Møtedato: 28.4.2021

Arkivnr.:	Saksbeh./tlf.:	Sted/dato:
	Rolandsen,Nilsen/75 51 29 00	Bodø, 21.4.2021

Styresak 51-2021 Roller og ansvar IKT – videre prosess og føringer for økonomisk langtidsplan

Saken var opprinnelig meldt som en orienteringssak, men er endret til ordinær styresak og kommer i tillegg til tidligere utsendt saksliste.
Saksdokumentene var ettersendt.

Formål
Formål med saken er å orientere styret om dialog med helseforetakene om oppfølging av Riksrevisjonens (RR) rapport – *Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer* gjeldende kritikk om uklarheter knyttet til roller og ansvar (vedlegg).

I tråd med Oppdragsdokument 2021 (OD2021), legger Helse Nord RHF eierskapet til regional infrastruktur til Helse Nord IKT. Helse Nord RHF vil legge høyere sikkerhetskrav til grunn, enn det helseforetakene hittil har gjort. Noe som innebærer at Helse Nord RHF i større grad vil legge fellesregionale føringer/bestillinger til Helse Nord IKT på vegne av foretaksgruppen. Helseforetakene gjennom de formelle ansvarsposisjoner disse ivaretar, vil være sentrale og naturlige deltagere i prosessen rundt bestillinger.

Bakgrunn
Det vises til Dokument 3:2 (2020-2021) Riksrevisjonens (RR) rapport – Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. I punkt *8.3.3. Uklare ansvarsforhold og oppgavefordeling i helseregionene vanskeliggjør forbedringsarbeidet* heter det bl.a.:
I Helse Nord, Helse Midt-Norge og Helse Sør-Øst mener de regionale IKT-leverandørene at manglende avklaring av ansvar og oppgaver mellom helseforetakene og dem er en av hovedutfordringene i arbeidet med å forebygge og avdekke dataangrep. De er gitt et ansvar for sikkerheten i den regionale IKT-infrastrukturen, men har ikke kontroll med alt helseforetakene kobler til denne. Lokale sikkerhetsbrudd kan utgjøre en risiko for regionen som helhet, og de regionale IKT-leverandørene mener manglende avklaringer gjør det tidkrevende å rydde opp i kjente svakheter. Blant annet oppleves dette som en utfordring der det må ryddes i det helseforetakene drifter selv, og der det er vanskelig å gjennomføre oppdatering av programvare for eldre utstyr og systemer ute i helseforetakene. I Helse Vest framstår ansvaret for oppgavene som klarere (vedlegg).

I OD2021 til helseforetakene heter det i krav nr. 98:
Helse Nord IKT har ansvaret og oppgaven for leveranse av IKT infrastrukturtjenester til helseforetakene på følgende områder: IKT-drift, IKT-produksjon, levering og innstallering av brukerutstyr, systemintegrasjon samt brukerstøtte og andre forvaltningsoppgaver som

naturlig tilknyttes områdene nevnt ovenfor. Ytterligere tydeliggjøring vil fremkomme i styringssystem for informasjonssikkerhet.

- *Styringskravet gjelder ikke området medisinsk utstyr som er særskilt regulert i egne forskrifter.*
- *Innen utløpet av 1. kvartal avklare om det foreligger andre områder som setter særlige lov/forskriftskrav krav for utførelse av de IKT-oppgaver her nevnt, og behandle slike i forbindelse med klargjøring av drifts- og forvaltningsmodeller med Helse Nord IKT.*

Ansvar for infrastruktur og føringer for fremtidig sikring av infrastruktur
Helse Nord RHF har overordnet ansvar for hele foretaksgruppen. Helse Nord RHF mener at dagens modell bidrar til å øke sårbarheten i foretaksgruppen.

