Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	22. april 2021

Sak 046-2021

Mål og strategi for informasjonssikkerhet i Helse Sør-Øst – overordnet styrende dokument

Forslag til vedtak:

Styret slutter seg til fremlagt overordnet styrende dokument for informasjonssikkerhet i Helse Sør-Øst.

Hamar, 13. april 2021

Cathrine M. Lofthus
administrerende direktør

1. Hva saken gjelder

Det overordnede styrende dokumentet for mål og strategi for informasjonssikkerhet i Helse Sør-Øst, inneholder føringer om at informasjonssikkerhet skal være integrert i helseforetakenes helhetlige styringssystem og at beslutninger om risiko innen informasjonssikkerhet tas i linjen på riktig ledelsesnivå.

Saken ble behandlet i styremøtet 11. mars 2021, styresak 026-2021. Dokumentet er nå justert på bakgrunn av de innspill som kom frem i styremøtet. Det foreslås at styret slutter seg til oppdatert overordnet styrende dokumentet for informasjonssikkerhet i Helse Sør-Øst.

2. Hovedpunkter og vurdering av handlingsalternativer

Spesialisthelsetjenesten er, som øvrige deler av samfunnet, stadig mer avhengig av digitale løsninger. Det er sentralt for måloppnåelsen at informasjonssikkerheten ivaretas på en god måte, og at ulike risikoer veies mot hverandre.

Videreutvikling av ledelsessystemet for informasjonssikkerhet er et kontinuerlig arbeid. Tydeliggjøring av overordnede rammer er viktig for det videre forbedringsarbeidet.

Det er i eForvaltningsforskriften krav om å ha beskrevet mål og strategi for informasjonssikkerhet. Videre er det anbefalt at informasjonssikkerhet er en integrert del av helseforetakenes helhetlige styringssystem[1]. Digitaliseringsdirektoratet er av Kommunal- og moderniseringsdepartementet pekt ut til å gi anbefalinger innen området ledelsessystem for informasjonssikkerhet. De anbefaler å benytte kriterier for å akseptere risiko, der beslutninger om risiko tas i linjen på riktig ledelsesnivå.

Overordnet styrende dokumentet for informasjonssikkerhet er utarbeidet som en del av en pågående revisjon av ledelsessystemet for informasjonssikkerhet[2] og er basert på anbefalingene som er omtalt ovenfor. Dokumentet tar også hensyn til funn fra Riksrevisjonens forvaltningsrevisjon av helseforetakenes forebygging av angrep mot sine IKT-systemer. Dokumentet vil bli brukt som ramme for videre revisjonsarbeid av ledelsessystem for informasjonssikkerhet og beskriver mål og strategi for informasjonssikkerhet. Dagens mål og strategi er beskrevet i ledelsessystemet for informasjonssikkerhet, men disse har ikke vært styrebehandlet.

[1] https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_3#KAPITTEL_3
[2] https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

Dokumentet ble presentert og diskutert i styremøtet 11. mars. Basert på innspill og kommentarer i styremøtet er dokumentet revidert. De vesentligste endringer i det oppdaterte utkastet er følgende:

- Utkastet beskriver innledningsvis litt om hva informasjonssikkerhet handler om og dokumentets plassering i virksomhetsstyringen
- Utkastet gir under avsnittet om mål for informasjonssikkerhet noen føringer for håndtering av målkonflikter, ved å understreke at pasientsikkerhet og helseberedskap skal tillegges stor vekt. Slike konflikter vil typisk kunne gjelde krav til tilgangsstyring, hvor tilgjengelighets- og konfidensialitetskrav kan stå mot hverandre
- Utkastet adresserer i avsnittet om strategi for informasjonssikkerhet hvordan ulike interesser mellom helseforetak (herunder Sykehuspartner HF) skal håndteres, og legger opp til at Helse Sør-Øst RHF skal kunne gi føringer for ivaretakelse av informasjonssikkerhet i regionen. Dersom et helseforetak ønsker å avvike fra regionale føringer, skal saken forelegges helseforetakets styre. Denne føringen er en speiling av krav i oppdrags- og bestillingsdokument for 2020, jf. styrevedtak i sak 107-2019, som omhandlet tilsvarende håndtering av eventuelle avvik for regionale IKT-føringer Dersom to helseforetak ikke kommer til enighet om hvorvidt en risiko kan aksepteres, skal saken drøftes med Helse Sør-Øst RHF.

I tillegg er det gjort enkelte mindre endringer; herunder nevnes enkelte sentrale regelverk, det presiseres at *krav til* informasjonssikkerhet skal kommuniseres, det klargjøres at krav til ansvar og kompetanse både gjelder i linjen og i fagmiljøer, krav til hva evaluering av tiltak skal omfatte er presisert, og det understrekes at risikoaksept krever et tilstrekkelig beslutningsgrunnlag.

Det er videre stilt overordnede krav til ledelsessystemet. Kravene vil bli operasjonalisert i underliggende dokumenter, både regionalt og lokalt. Blant annet vil det bli utarbeidet kriterier for å akseptere risiko, ansvar og organiseringen av området vil bli beskrevet, og ulike prosesser vil bli definert. Prosesser som blir definert vil for eksempel omhandle hvordan tilgang til IKT-systemer tildeles. Det vil også iverksettes opplæringstiltak.

3. Administrerende direktørs anbefaling

God informasjonssikkerhet er en forutsetning for god pasientbehandling. Administrerende direktør er opptatt av hvordan risiko forbundet med informasjonssikkerhet håndteres på en måte som gir trygge og effektive helsetjenester. Pasienter og pårørende forventer at opplysninger er tilgjengelige for helsepersonell og at informasjonen behandles på en trygg og sikker måte.

Foreslått overordnet styringsdokumentet for informasjonssikkerhet er i tråd med offentlige anbefalinger innen området og setter rammene for et informasjonssikkerhetsarbeid som skal ivareta informasjonsbehandlingen med tanke på helseforetakenes samlede mål. Dokumentet tar også hensyn til funn i Riksrevisjonens forvaltningsrevisjon av helseforetakenes forebygging av angrep mot sine IKT-systemer.

Dokumentet er oppdatert etter tilbakemeldinger fra forrige styrebehandling, og har vært fremlagt for de administrerende direktørene i helseforetakene som har sluttet seg til det oppdaterte dokumentet.

Administrerende direktør anbefaler at styret slutter seg til framlagte overordnet styrende dokument for informasjonssikkerhet i Helse Sør-Øst og at dokumentet gjøres gjeldende som foretaksgruppens øverste styrende dokumentet for informasjonssikkerhet.

Trykte vedlegg:

- Mål og strategi for informasjonssikkerhet i Helse Sør-Øst – overordnet styrende dokument

Utrykte vedlegg:

- Ingen