MedComs informationssikkerhedspolitik

Version
2.2

Revisions Historik			
Version	Forfatter	Dato	Bemærkning
2.2		20.02.17	

INDHOLDSFORTEGNELSE

1 INDLEDNING

MedComs informationssikkerhedspolitik dækker MedComs systemforvaltningsansvar for Sundhedsdatanettet (SDN), videoknudepunktet (VDX) og Klinisk Integreret Hjemmemonitorering databasen (KIH Databasen) samt de interne it-systemer, som anvendes i MedComs opgave som systemforvalter. Politikken understøtter og udmønter MedComs vision og mission.

Styring af informationssikkerhed er en vigtig opgave for MedCom som forvalter af 3 fællesoffentlige sundheds-it-systemer. MedCom har derfor som målsætning at efterleve relevante dele af ISO27001:2013. Informationssikkerhedspolitikken udgør den overordnede ramme og målsætning for informationssikkerheden i MedCom.

Informationssikkerheden styres efter en klart defineret model som angivet i MedComs ISMS. Det påhviler altid den ansvarlige leder at sørge for, at informationssikkerhedspolitikken efterleves.

MedCom er ansvarlig for, at de 3 fællesoffentlige sundheds-it-systemer er sikret i henhold til lovgivningen for behandling af persondata og mod brud på datas fortrolighed, integritet og tilgængelighed. MedComs ansvar er fastlagt i databehandleraftaler med de dataansvarlige.

2 INFORMATIONSSIKKERHEDSPOLITIKKENS FORMÅL OG MÅLSÆTNINGER

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

Formålet med informationssikkerhedspolitikken er at understøtte en sikker anvendelse af SDN, VDX og KIH Databasen efter en fastlagt styring af informationssikkerheden i MedCom. Politikken skal medvirke til, at data beskyttes mod brud på fortroligheden, integriteten og tilgængeligheden.

Det er et mål for MedCom, at styringen af informationssikkerheden vedvarende vedligeholdes og forbedres der, hvor det findes nødvendigt, så MedCom til enhver tid har tidssvarende tekniske og organisatoriske sikkerhedsforanstaltninger, som efterlever lovkrav og myndighedskrav til MedComs systemforvaltning. MedCom vil fremstå som en pålidelig systemforvalter, som behandler informationer sikkert.

Informationssikkerhedspolitikken må ikke udgøre en hindring for tilgængeligheden af kritiske helbredsinformationer, da sundhedspersoner med et behandlingsansvar altid skal kunne udveksle disse på en sikker måde i overensstemmelse med lovgivningen. Systemerne og data skal være tilgængelige, hvor der er behov for det og for de relevante brugere.

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

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

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 Database. Dette gælder også informationer, som MedCom er databehandlere af.

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

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 grundlæggende sikres, at de data 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 i form af sikkerhed og kvalitet.

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 persondatalovgivning
- 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 national lovgivning samt EU-direktiver, indtil de er omsat i dansk lovgivning. Af relevant national lovgivning kan nævnes Persondataloven, sikkerhedsbekendtgørelsen og Sundhedsloven.
- 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 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 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 og Persondataloven.

7 LEVERANDØRFORHOLD

Leverandører til SDN, VDX, KIH og MedComs interne systemer 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, med mindre kravet anses for at være af kritisk karakter.

MedCom følger op på leverandørers efterlevelse af informationssikkerhedskrav på driftsstatusmøder samt ved risikovurdering og 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 systemforvaltningsteam 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 Databasen godkendes af MedComs styregruppe. Den revurderes hvert år på baggrund af opdaterede risikovurderinger eller i forbindelse med væsentlige ændringer af MedComs systemforvalteransvar.

Informationssikkerhedspolitikken kommunikeres til alle MedComs ansatte, leverandører, tilsluttede organisationer, styregruppen og brugergrupper.

Informationssikkerhedspolitikken gøres tilgængelig på MedComs website.

Godkendt af MedComs styregruppe den 3. marts 2017