Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	16. november 2017

SAK NR 111-2017

ORIENTERINGSSAK - STATUS IKT-INFRASTRUKTURMODERNISERING OG ARBEIDET MED INFORMASJONSSIKKERHET I HELSE SØR-ØST

Forslag til vedtak:

Styret tar redegjørelsen om status IKT-infrastrukturmodernisering og arbeidet med informasjonssikkerhet til orientering.

Oslo, 9. november 2017

Cathrine M. Lofthus
administrerende direktør

1. Hva saken gjelder

Sykehuspartner HF har arbeidet med oppdraget gitt i foretaksmøtet 31. mai 2017, hensyntatt forholdene som fremkom i PWC-rapporten datert 22. juni 2017 og Helse Sør-Øst RHFs styrevedtak i sak 077-2017 behandlet i styremøte 28. juni 2017.

Sykehuspartner HF er gitt i oppdrag å stille IKT-infrastrukturmoderniseringen i bero. Videre skal Sykehuspartner HF utrede mulige alternative løsninger for videre modernisering av IKT-infrastrukturen. Oppdraget inkluderte også utarbeidelse av en plan for styrket tilgangsstyring og en bedre metodikk for risiko- og sårbarhetsanalyser.

I tillegg er det stilt krav til aktiviteter og prosjekter som er viktig for å bedre informasjonssikkerhet og sørge for sikker og stabil drift, herunder backup, lagring og innføring av analyseplattformen for å bedre informasjonssikkerheten gjennom sporing og logging.

Utover aktiviteter iverksatt av Sykehuspartner HF har også Helse Sør-Øst RHF iverksatt ulike aktiviteter relatert til informasjonssikkerhet.

Det ble i styremøte 14. september 2017 i sak 090 – 2017 gitt en orientering om status IKT-infrastrukturmodernisering og arbeidet med informasjonssikkerhet i Helse Sør-Øst

Hensikten med denne styresaken er å gi en statusrapport basert på arbeidet som skjer i regi av Sykehuspartner HF og Helse Sør-Øst RHF. Omtalen av arbeidet som skjer i regi av Sykehuspartner HF bygger på Sykehuspartners styresak 063-2017 *Oppfølging av vedtak fra foretaksmøte Sykehuspartner HF 31. mai 2017,* som ble behandlet i styremøte i Sykehuspartner HF 12. oktober 2017. Sykehuspartner HFs styresak ble oversendt til Helse Sør-Øst RHF 17. oktober 2017 og styresaken følger som vedlegg til denne saken.

2. Hovedpunkter og vurdering av handlingsalternativer

2.1 Bakgrunn

Sykehuspartner HF har arbeidet med oppdraget gitt i foretaksmøtet 31. mai 2017, hensyntatt forholdene som fremkom i PWC-rapporten datert 22. juni 2017 og Helse Sør-Øst RHFs styrevedtak i sak 077-2017 behandlet i styremøte 28. juni 2017.

Vedlagt denne saken er en oversikt (utarbeidet av Sykehuspartner HF som vedlegg til deres styresak 063-2017) som gir en kort status på samtlige vedtakspunkter fra foretaksmøtet 31. mai. Det har vært arbeidet spesielt med to forhold – tiltak innen informasjonssikkerhet og personvern og status og veien videre for infrastrukturmoderniseringen, inkludert vurdering av alternative gjennomføringsmodeller innenfor og utenfor kontrakt med DXC.

2.2 Aktiviteter i regi av Sykehuspartner HF

Informasjonssikkerhet og personvern

God kontroll med informasjonssikkerhet og personvern er helt avgjørende premisser for vurderingene av fremtidig modell for arbeidet med infrastrukturmodernisering i Helse Sør-Øst.

Sykehuspartner HF påpeker i sin styresak at det er avhengigheter mellom arbeidet som utføres innen informasjonssikkerhet og personvern og videre standardisering og modernisering. Det påpekes videre at det har vært en prioritert aktivitet å tydeliggjøre sikkerhetsmessige forutsetninger for infrastrukturløsningen, med spesielt fokus på tilganger til helseopplysninger, beskyttelse av sensitive personopplysninger og helhetlig risikovurdering. Sykehuspartner HF redegjør for at grunnlag for vurderinger av modell for infrastrukturmodernisering er lov og forskrift, Direktoratet for e-helse sine anbefalinger, samt policyer og sikkerhetsarkitektur. Det redegjøres for at dette i praksis betyr at noen tiltak må være ferdigstilte før man kan innstille på moderniseringsalternativ, mens øvrige må ferdigstilles før standardiseringen og moderniseringen kan videreføres.

