MedComs informationssikkerhedspolitik for Systemforvaltningen

1. Indledning

Denne informationssikkerhedspolitik dækker MedComs systemforvaltningsansvar for de 3 fællesoffentlige sundheds-it-infrastrukturer Sundhedsdatanettet (SDN), Videoknudepunktet (VDX) og Hjemmemonitoreringsdatabasen (KIH).

Politikken understøtter og udmønter MedComs vision og mission.

MedCom er ansvarlig for, at de 3 fællesoffentlige sundheds-it-infrastrukturer er sikret i henhold til lovgivningen for behandling af personoplysninger og mod brud på personoplysninger og informationers fortrolighed, integritet og tilgængelighed. MedComs ansvar er fastlagt i databehandleraftaler.

MedCom har som målsætning at efterleve relevante dele af ISO27001:2013, da styring af Informationssikkerheden er en vigtig opgave for MedCom som fællesoffentlig forvalter. Informationssikkerheden styres efter en klart defineret model som angivet i MedComs ISMS.

Det påhviler altid den ansvarlige leder at sørge for, at Informationssikkerhedspolitikken efterleves.

2. Informationssikkerhedspolitikkens formål og målsætninger

Formålet med informationssikkerhedspolitikken er at understøtte en sikker anvendelse af SDN, VDX og KIH efter en fastlagt styring af informationssikkerheden.

MedCom ønsker at fremstå som en pålidelig systemforvalter, som behandler personoplysninger og informationer i henhold til gældende regler og lovgivning.

Det er et mål for MedCom, at Informationssikkerheden vedvarende vedligeholdes og forbedres der, hvor det findes nødvendigt. Målet er, at MedCom til enhver tid har tidssvarende tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer implementeringen af gældende lovgivning og myndighedskrav.

MedComs Informationssikkerhed har betydning for tilgængeligheden, integriteten og fortroligheden af den digitale kommunikation i sundhedssektoren.

De oplysninger, som behandles i SDN, VDX og KIH, vil i mange tilfælde indeholde følsomme personoplysninger, som betyder, at der er et lovgivningsmæssigt og etisk ansvar for at beskytte disse i forhold til fortrolighed og dermed uvedkommendes kendskab.

MedCom er ligeledes ansvarlig for integriteten af personoplysninger og informationer i forbindelse med behandling og transmission. Informationer skal så vidt muligt sikres mod forvanskning, da modtagerne af de transmitterede sundhedsoplysninger træffer kritiske og livsvigtige beslutninger på baggrund af disse og som led i deres arbejde. Såfremt informationer ikke er pålidelige, vil dette skade tilliden til MedCom og samarbejdet mellem de tilknyttede parter.

Informationssikkerhedspolitikken må ikke udgøre en hindring for tilgængeligheden af personoplysninger og informationer, der indgår i behandlingen af patienter af autoriseret behandlingspersonale.

3. Omfang og gyldighedsområde

Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på driften og brugen af SDN, VDX og KIH. Dette gælder også personoplysninger og informationer, som MedCom er databehandlere af.

Informationssikkerhedspolitikken omfatter alle medarbejdere i MedCom og underleverandører til MedCom af SDN, VDX og KIH.

4. Risikovurdering og -håndtering

MedComs informationssikkerhedspolitik sætter rammerne for sikkerhedsniveauet, som MedCom leverer via sine leverancer.

Målene fastlægges på baggrund af periodiske vurderinger af forretningsmæssige informationssikkerhedsrisici, som MedCom gennemfører på vegne af og i samarbejde med repræsentanter for de dataansvarlige.

Det skal gennem løbende risikovurderinger sikres, at de personoplysninger og informationer, som MedCom er ansvarlige for, er tilgængelige og forbliver fortrolige, når de er vurderet som værende af fortrolig karakter samt fremstår med korrekt indhold.

Samtidig skal det sikres, at ressourcer til minimering af de identificerede risici prioriteres og allokeres til de områder, hvor MedCom kan tilføre den største værdi.

MedCom fastlægger som følge heraf et sikkerhedsniveau med følgende mål:

- Der udføres årligt en it-revision af MedCom og MedComs kritiske leverandører med henblik på at sikre, at MedCom lever op til den gældende Databeskyttelseslovgivning
- Der skal som minimum en gang årligt gennemføres it-risikovurderinger
- Data skal beskyttes mod uautoriseret fysisk og logisk adgang
- Data skal sikres mod tab af fortrolighed og integritet
- Der skal implementeres tilstrækkelige sikkerhedsforanstaltninger til at imødegå identificere risici og reducere dem til et acceptabelt risikoniveau.
- Medarbejdere skal trænes for at sikre efterlevelse af denne Informationssikkerhedspolitik
- Der skal styres og følges op på leverandører til sikring af stabil og sikker drift
- Der skal etableres it-beredskab, der sikrer fokuseret styring mod retablering af systemer og data, så vidt muligt samt nødplaner, der sikrer den fortsatte afvikling af forretningsprocesser
- Der skal sikres efterlevelse af lovgivning og myndighedskrav. Af relevant national lovgivning kan nævnes Databeskyttelsesloven, herunder Persondataforordningen (GDPR) samt alle tilknyttede bekendtgørelser og cirkulærer – samt i relevant omfang dansk implementering af 'Network and Information Systems Directive 2' (NIS2)
- Den anerkendte standard for styring af Informationssikkerhed, ISO/IEC 27001:2013 skal efterleves på relevante områder

