SYKEHUSINNKJØP

Sak 077-2017

Saksfremlegg til styret i Sykehusinnkjøp

Informasjonssikkerhet

Møtedato:	12.oktober	
Tidligere behandlet i styret/saksnr.	59/2017	
Type sak (orienteringssak, diskusjonssak, beslutningssak, temasak)	Orienteringssak	

Forslag til vedtak

1. Styret tar saken til orientering

2. Styret ber administrerende direktør komme tilbake til styremøte i januar med en plan for etablering av internkontroll for informasjonsikkerhet

Vadsø, 4.oktober 2017

Kjetil M. Istad
Administrerende direktør

1. Hva saken gjelder

I styresak 59/2017 ble styret informert om følgende:

«På initiativ fra styreleder har Sykehusinnkjøp HF starter arbeidet med en gjennomgang av foretakets rutiner for tilgangsstyring, nødvendig inngåelse av databehandleravtaler, gjennomføring av risiko- og sårbarhetsanalyser, etterfølgende kontrollregimer for logging og monitorering samt andre forhold tilknyttet informasjonssikkerhet. Det tas sikte på å legge frem styresak om dette på styremøte i oktober.»

Formålet med denne saken er å gi en status på fremdrift i arbeidet, samt vise hvilken plan man jobber etter for å få gjennomført bestillingen fra styreleder.

2. Hovedpunkter og vurdering av handlingsalternativer

Ny IT-sjef tiltrådte 1.september. Han har tatt rollen som informasjonssikkerhetsansvarlig og er dermed ansvarlig for gjennomføringen av oppdraget. Øvrige ressurser som bidrar til arbeidet er stabsleder og Kvalitetsleder.

Alle rutiner som bestillingen omfatter er vurdert med utgangspunkt i følgende spørsmål:

- Hvilke rutiner eksisterer i dag?
- Hva gjøres faktisk i dag?
- Hva må på plass for at rutinene skal oppfylle lovkrav?
- Hvordan skal man få etablert og iverksatt rutiner som oppfyller lovkrav?

I forhold til dagens situasjon har Sykehusinnkjøp HF få rutiner som oppfyller anbefalt praksis eller gjeldende krav. Det er stor bevissthet rundt disse mangler, og risiko reduseres derfor basert på godt skjønn og opplevd ansvar hos kompetente ansatte.

For å få etablert nødvendige rutiner om informasjonssikkerhet har man valgt å legge til grunn anbefalinger fra Direktoratet for forvaltning og IKT (DIFI). DIFI er Statens kompetansemiljø for informasjonssikkerhet og har utarbeidet en egen veileder som beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet. Innholdet i veilederen blir vurdert til å være anbefalt praksis på dette området.

Det er videre vurdert som overordnet viktig at dette arbeidet ikke organiseres som et selvstendig prosjekt, men må inngå i arbeidet rundt internkontroll, kvalitetsoppfølging og gevinstrealisering. I tillegg bør implementering så langt det er mulig bygge på systemstøtte og automatisering, forankret i referansearkitektur og nasjonale føringer for standardisering og samhandling.

For å sikre gjennomføring og fremdrift, bør arbeidet med å etablere internkontroll for informasjonsikkerhet forankres/følges opp i den ordinære virksomhetsplanen med tilhørende rapportering.

DIFI's veileder inneholder en ti-punktsplan som beskriver relevante aktiviteter som må gjennomføres for å etablere interkontroll på informasjonssikkerhetområdet:

Avklare behov og lage en plan
1 Analysere status
2 Planlegge etablering/forbedring

Få på plass det viktigste
3 Utforme/forbedre overordnede styrende dokumenter
4 Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen
5 Utforme og gjennomføre grunnopplæring
6 Etablere system for hendelses- og avvikshåndtering

Skap en god platform for internkontrollen
7 Etablere fellessikring og synliggjøre tilleggssikring
8 Etablere rammeverk for dokumentasjon

Lag et godt grunnlag for sentrale systematiske aktiviteter
9 Identifisere typiske oppgave- og informasjonstyper
10 Felles analyse av eksterne krav

Sykehusinnkjøp HF gjennomfører nå aktiviteter tilknyttet punkt 1 i denne planen. Virksomhetens organisering per i dag innebærer at divisjonen ikke har felles prosesser, systemstøtte etc. Det har derfor vært viktig å få kartlagt hver divisjon for seg for å få nødvendig oversikt over status. I forbindelse med prosjekt for etablering av felles plattform for IKT tjenester i Sykehusinnkjøp HF gjennomføres det derfor nå aktiviteter for å kartlegge staus per divisjon for følgende:

- Datakilder
- Informasjonstyper
- Systemstøtte
- Ansvars- og behandlerroller

IT-sjef vil koordinere aktiviteter i samarbeid med de enkelte divisjoner for å fullføre klassifisering av funksjonsområder og kartlegging av systemstøtte.

Fremdrift er betinget av prioritet og tilordning av ressurser, men er tett knyttet til etablering og utrulling av felles IKT-plattform. Den operative delen av støtteprosesser innefor IKT-området (ITIL) må samordnes med leverandør av driftstjenesten, Helse Nord IKT. Prosedyrer, rollebeskrivelser og ansvarsforhold vil inngå i Sykehusinnkjøp HF system for internkontroll.

Etableringsaktiviteter 1 og 2 er planlagt fullført ved inngangen av 2018.

3. Anbefaling

Det anbefales at styret tar saken til orientering og at styret ber administrerende direktør komme tilbake med plan for etablering av internkontroll for informasjonsikkerhet på styremøte i januar.

Utrykte vedlegg

- http://internkontroll.infosikkerhet.difi.no
- https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur/prinsipper