For samtlige tiltak må Sykehuspartner HF ha en troverdig og besluttet plan for hvordan avvik skal lukkes, og hvordan organisasjon, prosesser og teknologi skal spille sammen for å håndtere informasjonssikkerhet og personvern på en tilfredsstillende måte.

Sykehuspartner HF påpeker også i styresaken på at hoveddelen av tiltakene er arbeid som er nødvendig og ønskelig for regionen uavhengig av moderniseringsalternativ og som er en del av Sykehuspartner HFs generelle styrking av informasjonssikkerhetsområdet.

Det er i eget vedlegg (vedlegg 1) til styresaken i Sykehuspartner HF, gitt orientering om status for gjennomføringen av oppdraget gitt i foretaksmøte 31. mai 2017.

Særskilt om tilgangskontroll

Svakheter i styring og kontroll med tilganger var et av de viktigeste og mest alvorlige funnene i PWCs gjennomgang.

Det fremheves spesielt i styresaken at Sykehuspartner HF vil styrke sin satsning på tilgangsstyring for å kunne ivareta sitt ansvar innen dette området uavhengig av valg av modell. Videre vil fagmiljøene innen informasjonssikkerhet styrkes ytterligere, og det er lagt inn en økning av ressurser i budsjettet for 2018.

Det påpekes også i styresaken at uavhengig av driftsmodell vil Sykehuspartner HF fortsatt være ansvarlig for tilgangsstyring og selv ha utøvende kontroll på at tilganger gis i henhold til lov, forskrift og gjeldende retningslinjer. Sykehuspartner HF vil ved hjelp av organisering, prosesser og tekniske løsninger sikre tilstrekkelig identifikasjon, autentisering og autorisasjon for alle brukere, både internt i Sykehuspartner HF, ansatte hos de behandlingsansvarlige og for eksterne leverandører, innbyggere og andre samarbeidspartnere.

Særskilt om backup og lagring

Sykehuspartner HF er bedt om å iverksette nødvendige tiltak for å opprettholde sikker og stabil drift. I denne sammenheng er det pekt særskilt på blant annet backup-løsninger og lagring. Helse Sør-Øst RHF ga i brev datert 13. juli 2017 Sykehuspartner HF fullmakt til å gjennomføre investeringer for 35 millioner kroner knyttet til strakttiltak innen backup og lagring. Av Sykehuspartner HFs styresak fremgår det at for de mest kritiske tjenestene (kritikalitet 1 tjenester) vil backup og lagring være på plass i midten av oktober, mens de resterende tjenestene vil være på plass innen utgangen av året.

Sikker og stabil drift

Etter den opprinnelige planen skulle DXC overta innkjøp og utplassering av periferi- og lagringsutstyr fra mai 2017. Sykehuspartner HF ble både i juli og i august innvilget finansiering for bl.a. å kunne håndtere investeringer knyttet til sikker og stabil drift. I oktober kom det en ny henvendelse fra Sykehuspartner HF som er til behandling i Helse Sør-Øst RHF.

Status og veien videre for infrastrukturmoderniseringen

Sykehuspartner HF utreder mulige løsninger for videre infrastrukturmodernisering både innenfor og utenfor inngått kontrakt. Dette er omtalt nærmere i Sykehuspartner HFs styresak.

I saken er det redegjort for forutsetninger for de to alternativene som nå er under utredning og kriterier for vurdering av alternativene. En forutsetning er at alternativene oppfyller krav til informasjonssikkerhet og personvern, og det arbeides aktivt med å tydeliggjøre og konkretisere innholdet i denne forutsetningen.

Sykehuspartner HF påpeker i sin styresak at det er et omfattende og krevende arbeid som skal gjøres før anbefaling kan gis. Det legges stor vekt på å involvere og informere for å forankre arbeidet som gjøres. En troverdig prosess som gir et godt grunnlag for en anbefaling og vedtak, er sentralt for å skape tillit til det valget som gjøres og legger et godt grunnlag for gjennomføringsevnen.

2.3 Aktiviteter i regi av Helse Sør-Øst RHF

Uavhengig av arbeidet som pågår i Sykehuspartner HF er det igangsatt aktiviteter i regionen knyttet til informasjonssikkerhet. Dette er aktiviteter som dels er oppfølging knyttet til revisjoner og tilsyn og dels aktiviterer som har fått forsterket fokus som en følge av infrastukturmoderniseringsprosjektet og avtalen med ekstern leverandør.

Metodikk risikovurdering

Helse Sør-Øst RHF har i samarbeid med Sykehuspartner HF igangsatt et arbeid for å etablere rammer og opplegg for en forbedret metodikk for risiko- og sårbarhetsanalyser.

