SYKEHUSET ØSTFOLD

STYREMØTE 19. september 2016

Styresak nr.:	45-16	Sakstype:	Beslutningssak
Saksnr. arkiv:	16/02005		

Konsernrevisjon av leverandørenes tilgang til helse- og personopplysninger i medisinsk-teknisk utstyr (MTU)

Sammendrag:
Konsernrevisjonen har gjennomført en revisjon for å kartlegge og vurdere om leverandørenes tilgang til helse- og personopplysninger i MTU fyller kravene til informasjonssikkerhet. Det er avdekket enkelte svakheter og utarbeidet en handlingsplan med målrettede forbedringstiltak.

Forslag til vedtak:

1. Styret tar konsernrevisjonens rapport 8/2016 til etterretning.
2. Styret ber administrerende direktør følge opp tiltakene i handlingsplanen og gi styret en orientering om status i løpet av våren 2017.

Sarpsborg, den 05.09.2016

Just Ebbesen
administrerende direktør

Vedlegg:
1. Revisjonsrapport 8/2016 Leverandørenes tilgang til helse- og personopplysninger i medisinsk-teknisk utstyr
2. Handlingsplan etter konsernrevisjon

1. Administrerende direktørs anbefalinger / konklusjoner

Sykehuset Østfold (SØ) ser at revisjonen har vært nyttig for å sikre etablering av tilstrekkelig dokumentasjon, styring og kontroll med informasjonssikkerheten knyttet til helse- og personopplysninger. SØ har i samarbeid med Sykehuspartner (SP) definert roller og ansvar i det viktige arbeidet med informasjonssikkerheten knyttet til medisinsk-teknisk utstyr.

Administrerende direktør anbefaler at styret tar rapporten fra Konsernrevisjonen til etterretning og at handlingsplanen med tiltak og frister godkjennes og følges opp i tråd med regionale føringer for dokumentasjon, kontroll og styringssystemer.

2. Faktabeskrivelse

Medisinsk-teknisk utstyr (MTU) inneholder stadig mer sensitive opplysninger vedrørende pasienters helse- og persondata, og MTU integreres i økende grad med øvrige IKT-systemer. Bruk og forvaltning av disse opplysningene er underlagt strenge krav til informasjonssikkerhet. De ulike aktørene må ha definerte roller og ansvar knyttet til ivaretakelse av informasjonssikkerheten.

Helse Sør-Øst RHF (HSØ) har gjennomført en rekke tiltak i foretaksgruppen for å ivareta informasjonssikkerheten knyttet til MTU. SØ har i forbindelse med Prosjekt nytt østfoldsykehus (PNØ) vært pilot for flere av tiltakene.

Konsernrevisjonen i Helse Sør-Øst har gjennomført en revisjon i SØ for å kartlegge og vurdere om leverandørenes tilgang til helse- og personopplysninger i MTU er i tråd med kravene til informasjonssikkerhet, om de er regulert i avtaler, og om det er tilstrekkelig kontroll og hensiktsmessig tilgangsstyring.

Rapporten beskriver positive funn, svakheter som er avdekket under revisjonen og anbefalinger om tiltak til forbedring.

Følgende problemstillinger er belyst:

1. Er det etablert et system hvor krav til informasjonssikkerhet i MTU inngår i anskaffelsesprosessen og blir ivaretatt i avtaler med MTU-leverandører?
2. Blir kravene til informasjonssikkerhet operasjonalisert og etterlevd?

Revisjonen har vist at det er etablert et system i SØ for informasjonssikkerhet knyttet til MTU-leverandørenes tilganger til helse- og personopplysninger, som ikke er fullstendig i forhold til kravene i normen. Det pågår et regionalt arbeid med utvikling av felles maler for å sikre at det arbeides helhetlig og målrettet med informasjonssikkerhet i henhold til normens krav.

Sykehuspartner har, sammen med SØ, ansvar for at tildeling av rettigheter til MTU-leverandørene er satt i system. Det er en avklart ansvars- og rolledeling mellom SØ og SP.

SP er databehandler for alt IKT-utstyr som kjører på SP sin infrastruktur. Dette omfatter alt MTU ved SØ som er koblet til nett. Ansvars- og oppgavefordelingen mellom SØ og SP er beskrevet og

nedfelt i en tjenesteavtale. Det er SP som har ansvar for å tegne avtale med alle leverandører som skal ha fjernaksess til MTU i SØ, mens det er SØ som autoriserer brukere og bestiller tilganger til leverandørportalen.

Det er i revisjonen avdekket svakheter i SØ sin internkontroll og styringssystemet knyttet til informasjonssikkerhet. Dokumentasjonen er ikke oppdatert og ikke egnet for god styring og kontroll. Det pågår et regionalt arbeid for å utarbeide en mal for styringssystemet, og SØ arbeider med dokumentasjonen i tråd med de nye malene. Dokumentene var ikke ferdigstilt på revisjonstidspunktet.

SØ sine prosedyrer for innkjøp og anskaffelse inneholder ikke konkrete aktiviteter som skal sikre kravene til informasjonssikkerhet i kravspesifikasjonene for MTU-anskaffelser og videre i serviceavtaler. Revisjonen viser at kravene til informasjonssikkerhet i varierende grad er regulert i de undersøkte avtalene.

Ved gjennomgang av avtaler for eldre utstyr (anskaffet før PNØ) er det avdekket at noe av utstyret mangler tjenestebeskrivelser. Dette kan føre til at det kan oppstå usikkerhet rundt vesentlig informasjon med hensyn til drift og forvaltning av utstyret.

Revisjonen har påvist svakheter ved SØs styring og kontroll med MTU-leverandørenes aktivitet og begrenset mulighet til å forhindre og avdekke mulig misbruk av sensitiv informasjon når leverandørene ikke benytter leverandørportalen. Dette medfører at SØ i stor grad blir avhengig av leverandørens interne kontrollrutiner med tanke på informasjonssikkerhet, selv om leverandøren har avgitt taushetserklæring og underskrevet databehandleravtale.

Avvikshåndteringen, ledelsens gjennomgang (LGG) og risikovurderinger er satt i system og gjennomføres i eksisterende strukturer. Det er derimot ikke gjennomført sikkerhetsrevisjoner og oppfølging av databehandler på MTU-området etter PNØ.

Konsernrevisjonen har på bakgrunn av funnene kommet med anbefalinger til tiltak som er beskrevet i vedlagte handlingsplan.

3. Administrerende direktørs vurderinger

Administrerende direktør vurderer at revisjonen har vært viktig etter pilotering i PNØ/SØ og peker på svakheter som må ivaretas i det regionale arbeidet med felles maler.

Arbeidet med å rette opp påpekte svakheter, samt å følge opp konsernrevisjonens anbefalinger er godt i gang. Handlingsplanen, som legges fram sammen med rapporten, vurderes å være dekkende for konsernrevisjonens anbefalinger om tiltak og viser hvem som er ansvarlig for tiltaket og frist for oppfølging.