HELSE SØR-ØST

Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	28. juni 2017

SAK NR 077-2017

IKT-INFRASTRUKTURMODERNISERING I HELSE SØR-ØST

Forslag til vedtak:

1. Styret understreker at pasientene skal være sikre på at sensitive personopplysninger håndteres på en trygg og sikker måte. En modernisering av IKT-infrastrukturen er helt nødvendig og vil være et viktig bidrag for å kunne ivareta hensynet til personvern og informasjonssikkerhet.

2. Styret tar den endelige rapporten fra PwC til etterretning og forutsetter at de påpekte svakheter følges opp gjennom det oppdraget som er gitt til Sykehuspartner HF i foretaksmøte 31. mai 2017. Dette gjelder i særlig grad aktiviteter som vil styrke personvern og informasjonssikkerhet, herunder arbeidet med å bedre tilgangsstyringen og forbedret metodikk for risiko- og sårbarhetsanalyser. Styret understreker at dette arbeidet må gis høy prioritet og ber administrerende direktør avklare rammer og opplegg for gjennomføring av arbeidet med forbedret metodikk for risiko- og sårbarhetsanalyser i samarbeid med Sykehuspartner HF.

3. Styret konstaterer at Sykehuspartner HF har stilt programmet for IKT-infrastrukturmodernisering i bero.

4. Dagens situasjon knyttet til informasjonssikkerhet i foretaksgruppens IKT-infrastruktur gir grunn til bekymring. Styret tar til etterretning at selv om programmet for IKT-infrastrukturmodernisering er stilt i bero, skal enkelte prosjekter og aktiviteter som er viktige for å bedre informasjonssikkerheten og sørge for sikker og stabil drift videreføres. Disse tiltakene er ikke relatert til tjenesteutsetting. Dette gjelder følgende:
    a. Prosess- og verktøyprosjektet
    b. Applikasjonskonsolidering og -standardisering
    c. Identity and access management (IAM) -prosjektet.
    d. Etablering av en helhetlig løsningsarkitektur for modernisert infrastruktur inklusiv fremtidig regional sikkerhetsarkitektur
    e. Replanlegging av telekommunikasjon-modernisering
    f. Utvalgte helseforetaksspesifikke prosjekter

5. Styret ber administrerende direktør gå i dialog med Sykehuspartner HF for å avklare økonomiske rammer og omprioriteringer av investeringsmidler for å sikre at tiltakene i punkt 4 og andre nødvendige tiltak for å bedre informasjonssikkerheten og opprettholde sikker og stabil drift gjennomføres. Dette inkluderer backup-løsninger og lagring, samt innføring av analyseplattformen til alle helseforetak for å bedre informasjonssikkerheten gjennom sporing og logging.

6. Styret tar til etterretning status i det pågående arbeidet med å utrede alternative modeller for å gjennomføre moderniseringen. Styret understreker at alle alternativer må ivareta personvern og informasjonssikkerhet på en trygg og sikker måte og i tråd med lovgivningen. Styret understreker også at konsekvenser ved terminering av avtalen må utredes videre. Styret forventer en samlet sak til beslutning når utredningsarbeidet er gjennomført.

7. Styret legger vekt på at det videre arbeidet skjer med god involvering og medvirkning fra ansatte og tillitsvalgte.

8. Styret tar til etterretning de tiltak som Helse Sør-Øst RHF vil iverksette knyttet til å styrke kapasitet og kompetanse innenfor områdene personvern og informasjonssikkerhet. Styret legger også vekt på at styring og ledelse av det videre arbeidet med å modernisere IKT-infrastrukturen må styrkes og sikre god involvering av helseforetakene.

Hamar, 23. juni 2017

Cathrine M. Lofthus
administrerende direktør

1 Hva saken gjelder

Behovet for at pasientene skal være sikre på at sensitive personopplysninger ivaretas på en trygg og sikker måte stiller store krav til bl.a. IKT-infrastrukturen.

I styremøte i Helse Sør-Øst RHF 8. september 2016 ble det besluttet at infrastrukturmodernisering skulle skje i samarbeid med en ekstern leverandør. Sykehuspartner HF ble bedt om å inngå kontrakt med den tilbyder som samlet sett hadde det mest fordelaktige tilbudet. I dette styremøtet ble også IKT-informasjonssikkerhet diskutert, både på grunnlag av styresaken, presentasjon og drøftingsprotokoll.

HPE (Hewlett Packard Enterprises) ble valgt som leverandør og kontrakt ble inngått 14. oktober 2016. Programmet for modernisering av IKT-infrastruktur ble mobilisert høsten 2016 og planlagt overføring av driftsansvar og ansatte ble opprinnelig satt til 1. mai 2017. Som følge av fusjon ble kontrakten våren 2017 overført til Enterprise Services Norge AS (ESN) som er del av konsernet DXC Technology (DXC).

Det kom underveis i prosessen opp usikkerhet knyttet til ivaretakelse av informasjonssikkerhet, og administrerende direktør besluttet derfor å iverksette en ekstern gjennomgang av programmet i regi av ekstern revisor PwC. Den eksterne gjennomgangen har bl.a. sett på hvorvidt ansatte hos ekstern leverandør har hatt tilgang til sensitive personopplysninger og om programmet er organisert og styrt på en hensiktsmessig måte. En foreløpig redegjørelse ble fremlagt for styret 24. mai.

I styremøte 24. mai 2017 (sak 58-2017) ble det besluttet å stille moderniseringsprogrammet for IKT-infrastruktur i bero. Styret fattet følgende vedtak:

Styret understreker behovet for at pasientene må føle seg trygge på at sensitive personopplysninger ivaretas på en trygg og sikker måte og dette innebærer at en modernisering av IKT-infrastrukturen er helt nødvendig.