Prosjekt for statistisk logganalyse knyttet til elektronisk pasientjournal

Systematisk loggkontroll av oppslagslogger i behandlingsrettede helseregistre er en lovpålagt oppgave. Per i dag gjennomføres det stikkprøvekontroll, men dette omfatter kun et meget lite volum. Det er således behov for å etablere et effektivt verktøy for å oppfylle lovens krav til systematikk i loggkontrollen.

Det er besluttet å etablere et felles prosjekt mellom Helse Nord, Helse Midt-Norge og Helse Sør-Øst for å få implementert et system for statsitisk logganalyse (mønstergjenkjenning). Det er etablert et samarbeid med Norsk Helsenett knyttet til realisering av prosjektet. Basert på tilbakemeldinger fra de øvrige regionene vil prosjektet sannsynligvis realiseres først i Helse Sør-Øst.

Regionalt sikkerhetsråd

Regionalt sikkerhetsfaglig råd og regionalt risikovurderingsteam har fungert over flere år, men har ikke hatt tydelig nok forankring og et klart mandat. Det arbeides med å utarbeide mandat, avklare roller og ansvar, samt med å sikre god forankring hos de administrerende direktørene i helseforetakene som databehandlingsansvarlige.

Oppfølging av Riksrevisjonens revisjoner

Riksrevisjonen har utført undersøkelser av helseforetakenes styring av tilgang til helseopplysninger/ tilgangsstyring til elektroniske pasientjournaler (Dok 3:2 (2014–2015)) og ivaretagelse av informasjonssikkerhet i medisinsk-teknisk utstyr (Dok 3:2 (2015–2016)). Undersøkelsene påviste flere avvik og Helse- og omsorgsdepartementet stilte krav om lukking av avvikene i foretaksmøter i både 2015 og 2016.

Helse Sør-Øst RHF har etablert seks hovedtiltak for å lukke avvik knyttet til tilgangskontroll i elektronisk pasientjournal (EPJ) og åtte hovedtiltak knyttet til informasjonssikkerhet i medisinsk teknisk utstyr (MTU). Innen EPJ-området er en stor del av tiltakene gjennomført, og der hvor tiltak ikke er gjennomført foreligger det planer. I all hovedsak vil tiltakene være gjennomført i løpet av høsten 2017 og våren 2018. Også innen MTU-området er mange av tiltakene gjennomført, men det gjenstår i større grad tiltak under planlegging.

Helse- og omsorgsdepartementet avholdt 30. oktober 2017 møte med de regionale helseforetakene hvor status for lukking av avvik ble gjennomgått. Helse Sør-Øst RHF vil som oppfølging av statusrapporteringen be helseforetakene melde tilbake skriftlig på status for arbeidet med lukking av avvik, samt be om konkrete tidsplaner for lukking av avvik der hvor det ikke forelå slike planer pr. 30. oktober 2017. Videre vil oppfølging av helseforetakenes planer for lukking av avvik inngå i oppfølgingsmøter med helseforetakene.

3. Brev fra Datatilsynet

Datatilsynet har i brev av 24.10.2017 til helseforetakene i Helse Sør-Øst gitt varsel om vedtak med overtredelsesgebyr på kr 800 000 for brudd på personvernlovgivningen knyttet til infrastrukturmoderniseringen.

De lovovertredelser og kritikkverdige forhold som er omtalt i Datatilsynets forhåndsvarsel, er i all hovedsak knyttet til manglende risikovurderinger, manglende ledelsesforankring og mangelfullt system for å sikre at helseforetakene blir satt i stand til å ta sitt lovpålagte ansvar som databehandlingsansvarlig. De forhold som fremkommer av datatilsynets brev er i tråd med de funn PwC tidligere har gjort i sine gjennomganger. Helse Sør-Øst RHF har som følge av den eksterne gjennomgangen til PwC allerede gjort tiltak med hensyn til forsterkning av risiko- og sårbarhetsanalyser. Dette er også gjenspeilet i styret for Helse Sør-Øst RHF sitt vedtak 24. mai, der det i pkt 4 ble vedtatt følgende:

«Styret ber styreleder avholde foretaksmøte i Sykehuspartner HF som sikrer at prosjektet stilles i bero, og at følgende arbeid prioriteres for å belyse hvordan videre infrastrukturmodernisering kan sikres:

- System for tilgangsstyring må gjennomgås, forsterkes og implementeres
- Metodikk for risiko- og sårbarhetsanalyser knyttet til informasjonssikkerhet må gjennomgås, forsterkes og implementeres
- Fornyede risiko- og sårbarhetsanalyser må gjennomføres og forankres med helseforetakene som databehandleransvarlige
- Nødvendige endringer knyttet til leveranse og leveranseplaner i kontrakten som ivaretar IKT-informasjonssikkerhet på en trygg og sikker måte må utredes
- Plan for styrking av styring, ledelse og gjennomføring av prosjektet må utarbeides»