I tråd med OD2021, krav nr. 98, tar Helse Nord RHF sikte på å etablere en fellesregional styring av sykehusenes IKT infrastruktur, og legger oppgaven med drift og forvaltning av infrastruktur til Helse Nord IKT. Hvor Helse Nord RHF vil representere bestiller på vegne av foretaksgruppen for hva som skal være (sikkerhets-)nivå for denne. Helseforetakene skal være deltagende i prosessen og gi tydelige innspill til Helse Nord RHF som ivaretar helseforetakenes selvstendige juridiske ansvar. Det arbeides med å dokumentere formalgrunnlag og å konkretisere avgrensninger for endringen.

I tråd med krav 103[1] vil Helse Nord RHF fremover legge et høyere sikkerhetsnivå til grunn enn det helseforetakene har gjort tidligere. Dette betyr at aktiviteter knyttet til informasjonssikkerhet skal sikres høy prioritet, og Helse Nord RHF vil påse at innføringsløpene blir tilfredsstillende ressurs-satt.

Føringer for økonomisk langtidsplan
Endringer slik beskrevet i OD2021 vil få implikasjoner for økonomisk langtidsplan, bl.a. ved at kostnadene på innføringsløpene i helseforetakene blir konkretisert i økonomisk langtidsplan. Adm. direktør anbefaler derfor at:

- Regionalt besluttede investeringer f.o.m. 2021, samt investering i VDI-løsning, bæres av Helse Nord RHF.
- Helse Nord RHF i fremtiden finansierer regionalt besluttede tiltak knyttet til IKT infrastruktur som representerer standardprodukter som helseforetakene skal benytte.
- Økonomisk langtidsplan må synliggjøre kostnadene til innføringsløpene i helseforetakene. Dette for å sikre at kritiske oppgaver er tilfredsstillende ressurs-satt.
- Helseforetakene selv skal finansiere innføring og volumuttak/bruk lokalt.

Helse Nord RHF vil komme tilbake til driftsøkonomiske konsekvensen av investeringene til helseforetakene, og hvordan incentivene til kritisk vurdering av behov kan opprettholdes og rett kostnad pr. pasient kan beregnes.

[1] [1] *Levere IKT-tjenester i tråd med virkemidler som besluttes av Helse Nord RHF, eksempelvis regionale systemvalg/systemløsninger, arkitekturbeslutninger/føringer, føringer for infrastruktur, regionalt styringssystem for informasjonssikkerhet.*

Adm. direktørs vurdering
Adm. direktør viser til dialog med styreledere og adm. direktører i helseforetakene, og ser at det er behov for en god prosess i forkant av beslutning om endring av roller og ansvar knyttet til infrastruktur.

Adm. direktør ber styret om aksept for å legge føringer i økonomisk langtidsplan som sikrer at oppgavene som skal ivaretas innenfor IKT-feltet blir tilfredsstillende ressurs-satt og at budsjettrammene legges til den enhet som skal fatte beslutningene.

Styret i Helse Nord RHF inviteres til å fatte følgende vedtak:

1. Styret i Helse Nord RHF tar informasjonen om arbeidet med å klargjøre roller og ansvar innenfor IKT-området til orientering, og ber om at saken legges frem for endelig beslutning på senere tidspunkt.

2. Styret ber om at overordnede implikasjoner for investeringsplanen og behov knyttet til innføringsløpene innarbeides og synliggjøres ved rullering av økonomisk langtidsplan, som legges frem i juni 2021.

Bodø, den 21. april 2021

Cecilie Daae
adm. direktør

Vedlegg: Utdrag av Dokument 3:2 – Riksrevisjonens kontroll

Vedlegg – Utdrag av Dokument 3:2 (2020-2021) – Riksrevisjones kontroll

8.3.3 Uklare ansvarsforhold og oppgavefordeling i helseregionene vanskeliggjør forbedringsarbeidet

Ledelsen i de regionale helseforetakene, helseforetakene og de regionale IKT-leverandørene skal sørge for at det er tydelig hvem som har ansvar for hva på informasjonssikkerhetsområdet. Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger. De regionale helseforetakene må også sørge for samordning innad i helseregionene på IKT-sikkerhetsområdet, slik at hensyn til helheten og fellesskapet blir ivaretatt.