1. *Styret tar den foreløpige redegjørelsen fra PwC til etterretning.*

2. *Forutsetningen for infrastrukturmodernisering har vært at tilganger til sensitive personopplysninger ivaretas på en trygg og sikker måte, og styret konstaterer at dette ikke er ivaretatt.*

3. *Prosjektet, inkl virksomhetsoverdragelse og overdragelse av driftsansvar fra Sykehuspartner til ekstern leverandør, stilles i bero inntil videre.*

4. *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.*

5. *Styret vil behandle saken igjen på et ekstraordinært styremøte i uke 26 når endelig rapport fra PwC og foreløpige resultater av utredningsarbeidet i punktet over foreligger. Som en del av dette vil også terminering måtte vurderes.*

6. *Styret ber administrerende direktør komme tilbake til styret med en utvidet orientering om hvordan pasientsikkerheten og personsensitiv informasjon håndteres i dagens situasjon.*

Basert på vedtaket i styremøte den 24. mai 2017 ble Sykehuspartner HF i foretaksmøte den 31. mai 2017 bedt om å stille programmet for IKT-infrastrukturmodernisering i bero. Videre ble Sykehuspartner HF gitt i oppdrag å redegjøre for dagens driftsituasjon når det gjelder konfidensialitet, integritet og tilgjengelighet, herunder redundans og backup-løsninger ved ulike hendelser. Dette som grunnlag for å vurdere tiltak som raskt kan iverksettes for å bedre informasjonssikkerheten. I tillegg ble Sykehuspartner HF bedt om å utarbeide en plan for styrket tilgangsstyring og en bedre metodikk for risiko- og sårbarhetsanalyser, samt utrede mulige alternativer for etablering av en modernisert IKT-infrastruktur, herunder en konsekvensvurdering av en eventuell terminering av avtalen.

Frist for en foreløpig rapport fra Sykehuspartner HF ble satt til 20. juni 2017.

Endelig rapport fra PwC ble mottatt 22. juni 2017.

Administrerende direktør vil i denne saken redegjøre for hovedpunktene i PwCs endelige rapport og den foreløpige tilbakemelding Sykehuspartner HF har gitt på overnevnte oppdrag, samt anbefale oppfølgende aktiviteter.

2 Hovedpunkter og vurdering av handlingsalternativer

2.1 PwCs rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur

PwC har i perioden 4. mai – 21. juni 2017 gjennomført undersøkelser knyttet til påstander om at en ekstern leverandørs brukertilganger til Helse Sør-Østs IKT-infrastruktur kan ha gitt tilgang til sensitive personopplysninger, herunder helseopplysninger.

Den endelige PwC-rapporten ble mottatt 22. juni 2017. PwCs hovedfunn og vurderinger fra foreløpig redegjørelse gitt 24. mai 2017 er på de fleste punkter uendret, herunder:

a. Det har ikke vært tilstrekkelig kontroll på tilgangsstyring og ikke tilstrekkelig sporbarhet på tilganger til helseopplysninger
b. En rekke personer tilknyttet ekstern leverandør har hatt mulighet til å få tilgang til helseopplysninger
c. Manglende databehandleravtaler hos ekstern leverandør
d. Systemet for gjennomføring av risikovurderinger har ikke fungert som en effektiv kontrollmekanisme
e. Upresis kommunikasjon og manglende eskalering til administrerende direktør i Helse Sør-Øst RHF

Alle disse fem punktene er beskrevet nedenfor. I tillegg beskrives også PwCs overordnede vurdering av styringsmodellen for programmet.

Oppsummering av funn relatert til tilganger og tilgangsstyring (punkt a-b over)
PwCs undersøkelser viser at 36 personer med tilknytning til ekstern leverandør har hatt utvidede administratorrettigheter som innebærer mulighet for tilgang til helseopplysninger. Tildelingen av brukere med utvidede administratorrettigheter, kombinert med begrenset sporbarhet, gir mulighet for brukere til å benytte systemer som inneholder eller prosesserer helseopplysninger uten at brukernes aktivitet i særlig grad kan etterprøves. I tillegg har 86 personer hatt privilegerte rettigheter av en mindre omfattende karakter. PwC har i sin endelige rapport verifisert at alle disse tilgangene nå er stengt.

I rapporten konstateres det at mangelen på oversikt over antall brukere med rettigheter som kan medføre tilgang til helseopplysninger, kombinert med svake kontrollrutiner og liten grad av sporbarhet, øker risikoen for uautorisert tilgang.

PwCs undersøkelser har også avdekket svakheter og mangler i loggføringen av brukeraktivitet, noe som i hovedsak knytter seg til tekniske begrensninger i infrastrukturen. Basert på overnevnte konkluderer PwC med at Sykehuspartner HF ikke har tilstrekkelig kontroll på tilgangsstyring og ikke tilstrekkelig sporbarhet på tilgang til helseopplysninger.

PwCs undersøkelser av sentrale servere knyttet til elektronisk pasientjournal har ikke avdekket misbruk eller forsøk på misbruk av tilgang til helseopplysninger. Samtidig presiserer PwC at datagrunnlaget ikke er fullstendig fordi det sentrale logginnsamlingssystemet ikke dekker hele foretaksgruppen.

Imidlertid tilsier aktiviteten som PwC har gjennomfør at dersom noen skulle ha tilegnet seg helseopplysninger i vesentlig grad, så må dette ha vært gjennomført med hensikt og med en innsats for å skjule spor. Dette medfører at en slik aktivitet i så fall må ha innebefattet både forberedelser og systematisk skjuling av spor i etterkant. Sett i sammenheng med de relativt omfattende kravene til bakgrunnssjekk og personellkontroll hos den eksterne leverandøren som er stilt gjennom kontrakten, mener PwC at dette fremstår som lite sannsynlig. Det er, som nevnt, heller ikke avdekket at helseopplysninger er på avveie.