Helse Sør-Øst RHF er i samarbeid med helseforetakene i regionen videre i gang med å se på hvordan risikovurderinger og ledelsesforankring generelt kan settes bedre i system i foretaksgruppen. Som datatilsynet påpeker bør det etableres rutiner som ivaretar helseforetakenes autonomi ved felles beslutninger, «for å sikre etterlevelse av kravene i personopplysningsforskriften i forbindelse med konsernovergripende avtaleinngåelser og i alle saker som har betydning for virksomhets plikter til å etterleve kravene i personopplysningsforskriftens kapittel 2».

I lys av Datatilsynets brev legger Helse Sør-Øst RHF til grunn at det også er nødvendig å se nærmere på hvordan risikovurdering og ledelsesforankring er satt i system på eksempelvis nasjonale initiativ som Helsenorge plattformen og andre steder der pasientopplysninger som helseforetakene er databehandlingsansvarlige for blir eksponert.

4. Administrerende direktørs anbefaling

Administrerende direktør konstaterer at Sykehuspartner HF arbeider med oppdraget gitt i foretaksmøte 31. mai 2017 og styrevedtak i Helse Sør-Øst RHF den 28. juni 2017. Det er igangsatt aktiviteter for å svare opp bestillingene og det rapporteres jevnlig til styret i Sykehuspartner HF.

Helse Sør-Øst RHF har dialog med Sykehuspartner HF om både det pågående arbeidet og for å sikre økonomiske midler og omprioriteringer til nødvendige investeringer.

Administrerende direktør vil igjen understreke at pasientene skal kunne føle seg trygge på at sensitive personopplysninger håndteres på en trygg og sikker måte. Det er viktig at det gjennomføres tiltak av betydning for informasjonssikkerhet på kort sikt og at det i arbeidet med å utrede alternativer for videre infrastrukturmodernisering legges til grunn at kravene som er stilt til informasjonssikkerhet innfris. Dette innebærer at de forholdene som er påpekt i PWCs rapport må løses og at informasjonssikkerhet, herunder tilgangsstyring- og kontroll, må håndteres i samsvar med de krav og forventninger som følger av styrebehandling i Helse Sør-Øst RHF og foretaksmøte med Sykehuspartner HF.

Arbeidet som Sykehuspartner HF har igangsatt for å kartlegge alle registre som foretaket behandler og hvilke personopplysninger som inngår i disse, er avgjørende for å kunne vurdere modell for infrastrukturmodernisering. Videre er det viktig at Sykehuspartner HF utreder hvilke funksjoner og oppgaver som må håndteres av foretaket i egen regi av hensyn til informasjonssikkerhet. Det må også utredes hvilke tilganger som kan gis til eksterne leverandører generelt sett.

Samtidig vil administrerende direktør påpeke at ledelsen i Sykehuspartner HF fortløpende må forsikre seg om at det er enn reell og bred involvering av ansatte/fagmiljøer og tillitsvalgte i det arbeidet som nå utføres med vurdering av de ulike alternativene for infrastrukturmodernisering.

Administrerende direktør vil prioritere regionale prosjekter og aktiviteter knyttet til informasjonssikkerhet og fortløpende vurdere behovet for tiltak og aktiviteter utover det som det er redegjort for i denne saken.

Direktoratet for e-helses arbeid knyttet til informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren er startet opp og leveransen til Helse- og omsorgsdepartementet vil legge premisser for modell for infrastrukturmodernisering. Både Helse Sør-Øst RHF, Sykehuspartner HF og helseforetakene i regionen har med deltagere inn i arbeidet. Direktoratet for e-helse har fått utsatt frist for sitt arbeid og skal levere sin utredning innen 1. desember 2017.

Sykehuspartner HF angir at resultatet av utredningene som pågår knyttet til modell for infrastrukturmodernisering og et fullstendig beslutningsgrunnlag vil kunne foreligge mot slutten av året. Administrerende direktør planlegger å gjennomføre en ekstern gjennomgang av de anbefalinger som kommer fra styret i Sykehuspartner HF før beslutningssak fremlegges for styret i Helse Sør-Øst RHF. Administrerende direktør vil holde styret løpende informert om det arbeidet som pågår knyttet til infrastrukturmodernisering og informasjonssikkerhet og anbefaler at styret tar saken til orientering.

Trykte vedlegg

- Sykehuspartner HF – styresak 063-2017 Oppfølging av vedtak fra foretaksmøte Sykehuspartner HF 31. mai.2017

Utrykte vedlegg:

- Ingen