Undersøkelsen viser at det er uklarheter mellom IKT-leverandørene og helseforetakene om hvem som skal gjennomføre konkrete informasjonssikkerhetstiltak:

- Det er i mange tilfeller uklart hvem som skal gjøre nødvendig opprydding og forbedringstiltak.
- Det er uklart hvordan ansvaret for ivaretakelse av sikkerheten i medisinsk-teknisk utstyr skal fordeles

Opprydding og forbedringstiltak blir forsinket eller satt på vent fordi det ikke er avklart hvem som skal utføre oppgaven. I noen tilfeller er ansvaret delt mellom flere parter (helseforetak og regional IKT-leverandør), og arbeidet stopper opp fordi én av partene ikke tar sin del av ansvaret. Både helseforetakene og IKT-leverandørene påpeker at det gjenstår praktiske avklaringer om oppgavefordeling dem imellom.

I Helse Nord, Helse Midt-Norge og Helse Sør-Øst mener de regionale IKT-leverandørene at manglende avklaring av ansvar og oppgaver mellom helseforetakene og dem er en av hovedutfordringene i arbeidet med å forebygge og avdekke dataangrep. De er gitt et ansvar for sikkerheten i den regionale IKT-infrastrukturen, men har ikke kontroll med alt helseforetakene kobler til denne. Lokale sikkerhetsbrudd kan utgjøre en risiko for regionen som helhet, og de regionale IKT-leverandørene mener manglende avklaringer gjør det tidkrevende å rydde opp i kjente svakheter. Blant annet oppleves dette som en utfordring der det må ryddes i det helseforetakene drifter selv, og der det er vanskelig å gjennomføre oppdatering av programvare for eldre utstyr og systemer ute i helseforetakene. I Helse Vest framstår ansvaret for oppgavene som klarere.

I alle de fire regionene er det uklarheter rundt ansvaret for å ivareta sikkerheten i medisinsk-teknisk utstyr, som for eksempel røntgenutstyr eller måleinstrumenter. Medisinsk-teknisk utstyr har blitt stadig mer integrert i IKT-området ved at en større andel av utstyret i praksis er datamaskiner med egne lagringsenheter og oppkobling mot nettverk. Også Riksrevisjonens undersøkelse av informasjonssikkerhet i medisinsk-teknisk utstyr, som ble rapportert i Dokument 3:2 (2015-2016), viste at det var uklare ansvarslinjer for informasjonssikkerheten for slikt utstyr, både internt i helseforetakene og mellom helseforetakene og de regionale IKT-leverandørene.

Hvordan oppgavene er fordelt for slikt utstyr mellom regional IKT-leverandør og helseforetak varierer, både mellom regioner og mellom helseforetak i samme region. Helse Vest skiller seg ut ved at regional IKT-leverandør ikke er involvert i drift av regionens medisinsk-tekniske utstyr, og i liten grad i sikring av utstyret. Medisinsk-teknisk utstyr er plassert i et nettverk som er sikret av Helse Vest IKT, men for øvrig er det helseforetakene i regionen som ivaretar sikkerheten gjennom sikkert oppsett, sikkerhetsoppdateringer, tilgangskontroller og overvåking.

Etter vår vurdering er det ikke godt nok avklart innad i helseregionene hvem som har ansvaret for å gjennomføre nødvendige informasjonssikkerhetstiltak. I noen tilfeller må helseregionene klargjøre ansvar- og myndighetsforholdene i styringssystemene, i andre tilfeller må det gjøres presiseringer i databehandleravtaler, tjenesteavtaler og andre avtaler om hvem som har det formelle ansvaret og hvem skal utføre oppgaver. Konsekvensen av manglende avklaringer er at viktige tiltak for å forebygge dataangrep blir forsinket eller ikke gjennomført.