Manglende databehandleravtaler hos ekstern leverandør (punkt c over)
Det er det enkelte helseforetak som er ansvarlig for å behandle personopplysninger, herunder helseopplysninger. Dersom behandling av personopplysninger settes ut til andre virksomheter, kan ikke dette gjøres uten at det er skriftlig avtalt (databehandleravtale). I Helse Sør-Øst har helseforetakene inngått slik avtale med Sykehuspartner HF. Settes behandling av personopplysninger ut til en ekstern leverandør skal det tilsvarende inngås databehandleravtaler mellom Sykehuspartner HF og den aktuelle eksterne leverandøren som «speiler» forpliktelsene til databehandling mellom Sykehuspartner HF og det enkelte helseforetaket. Settes behandlingen videre ut til en underleverandør av ekstern leverandør skal forpliktelsene likeledes videreføres nedover i leverandørkjeden gjennom skriftlige avtaler. Dette må framgå av den skriftlige avtalen i hvert enkelt ledd av leverandørkjeden

PwC anser at Sykehuspartner HF har oppfylt sitt ansvar med å gjøre gjeldende forpliktelsene knyttet til databehandling til den eksterne leverandøren gjennom det avtaleverket som ble etablert mellom partene.

PwC kan ikke se at den eksterne leverandøren har dokumentert oppfyllelse av kravet i avtalen til å videreføre de konkrete forpliktelsene knyttet til databehandlingen videre i leverandørkjeden.

Systemet for gjennomføring av risikovurderinger (punkt d over)
Den endelige PwC-rapporten bekrefter at sentrale informasjonssikkerhetsrisikoer knyttet til kontrakt med ekstern leverandør ikke ble tilstrekkelig vurdert. Uklare kriterier for risikoaksept fører til usikkerhet med hensyn til hvem som kan akseptere hvilke risikoer. Dette kan ha ført til at man ikke eskalerte risikoer som burde vært eskalert og at systemet for vurdering av risiko ikke har fungert som en effektiv kontrollmekanisme.

En rapport knyttet til en risikovurdering av dagens situasjon (utført av EY i 2013) beskriver omfattende svakheter i informasjonssikkerhet i Helse Sør-Øst innenfor de tre områdene sikkerhetsstyring, drift og forvaltning og teknologi. Infrastrukturmoderniseringsprogrammet har gjennom sikkerhetskravene i kontrakten (til den fremtidige løsningen) som formål å utbedre teknologiske svakheter i IKT-infrastrukturen, samt gjennom utkontraktering av drift, forbedre og effektivisere driften av løsningen. Kravene i kontrakten er basert på en internasjonal standard og beste praksis innen informasjonssikkerhet.

PwCs funn indikerer at observasjonene i EY rapporten som omfatter styring av informasjonssikkerhet i stor grad fremdeles er gjeldende og at det ikke er iverksatt tilstrekkelige tiltak for å utbedre disse svakhetene. Dette har ført til at programmet og foretaksgruppen ikke har hatt oversikt over den totale risiko- og sårbarhetssituasjonen og dermed heller ikke oversikt over hvilke tiltak som ville være nødvendige for å ha kontroll med personvern og informasjonssikkerhet ved gjennomføring av avtalen.

En av de sentrale manglene er relatert til gjennomføring av risikovurderinger. Siden risikovurderinger i programmet er gjennomført som relative vurderinger i forhold til dagens situasjon, slik at man kun har vurdert den endrede / nye risikoen som tiltaket medfører, har programmet ingen oversikt over om dagens løsning totalt sett er innenfor et akseptabelt nivå.

Oppsummert kan det konkluderes med at systemet for vurdering av risiko ikke har fungert som et effektivt kontrollsystem.

Upresis kommunikasjon og manglende eskalering (punkt e over)
PwC slår fast at «Presentasjonen til styret i Helse Sør-Øst RHF i sak 069-2016 vedrørende IKT-infrastrukturmodernisering var upresis og varsler om dette ble ikke kommunisert til administrerende direktør i Helse Sør-Øst RHF».

Kontrakten med den eksterne leverandøren regulerer en tre-trinns prosess, henholdsvis nåværende driftsmodell i regi av Sykehuspartner HF (CMO), moderniseringsfasen (TMO) og fremtidig operasjonell drift på modernisert IKT-infrastruktur hos leverandør (FMO). I CMO-fasen er det behov for at leverandør får tilgang til nåværende IKT-infrastruktur hos Sykehuspartner blant annet for å gjennomføre aktiviteter knyttet til kunnskapsoverføring og kartlegging av IKT-infrastruktur. Det følger av kontrakten at representanter for leverandøren skal gis tilgang for å kunne utøve nødvendige oppgaver i nåværende IKT-infrastruktur etter forutgående risikovurderinger. Tilstanden på IKT-infrastrukturen innebærer at enkelte av disse tilgangene også vil innebære muligheten for å få tilgang til pasientopplysninger.

I Helse Sør-Øst RHFs styresak 069-2016, 8. september 2016, ble det gitt en presentasjon hvor det bl.a. ble presentert følgende informasjon:

- «Personell som drifter IKT-infrastruktur skal ikke ha tilgang til personsensitiv informasjon – egne sikkerhetsmekanismer for dette»
- «Ekstern partner vil ikke ha tilgang til pasientdata»

PwC påpeker i sin rapport at «Det framgår ikke av presentasjonen hvilke faser i kontraktsforløpet disse kravene knytter seg til.»

Deler av informasjonen presentert for styret i Helse Sør-Øst RHF gjenspeilte altså ikke det faktum at gjennomføringen av kontrakten vil kreve at eksternt driftspersonell vil få mulighet til å få tilgang til helseopplysninger etter at en risikovurdering er gjennomført og godkjent. Den upresise informasjonen ble adressert i e-poster til sentrale personer i Helse Sør-Øst RHF, og PwC påpeker at det er uheldig at Sykehuspartner HF ikke adresserte dette mer formelt i linjen, ved for eksempel et saksfremlegg for styret i Sykehuspartner HF.

Styreak 069-2016 burde inneholdt en mer presis fremstilling av de ulike fasene i kontraktsforløpet, herunder hvilke tilganger ekstern leverandør ville få i de ulike fasene.

Overordnet vurdering av programmets styringsmodell

PwC henviser til at konsulentselskapet Metier i mars 2017 gjennomførte en ekstern vurdering av infrastrukturmoderniseringsprogrammet med formål om å sikre at programmet er styrt og organisert slik at det kan lykkes i å nå mål og realisere gevinster, samt vurdere organisering og styringsdokumentasjon opp mot beste praksis. Overordnet pekes det på manglende styringsdokumentasjon og uklarheter i styringsstruktur og ansvarsdeling. Metier anbefaler en rekke tiltak knyttet til bedre styring, inkludert at Sykehuspartner HF bør styrke egen programorganisasjon med ekstern kapasitet.

