninger, skal den fællesregionale informationssikkerhedspolitik anvendes.

Den fællesregionale og regionernes egne informationssikkerhedspolitikker gælder derimod ikke borgere, der med sikker identifikation og gennem borgervendte systemadgange har adgang til egne oplysninger.

4. Målsætninger

I efterlevelsen af ISO 27001-standarden har regionerne følgende fælles målsætninger:

For at sikre et tilstrækkeligt og acceptabelt sikkerhedsniveau er det nødvendigt at vurdere risikobilledet, lige fra sårbarheder i de enkelte systemer til risikoen for at blive udsat for hackerangreb.

A. Regionens sikkerhedsniveau og risikobillede fastlægges med afsæt i en overordnet risikovurdering[2]. Risikovurderingen skal
   - skabe overblik over regionens risikoprofil, der er et overblik over identificerede informationssikkerhedsrisici
   - sikre udarbejdelse og vedligeholdelse af et katalog over identificerede trusler
   - identificere de mest sårbare og kritiske systemer
   - sikre ledelsens involvering i definitionen af sikkerhedsniveauet
   - skabe bevidsthed om sikkerhed i organisationen
   - danne grundlag for udarbejdelsen af en handlingsplan for at imødegå identificerede trusler mod systemerne.

B. Med udgangspunkt i den enkelte regions risikovurdering fastlægger regionen egen tidsramme og metode for at
   - udarbejde og vedligeholde et SoA [3]dokument (Statement of Applicability)
   - udarbejde politikker, retningslinjer og instrukser samt føre tilsyn med at de bliver overholdt
   - udarbejde og teste it-beredskabsplaner og nødprocedurer
   - udarbejde og iværksætte opmærksomhedsskabende tiltag
   - rapportere jævnligt til relevante ledelseslag om informationssikkerhed.

I efterlevelsen af gældende lovgivning har regionerne følgende målsætninger:

C. Den til enhver tid gældende lovgivning på området, særligt lovgivning inden for persondatabeskyttelse, skal efterleves i regionerne og hos deres samarbejdspartnere, herunder ved
   - sikring af at enhver behandling af følsomme personoplysninger foregår efter en risikobaseret tilgang og i overensstemmelse med gældende lovgivning
   - sikring af, at videregivelse og overladelse af oplysninger udelukkende sker i henhold til lovhjemmel og databehandleraftaler
   - at dokumentere datastrømme, sikringstiltag og kontroltiltag
   - overholdelse af tekniske krav til logning, autorisation og rollestyring
   - dokumenteret systematisk logopfølgning
   - forpligtelse af leverandører til at sikre et tilstrækkeligt og forsvarligt informationssikkerhedsniveau gennem krav og kontrol
   - registrering af brud eller mulige brud på informationssikkerheden.

[2] I risikovurderingen identificeres, analyseres og evalueres risici med udgangspunkt i den definerede kontekst.

[3] SoA kan forstås som en erklæring af, hvilket sikkerhedsniveau organisationen aktivt har besluttet sig for og hvorfor.

5. Godkendelse

Den Fællesregionale Informationssikkerhedspolitik planlægges godkendt af de fem regionsråd i 2016.