- Der skal gennemføres revurderinger af MedComs ledelsessystem vedrørende forbedring af ledelsessystemet og Informationssikkerheden
- Der skal gennemføres monitorering og rapportering af sikkerhedshændelser

Informationssikkerhedspolitikken uddybes i specifikke politikker og procedurer, der dækker prioriterede områder inden for ISO27001:2013. MedCom er ansvarlig herfor.

5. Sikkerhedsbevidsthed

Efterlevelse af politikker og procedurer påhviler topledelsen. Linjeledelsen har ansvaret for, at processer og procedurer, der understøtter Informationssikkerheden, efterleves i medarbejdernes daglige arbejde - herunder at sikre, at medarbejderne gennemgår den nødvendige træning, samt at de nødvendige ressourcer allokeres ud fra en overordnet vurdering.

Alle medarbejdere i MedCom har et ansvar for at beskytte personoplysninger, informationer og informationssystemer. Alle medarbejdere skal derfor både i forbindelse med og løbende under ansættelsen være orienteret om kravene til det generelle sikkerhedsniveau samt de regler, som er specifikke for den enkelte medarbejders opgaver.

Der følges løbende op på sikkerhedsbevidstheden hos medarbejderne for at kunne opretholde det ønskede sikkerhedsniveau, og Informationssikkerheden skal integreres i MedComs procedurer, så kravene efterleves som en naturlig del af arbejdet.

6. Dispensation fra informationssikkerhedspolitikken

Dispensation fra Informationssikkerhedspolitikken og de tilhørende retningslinjer kan imødekommes på baggrund af en risikovurdering og eventuelt implementering af nødvendige kompenserende sikringsforanstaltninger.

Dispensationer skal godkendes af MedComs ledelse, inden handlinger kan gennemføres. Dispensationerne skal dokumenteres. Der vil ikke kunne gives dispensation i strid med gældende lovgivning, herunder Sundhedsloven, Persondataforordningen og Databeskyttelsesloven.

7. Leverandørforhold

Leverandører og underleverandører til SDN, VDX, KIH er underlagt MedComs krav til Informationssikkerhed og indgåede databehandleraftaler imellem MedCom og den pågældende leverandør. Disse forhold indgår i leverandørkontrakterne. Skærpelse af kravene til sikkerhed fra MedComs side, træder disse dog først i kraft ved næste kontraktperiode, medmindre kravet anses for at være af kritisk karakter.

MedCom følger op på leverandørers efterlevelse af Informationssikkerhedskrav på driftsstatusmøder samt ved risikovurdering, revisionserklæringer eller audit af leverancerne. Manglende overholdelse af Informationssikkerhedskravene håndteres i overensstemmelse med kontraktens bestemmelser.

8. Brud på informationssikkerheden

Hvis en medarbejder har mistanke om eller kan konstatere brud på Informationssikkerheden, skal dette hurtigst muligt rapporteres til MedComs ledelse, MedComs DPO, MedComs systemforvaltningsteam, MedComs sikkerhedsansvarlig eller nærmeste leder.

Overtrædelse af Informationssikkerhedspolitikken og de heraf afledte retningslinjer behandles efter nærmere vurdering af nærmeste leder og i yderste konsekvens efter de gældende personaleretlige regler og personalehåndbogen.

9. Godkendelse og kommunikation

Informationssikkerhedspolitikken gældende for MedComs systemforvaltning af SDN, VDX og KIH godkendes af MedComs styregruppe.

Den revurderes hvert år på baggrund af opdaterede risikovurderinger eller i forbindelse med væsentlige ændringer af MedComs systemforvalteransvar.

Informationssikkerhedspolitikken gøres tilgængelig på MedComs website.

Behandlet i MedComs styregruppe den 27. november 2024.

Revisions Historik

Version	Forfatter	Dato	Bemærkning
2.2		20.02.17	
2.3	TGJ	01.06.18	Justering under punkt 4 med indførelse af Databeskyttelsesloven i stedet for Persondataloven.
2.4	LAH/TGJ	18.08.21	Sproglige ændringer og præciseringer.
2.4	TGJ	28.08.22	Behandlet i MedComs styregruppe. Ingen ændringer.
2.4	TGJ	14.12.23	Behandlet i MedComs styregruppe. Ingen ændringer.
2.4	TGJ	07.03.24	Behandlet i MedComs styregruppe. Ingen ændringer.
2.5	TGJ	27.11.24	Behandlet i MedComs styregruppe. Der er under pkt. 4 indsat reference til NIS2 under lovgivning, som MedCom i relevant omfang skal overholde.