2.2 Foreløpig redegjørelse fra Sykehuspartner HFs arbeid

I foretaksmøte i Sykehuspartner HF den 31. mai 2017 ble følgende vedtatt:

1. *Programmet for IKT-infrastrukturmodernisering i Sykehuspartner HF stilles i bero inntil videre.*

2. *Programmets ressurser forutsettes disponert til utredning av de forhold som styret i Helse Sør-Øst RHF har påpekt. Dette arbeidet skal skje i nært samarbeid med Helse Sør-Øst RHF.*

3. *Sykehuspartner HF skal redegjøre for dagens driftssituasjon når det gjelder konfidensialitet, integritet og tilgjengelighet, herunder redundans og back-up løsninger ved ulike hendelser. Spesifikt skal Sykehuspartner beskrive hvordan konfidensialitetsproblemstillingene knyttet til privilegerte tilganger ved drift av IKT-infrastruktur håndteres.*

4. *Sykehuspartner HF skal utarbeide en plan for styrket tilgangsstyring og en bedre metodikk for risiko- og sårbarhetsanalyser. Planen må ivareta informasjonssikkerhet og personvern innenfor lovmessige krav, samt de nye EU-personvernkravene (GDPR) som blir gjeldende fra mai 2018.*

5. *Sykehuspartner HF skal utrede mulige alternativer for etablering av en modernisert IKT-infrastruktur i Helse Sør-Øst, basert på inngått avtale med* Enterprise Services Norge AS. *Alternativene skal ivareta at informasjonssikkerhet og personvern håndteres på en trygg og sikker måte og i tråd med lovgivningen. For alle alternative gjennomføringsplaner skal det som et minimum beskrives:*
   - *Hovedtrekk i leveranser og leveranseplan*
   - *Risiko for eksponering av personsensitive opplysninger til egne ansatte og leverandør(er)*
   - *Kontraktuelle forhold og konsekvenser*
   - *Økonomiske konsekvenser*

6. *Sykehuspartner HF skal i tillegg utarbeide forslag til styrket styring og ledelse av prosjektet. Forslaget skal ivareta at organisering og styring av programmet utformes slik at det lykkes å nå programmålene og hente ut gevinstpotensialet. Det skal særskilt vektlegges at gjennomføringen av prosjektet skjer på en kontrollert måte, med et forsvarlig risikonivå. Forslag til organisering må også beskrive hvordan Sykehuspartner HF sikrer tilstrekkelig kompetanse og kapasitet for å gjennomføre et prosjekt av dette omfang og kompleksitet.*

7. *I tillegg til beskrivelse av gjennomføringsalternativer skal Sykehuspartner HF også gi en overordnet konsekvensvurdering av en eventuell terminering av avtalen med* Enterprise Services Norge AS. *Dette omfatter både økonomiske og praktiske konsekvenser av termineringen, herunder konsekvenser for fremdrift av andre prosjekter.*

2.2.1 Status for programmet og programmets ressurser

Sykehuspartner HF har i styremøte 20. juni 2017 bekreftet at programmet er stilt i bero. Dette omfatter bl.a.:

- Sykehuspartner HF har lagt ned programstyret 31. mai 2017
- Det er iverksatt aktiviteter for å sikre at prosjekter avsluttes på en ryddig måte og sikre at bevaringsverdig informasjon ikke går tapt.
- En kjernegruppe (fra ekstern leverandør og Sykehuspartner HF) vil bli beholdt for å utrede alternativer for infrastrukturmodernisering (ref. vedtak 2 og 5 fra foretaksmøteprotokollen 31. mai 2017) basert på inngått kontrakt med ekstern leverandør.
- Prosjektledere og prosjektressurser som var disponert av programmet og som ikke skal benyttes i utredningen av alternativer for infrastrukturmodernisering eller aktiviteter som må videreføres som forberedelse for videre modernisering, er fristilt.
- Ressurser som Sykehuspartner HF har leid inn til å støtte gjennomføringen av programmet og som ikke er nøkkelressurser for utredningen av alternativer for infrastrukturmodernisering blir avviklet. Konsulentavtalene inngått gjennom Sykehusinnkjøps-forhandlede rammeavtaler har en oppsigelsestid på 30 dager.

Noen av aktivitetene som er påbegynt og som var planlagt gjennomført i programmet, er ansett som viktig for foretaksgruppen å videreføre uavhengig av videre tilnærming til gjennomføring av infrastrukturmodernisering, også i alternativer som innebærer en terminering av avtalen med ekstern leverandør:

1) Prosess- og verktøyprosjektet.
   Aktiviteten gjelder utvikling og innføring av saksbehandlingsverktøy og prosess-støtte for driftsprosessene og er viktig for sikker og stabil drift.

2) Applikasjonskonsolidering og –standardisering.
   Aktiviteten omfatter kartlegging av applikasjoner og sanerings-/konsolideringspotensialet. Tiltaket er en forutsetning for effektiv modernisering av IKT-infrastrukturen i Helse Sør-Øst, uavhengig av modell for modernisering.
3) Identity and access management (IAM) –prosjektet.
   Prosjektet er et nødvendig element for å oppnå en sikker løsning innen tilgangskontroll og -styring.
4) Etablering av en helhetlig løsningsarkitektur for modernisert infrastruktur inklusiv fremtidig regional sikkerhetsarkitektur.
   Dette er et nødvendig element i en felles infrastrukturløsning og nødvendig for å kunne møte de nye EU-personvernkravene (GDPR) og andre sikkerhetskrav. Arbeidet er en fortsettelse på avklaring hvordan informasjonsbehandlingen skal deles inn og styres fremover. Dette er en forutsetning uavhengig av modell for modernisering.
5) Replanlegging av modernisering av telekommunikasjon.
   Teknologiskiftet innen telekommunikasjon gjør det nødvendig for Helse Sør-Øst å skifte ut eksisterende telekommunikasjonsløsninger uavhengig av modell for modernisering.

I tillegg til ovennevnte, har styret i Sykehuspartner HF anbefalt videreføring av enkelte viktige helseforetaksspesifikke prosjekter.

Forslag til prosjekter som anbefales videreført er en foreløpig anbefaling. Det pågår fortsatt en vurdering av konsekvenser av at programmet er stilt i bero og hvilke øvrige aktiviteter som bør videreføres.

Sykehuspartner HF er i ferd med å utrede det nåværende økonomiske pådraget fra programmet mens det er stilt i bero. En prognose på det samlede kostnadsbildet er forventet å foreligge ultimo juni. Kostnadskonsekvensen ved fristilling av ressurser hos ekstern leverandør med underleverandører vil dessuten bli gjenstand for forhandlinger. De kostnadsmessige konsekvenser vil ikke være endelig avklart før forhandlinger er gjennomført.

2.2.2 Dagens driftssituasjon knyttet til informasjonssikkerhet

Den samlede porteføljen av IKT-infrastruktur og applikasjoner er svært omfattende. Sykehuspartner HF drifter og vedlikeholder en portefølje av systemkomponenter som i dag inneholder i overkant av 3000 applikasjoner, hvor Sykehuspartner HF leverer applikasjonsdrift og applikasjonsforvaltning. Det er så langt en overordnet vurdering som er gjort av Sykehuspartner HF knyttet til dagens driftssituasjon.

Sykehuspartner HF påpeker i sin foreløpige redegjørelse at det er en sammenheng mellom moderniseringen av applikasjonsområdet og IKT-infrastrukturen. Evnen til å etablere og opprettholde en modernisert IKT-infrastruktur med en tilfredsstillende informasjonssikkerhet er avhengig av at foretaksgruppen forenkler og standardiserer den samlede IKT-porteføljen. Dette ble også drøftet i styresak 069-2016, hvor det blant annet heter:

En viktig forutsetning for at modernisering av foretaksgruppens IKT-infrastruktur skal oppnå de planlagte gevinstene er at foretaksgruppen samlet sett evner å bidra til forenkling og standardisering av applikasjoner og tjenestenivåer. Dette er en forutsetning uavhengig av om en modernisert IKT-infrastruktur utvikles og driftes i egen regi eller av en ekstern partner. Dagens samlede applikasjonsportefølje ved helseforetakene er omfattende (~3000 applikasjoner). Etter gjennomført modernisering er det antatt at den samlede porteføljen i regionen er på rundt 700 applikasjoner.

En viktig del av Sykehuspartner HFs arbeid med informasjonssikkerhet er gjennomføring av risiko- og sårbarhetsvurderinger for å vurdere en tjenestes evne til å oppfylle prinsippene om konfidensialitet, integritet, tilgjengelighet og sporbarhet. Risiko- og sårbarhetsvurderingene gir blant annet oversikt over risikoer som er vurdert å være utenfor akseptabelt risikonivå, med tilhørende forslag til risikoreduserende tiltak. Hittil har det ikke i tilstrekkelig grad vært etablert omforente regionale kvantifiserbare kriterier for akseptabelt risikonivå. Dette har medført at det har vært vanskelig å forutse riktig risikonivå for leveranseprosjektene og at like hendelser/risikoer har vært behandlet ulikt. Sykehuspartner HF har heller ikke hatt tilstrekkelig oppfølging av status på gjennomføring av tiltakene. Over tid har det således oppstått en situasjon hvor det er uavklart om risikoeier har gjennomført aktuelle risikoreduserende tiltak. Sykehuspartner HF konkluderer med at dette påvirker negativt Sykehuspartner HFs evne til å etablere og opprettholde et tilfredsstillende informasjonssikkerhetsnivå.

Sykehuspartner HF har gjennomført flere forbedringer knyttet til tilgangsstyring de siste årene, men det eksisterer fremdeles en betydelig informasjonssikkerhetsrisiko knyttet til infrastrukturens beskaffenhet. Uten at det gjennomføres utbedringer i eksisterende infrastruktur eller denne erstattes i sin helhet av nye tjenester, vil informasjonssikkerhetsrisiko knyttet til tilgangsstyring fortsatt være høy.

2.2.3 Plan for styrket tilgangsstyring og forbedrede risiko- og sårbarhetsanalyser

Tilgangsstyring skal sikre at rett person får rett tilgang, til rett funksjon eller informasjon, til rett tid og fra rett sted, med tilhørende sporbarhet og kontrollmekanismer. Tilgangsstyring er summen av prosedyrer, retningslinjer og teknologi som regulerer denne tilgangen.

Det er flere utfordringer ved dagens praksis knyttet til tilgangsstyring som krever fortsatt arbeid. Dette omfatter organisering, ansvarsfordeling, styring, policy, prosesser og rutiner for tilgangsstyring. I tillegg vil det iverksettes tiltak for å sikre sporbarhet og bedre kontrollmekanismer.
I og med at området er stort og komplekst anbefaler Sykehuspartner HF at strakstiltak fokuseres mot privilegerte tilganger som benyttes for drift, forvaltning og leverandøraksess.

Sykehuspartner HF viser til at de har iverksatt en rekke strakstiltak:

- Forsterket rutine for tildeling av privilegerte tilganger
- Forsterket rutine for gjenåpning av eksisterende tilganger
- Gjennomgang av kontroll og rapporteringsbehov
- Full gjennomgang av tilganger for leverandører og eksternt personell
- Påbegynt deaktivering av tilganger for leverandører og eksternt driftspersonell som ikke har tjenstlige behov

- Bedret kontrollrapportering av tilgangsendringer for leverandører og eksternt personell

Sykehuspartner HF har også kommunisert at det vil bli gjennomført vurderinger av endringer og/eller bredding av allerede tilgjengelige produkter som f.eks.:

- Oppgradering av saksbehandlingsverktøyet (HPSM) for å sikre at godkjenningsprosessen styrkes (jfr. avsnitt 2.2.1)
- Økt bruk av passordhvelvet (PAM) for privilegerte tilganger
- Bredding av analyseplattformen til alle helseforetakene for å sikre økt sporbarhet og kontroll-/ rapporteringsmulighet

I tillegg til ovennevnte er fortsettelsen av IAM-prosjektet (jfr. avsnitt 2.2.1) en viktig og sentral komponent for å sikre god tilgangsstyring.

Sykehuspartner HF foreslår også at det etableres et prosjekt for forbedret metode og leveranse av risiko- og sårbarhetsanalyser i Helse Sør-Øst. Dette prosjektet skal også ivareta informasjonssikkerhet og personvern innenfor lovmessige krav, samt de nye EU-personvernkravene (GDPR).

2.2.4 Utredning av alternative løsninger for modernisering av infrastruktur i samarbeid med ekstern leverandør

Det er startet utredning av alternativer for etablering av en modernisert IKT-infrastruktur ved bruk av inngått avtale med ekstern leverandør. Sykehuspartner HF har skissert tre hovedalternativer som vil bli utredet nærmere:

- Alternativ 1
  Gjennomføre modernisering med forsterkede tiltak innen informasjonssikkerhet, kombinert med avbestilling av delleveranse knyttet til driftsansvaret, herunder virksomhetsoverdragelse, for eksisterende IKT-infrastruktur. Alternativet innebærer at Sykehuspartner HFs personale vil fortsette å drifte dagens infrastruktur mens ekstern leverandør først vil ta over når den fremtidige plattformen er etablert.
- Alternativ 2
  Gjennomføre modernisering med forsterkede tiltak innen informasjonssikkerhet, kombinert med delvis/stegvis virksomhetsoverdragelse av driftsansvaret for dagens IKT-infrastruktur til ekstern leverandør, der for eksempel de enkelte teknologiområder overdras på ulike tidspunkt.
- Alternativ 3
  Gjennomføre modernisering med forsterkede tiltak innen informasjonssikkerhet før virksomhetsoverdragelsen av det fulle driftsansvaret for dagens IKT-infrastruktur til ekstern leverandør. Dette alternativet er det som er mest i tråd med kontraktens opprinnelige intensjoner.

I følge Sykehuspartner HF er de foreløpige vurderingene kommet for kort til at noen av de tre alternative gjennomføringsmodellene kan avskrives som uaktuelle i den form og på det nivå de er beskrevet i dag. Samtidig kan heller ikke terminering av avtalen utelukkes.

2.2.5 Styrket styring og ledelse av prosjektet.

Det ble våren 2017 i regi av Sykehuspartner HF gjennomført en ekstern gjennomgang av styringsmodellen i programmet. Gjennomgangen ble utført av Metier som i sin rapport anbefalte en rekke tiltak for bedret styringsmodell i programmet.

I tillegg vil valgt alternativ (jfr. alternativene i 2.2.4, inkludert terminering) kunne medføre ulike behov for endringer i programmets organisering og styringsmodell.

Endelig plan for styrking av styring og organisering må dermed ses i sammenheng med endelig beslutning om veien videre.

2.2.6 Konsekvens ved terminering

Sykehuspartner HF har utarbeidet en foreløpig redegjørelse for konsekvenser ved terminering. Kostnader ved terminering kan på et overordnet nivå deles inn i følgende elementer:

- Direkte kostnader til ekstern leverandør
  Kostnader til ekstern leverandør utgjør i all hovedsak pådratte kostnader, kostnader forbundet med omstilling og eventuelle grunnlagsinvesteringer.
- Kostnader knyttet direkte eller indirekte til ressurser i Sykehuspartner HF
  Både påløpte og forpliktede fremtidige kostnader må inkluderes i det totale kostnadsbildet. Fremtidige kostnader er ikke estimert, men antas å kunne begrenses vesentlig som følge av at eksterne ressurser som er hentet inn for å fristille interne ressurser kan sies opp med en måneds varsel og at egne ansatte antas å kunne omdisponeres til andre oppgaver.
- Konsekvenser for andre prosjekter
  Det kjøres i dag en rekke prosjekter (i all vesentlighet alle prosjekter under «Digital Fornying») som er avhengige av en planlagt modernisering av IKT-infrastrukturen. En forsinkelse i den planlagte moderniseringen vil kunne få konsekvenser for fremdriften og dermed kostnader forbundet med disse prosjektene. Omfanget av dette er p.t. ikke analysert utover at man har identifisert hvilke større prosjekter som er avhengige av en modernisering av IKT-infrastrukturen.

Til fradrag kommer en eventuell gjenbruksverdi av arbeid allerede utført (design, hardware, etc.). Kontrakten medfører ikke et særskilt avbestillingsgebyr dersom kontrakten termineres i etableringsfasen.

Sykehuspartner HF påpeker at det først etter forhandlinger med ekstern leverandør vil være mulig å konkludere med hva som vil blir den endelig kompensasjonen til ekstern leverandør.

2.3 Regionale tiltak knyttet til informasjonssikkerhet og personvern

Administrerende direktør har gjennomgått flere underliggende rapporter som beskriver dagens situasjon, herunder PwCs rapport og Sykehuspartner HFs foreløpige rapport. I tillegg til de tiltak som er identifisert

i Sykehuspartner HF fremstår det tydelig at det er behov for tiltak også på regionalt nivå. Det er derfor besluttet at følgende tiltak skal gjennomføres:

- Styrking av området «Personvern og informasjonssikkerhet» i det regionale helseforetaket gjennom å øke kapasitet og kompetanse innen området.
- Iverksette et regionalt arbeid knyttet til videreutvikling av felles regional metodikk for risiko- og sårbarhetsanalyser, en enhetlig prosedyre for gjennomføring og en omforent forståelse for akseptabelt risikonivå.

Det at infrastrukturmoderniseringen er stilt i bero har konsekvenser for den samlede IKT-virksomheten i Helse Sør-Øst. Det er behov for å gå gjennom prosjektene i Digital fornying for å vurdere tidsplaner og ressurser, samt vurdere prioritering av prosjektene for å sikre et akseptabelt risikonivå.

3 Administrerende direktørs anbefaling

Administrerende direktør vil understreke at pasientene skal være sikre på at sensitive personopplysninger håndteres på en trygg og sikker måte.

En rekke funn i PwC-rapporten gir grunn til bekymring. Det er åpenbart at det ikke er god nok kontroll med tilgangsstyring og sporbarhet av tilgang til pasientinformasjon i IKT-infrastrukturen. Det er likeledes påvist at metodikken for risiko- og sårbarhetsanalyser har svakheter og at systemet for gjennomføring av risikovurderinger ikke har fungert som den kontrollmekanismen det var ment som. De påpekte svakheter følges opp gjennom det oppdraget som er gitt til Sykehuspartner HF i foretaksmøte 31. mai 2017.

Administrerende direktør ser at det i tillegg er behov for rask iverksettelse og gjennomføring av flere tiltak for å forbedre tilgangsstyring, logging og overvåking i driften av IKT-infrastrukturen, samt knyttet til backup og lagring. Administrerende direktør vil gå i dialog med Sykehuspartner HF for å avklare økonomiske rammer og omprioriteringer av investeringsmidler for å sikre at tiltakene for å bedre informasjonssikkerheten gjennomføres. Videre er det behov for å iverksette tiltak på regionalt nivå, spesielt knyttet til å forbedre metodikken for risiko- og sårbarhetsanalyser, inkludert riktig involvering av databehandlingsansvarlige. Administrerende direktør vurderer også at det er nødvendig med en styrking av kompetanse og kapasitet innenfor personvern og informasjonssikkerhet i det regionale helseforetaket for å kunne ivareta en sterkere koordinerende rolle i dette arbeidet.

I tillegg til gjennomføring av en rekke umiddelbare tiltak vil også mange funn i PwC-rapporten måtte hensyntas av Sykehuspartner HF i den videre utformingen av alternativer for å modernisere foretaksgruppens IKT-infrastruktur.

Administrerende direktør viser til PwCs omtale av EY-rapporten fra 2013 om risikovurdering av Helse Sør-Østs standard plattform. PwCs funn indikerer at observasjonene i EY rapporten som omfatter styring av informasjonssikkerhet i stor grad fremdeles er gjeldende og at det ikke er iverksatt tilstrekkelige tiltak for å utbedre disse svakhetene. EY-rapporten har etter det administrerende direktør kjenner til ikke blitt fremlagt i en endelig versjon og den ser heller ikke ut til å ha vært behandlet i Sykehuspartners ledelse eller styringsorganer. Administrerende direktør har fått rapporten tilsendt etter at oppdraget om

ekstern gjennomgang ble gitt til PwC. Det er sterkt beklagelig at en så viktig rapport ikke ser ut til å ha blitt behandlet ledelses- og styringsmessig i Sykehuspartner. Kunnskap om innholdet i denne rapporten ville gitt viktig oversikt over den totale risiko- og sårbarhetssituasjonen og dermed hvilke tiltak som ville vært nødvendige for å ha kontroll med personvern og informasjonssikkerhet uavhengig av modell for modernisering av IKT-infrastrukturen.

Behovet for modernisering av IKT-infrastruktur i foretaksgruppen har vært i tema i mange år. Mye arbeid er gjennomført både knyttet til etablering av regionale datasentre og utrulling av moderniserte IKT-klientplattformer ved helseforetak.

Samtidig er dagens IKT-infrastruktur preget av å være sammensatt og knyttet til den gamle sykehusstrukturen. Sikkerhetsmessige forhold, men også andre tekniske forhold, hindrer muligheten for å etablere gode felles løsninger innenfor det kliniske området.

Det har vært utredet ulike alternativer for modernisering og standardisering for IKT-infrastruktur. Styret besluttet i sak 069-2016 at man skulle tilknytte seg en ekstern leverandør som kunne bistå med rask modernisering og med større grad av automatisering.

Sykehuspartner HF skal på en kostnadseffektiv måte levere trygge og stabile tjenester til helseforetakene. En modernisert infrastruktur i foretaksgruppen vil kunne driftes og vedlikeholdes med vesentlig mindre bruk av ressurser og dermed legge grunnlaget for en mer effektiv drift enn det som er mulig med dagens infrastruktur.

Basert på ovennevnte er det administrerende direktørs vurdering at det er viktig for Helse Sør-Øst å gjennomføre en modernisering av IKT-infrastrukturen. Dette er en helt sentral forutsetning for en vellykket realisering av Digital fornying og for å tilrettelegge for en mer effektiv drift i Sykehuspartner HF. En modernisert IKT-infrastruktur er også helt nødvendig for å kunne ivareta personvern og informasjonssikkerhet på en trygg og sikker måte. Behovet for en moderniser IKT-infrastruktur bekreftes også av PwC som i sin rapport anbefaler at Helse Sør-Øst fortsetter å prioritere arbeidet med sin IKT-infrastrukturmodernisering. PwC sier bl.a. følgende:

Helse Sør-Øst har et stort behov for å modernisere sin IKT-infrastruktur og arbeidet er en forutsetning for å kunne innføre bedre og regionale løsninger for helsepersonell, pasienter, innbyggere og administrativt personell. IKT-infrastrukturmoderniseringen er nødvendig for å rette mangler innen informasjonssikkerhet, bl.a. knyttet til tilgangsstyring og sporbarhet som denne rapporten peker på. Helse Sør-Øst utgjør over 50% av spesialisthelsetjenesten i Norge og foretaksgruppens evne til å lykkes med sin IKT-strategi setter sterke føringer for den kommunale, regionale og nasjonale IKT-utviklingen i helsesektoren. Vi anbefaler at Helse Sør-Øst RHF og Sykehuspartner HF fortsetter å prioritere arbeidet med IKT-infrastrukturmodernisering.

Helse Sør-Øst RHF har mottatt foreløpig rapport fra Sykehuspartner HFs styre vedrørende oppfølging av vedtak fra foretaksmøte 31. mai 2017. Rapporten bekrefter svakhetene i dagens infrastruktur og tilknyttet tilgangsstyring, sporing, overvåkning, m.m.

Administrerende direktør konstaterer at Sykehuspartner HF har stilt programmet for modernisering av IKT-infrastruktur i bero. Videre påpeker administrerende direktør betydningen av en rask reduksjon i pådraget av ressurser i programmet.

Styret i Sykehuspartner HF har godkjent at enkelte prosjekter som har vært organisert som en del av infrastrukturmoderniseringsprogrammet, men som ikke er direkte relatert til virksomhetsoverdragelse av drift av IKT-infrastruktur, videreføres i regi av Sykehuspartner HF. Prosjektene er av stor viktighet for bl.a. å forbedre tilgangsstyring og sikre stabil drift, og administrerende direktør støtter styret i Sykehuspartner HFs beslutning om å videreføre disse.
Administrerende direktør slutter seg også til Sykehuspartner HFs vedtak om å gjennomføre tiltak innen bl.a. backup og lagring. Videre ser administrerende direktør positivt på at styret i Sykehuspartner HF prioriterer problemstillingene knyttet til manglende tilgangsstyring høyt og at det foreslås en rekke tiltak, herunder innføring av analyseplattformen til alle helseforetak for å øke informasjonssikkerheten gjennom sporing og logging.

Administrerende direktør vil som angitt over gå i dialog med Sykehuspartner HF for å avklare økonomiske rammer og omprioriteringer av investeringsmidler for å sikre at tiltakene for å bedre informasjonssikkerheten gjennomføres

I forhold til det foreslåtte prosjektet for å utvikle en bedre metode for risiko- og sårbarhetsanalyse vil administrerende direktør ta initiativ til nærmere dialog med Sykehuspartner HF om opplegg for gjennomføring av dette arbeidet, herunder hva som skal være et regionalt ansvar.

Når det gjelder løsninger for modernisering av infrastruktur i samarbeid med ekstern leverandør, arbeider Sykehuspartner HF med tre mulige alternativer. Administrerende direktør har merket seg at de foreløpige vurderingene er kommet for kort til at noen av de tre alternative gjennomføringsmodellene kan avskrives som uaktuelle i den form og på det nivå de er beskrevet i dag. Slik administrerende direktør vurderer alternativene på det nåværende tidspunkt fremstår et alternativ hvor man beholder driftsansvaret i Sykehuspartner frem til man har modernisert infrastrukturen som det tryggeste informasjonssikkerhetsmessig.

Administrerende direktør understreker at risikobildet for de tre gjennomføringsmodellene skal tydeliggjøres, spesielt risiko for eksponering av personsensitive opplysninger til egne ansatte og leverandør(er). Endelig avklaring kan først skje etter at forhandlinger med ekstern leverandør er sluttført. Kost-nytteanalysen som lå til grunn for beslutningen i styresak 069-2016 må oppdateres som ledd i utredning av alternativ gjennomføringsmodell. Dette gjelder også egenregi-alternativet, slik at man sikrer et godt beslutningsunderlag.

Administrerende direktør påpeker videre at terminering av avtalen ikke kan utelukkes og derfor skal vurderes.

Sykehuspartner HF nå legger opp til en plan for å gjennomføre prosessen med å utforske handlingsrommet innenfor mulige alternativer sammen med ekstern leverandør. Resultat av dette arbeidet vil presenteres for styret og administrerende direktør legger også opp til at dette arbeidet underlegges en ekstern kvalitetssikring før endelig beslutning.

Administrerende direktør viser til at det er stilt spørsmål ved nivået på de ulike teknologiske komponentene som inngår i kontrakten med ekstern leverandør. Dette er forhold som vil bli vurdert nærmere i det videre arbeidet.

Administrerende direktør har videre registrert at det fra flere hold har vært stilt spørsmål knyttet til hvorvidt Helse Sør-Øst sin infrastruktur bør anses som kritisk infrastruktur i henhold til sikkerhetsloven. Administrerende direktør vil derfor ta et initiativ til at det gjøres en vurdering av hvorvidt hele eller deler av infrastrukturen burde vært kategorisert som kritisk infrastruktur. Det vil være dialog med Helse- og omsorgsdepartementet og Nasjonal sikkerhetsmyndighet om dette. Administrerende direktør viser også til oppdrag gitt av Helse- og omsorgsdepartementet til Direktoratet for e-helse 9. juni 2017. Direktoratet er gitt i oppdrag å identifisere og foreslå gode rutiner for å sikre at de til enhver tid gjeldende krav til informasjonssikkerhet ved bruk av private leverandører etterleves. Direktoratet skal som del av oppdraget utarbeide en overordnet status for bruk av nasjonale og internasjonale leverandører. Det er også bedt en vurdering om det er tjenester som ikke bør overlates til private underleverandører. Spesielt skal det sees på hvilke situasjoner og hvordan det eventuelt bør og kan skilles mellom norske, EØS-baserte og globale underleverandører, herunder behovet for å se på forholdet mellom helsetjenesten og sikkerhetsloven. Fristen for arbeidet er satt til 1. november 2017.

I den endelige PwC-rapporten er det påpekt at styringen og ledelsen av arbeidet med IKT-infrastrukturmodernisering i Sykehuspartner HF ikke har vært god nok. En styrking av dette er avgjørende for en vellykket gjennomføring av IKT-infrastrukturmoderniseringen. Administrerende direktør viser også til foretaksmøte i Sykehuspartner HFs vedtak 31. mai 2017 om at Sykehuspartner HF skal utarbeide forslag til styrket styring og ledelse av prosjektet, herunder hvordan det skal sikres tilstrekkelig kompetanse og kapasitet for å gjennomføre et prosjekt av dette omfang og kompleksitet. Dette vil adresseres når det er avklart hvordan infrastrukturmoderniseringen skal gjennomføres.

Administrerende direktør legger stor vekt på at det videre arbeidet skjer med god involvering og medvirkning fra ansatte og tillitsvalgte og slik at ulike synspunkter og vurderinger fremkommer.

Trykte vedlegg

- Rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod). PwC 22. juni 2017
- Sykehuspartner HF - Foreløpig rapport – Oppfølging av vedtak fra foretaksmøte Sykehuspartner HF 31.05.2017