Møtedato: 14. desember 2016

Arkivnr.:	Saksbeh/tlf:	Sted/Dato:
	Ida Marthinussen/Hilde Rolandsen	Bodø, 8.12.2016

Styresak 153-2016 Informasjonssikkerhet i foretaksgruppen - lukking av svakheter, oppfølging av styresak 95-2015

Saksdokumentene var ettersendt.

Formål

Styret i Helse Nord RHF behandlet *styresak 95-2015 Informasjonssikkerhet i foretaksgruppen* i styremøte 30. september 2015. Styret fattet følgende vedtak i punkt 2: *Styret ber adm. direktør om å legge frem en helhetlig plan innen utgangen av 2016 for lukking av svakhetene som er påpekt i Riksrevisjonens rapport Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013. Dokument 3:2 (2014-2015), del II, sak 2 og 3.*

Denne styresaken er en oppfølging av vedtakets punkt 2 i styresak 95-2015 for å orientere styret i Helse Nord RHF om svakheter i informasjonssikkerheten og pågående arbeid for å oppnå tilfredsstillende informasjonssikkerhet.

Bakgrunn

På oppdrag fra Helse- og omsorgsdepartementet gjennomførte Norsk Helsenett SF i 2015 en inntrengningstest mot Universitetssykehuset Nord- Norge HF (UNN) og Helse Nord IKT. I 2016 ble det gjennomført en ny inntrengningstest mot Nordlandssykehuset HF og Helse Nord RHF. Begge disse testene avdekker svakheter.

Riksrevisjonen har også i flere rapporter påvist svakheter ved risikostyring av informasjonssikkerheten ved helseforetakene.

Oppfølging av informasjonssikkerhet i Helse Nord

Helse Nord IKT

For å følge opp de svakheter som er blitt avdekket gjennom inntrengningstestene, og andre sentrale sikkerhetsutfordringer har Helse Nord IKT iverksatt FAKT-programmet (Felles arkitektur, konsolidering og teknologi). Dette er et helhetlig program for modernisering, etablering og realisering av de regionale IKT-tjenester.

Helhetlig IKT-sikkerhet er et eget prosjekt under dette programmet, som har til formål å beslutte og forankre overordnet målbilde for IKT-sikkerhet i Helse Nord. Prosjektet skal utarbeide en anbefaling av tiltak med prioriteringer og tidsplan for å lukke avvikene. Tiltak for å lukke identifiserte avvik vil bli gjennomført fortløpende, men det er sannsynlig at noen av disse vil fortsette utover 2017. Detaljert beskrivelse i eget utrykt vedlegg som er unntatt offentlighet etter Offentleglova § 24 tredje ledd.

Helse Nord RHF
Nettverk for informasjonssikkerhet er blitt endret til fagråd for informasjonssikkerhet (FRIS). Formålet med dette er oppnå en målrettet utvikling og styring på dette området. I denne sammenheng er dette arbeidet styrket med ressurser ved å ansatte informasjonssikkerhetsleder i Helse Nord RHF, som også er leder for FRIS.

Status oppfølging av Riksrevisjonens undersøkelser
I 2015 sendte Helse Nord RHF et likelydende brev til styreleder og adm. direktør ved helseforetakene i regionen om oppfølging av Riksrevisjonens rapporter, og da med henblikk på svakheter ved risikostyring av informasjonssikkerheten. Bakgrunnen for brevet er at Helse Nord RHF vurderer at fagfeltet informasjonssikkerhet ikke er blitt gitt tilstrekkelig fokus og prioritet. Dette er et komplekst og ressurskrevende fagfelt.

Status som ble presentert i styrene i forbindelse med oppdragsdokumentet 2015 er ikke tilstrekkelig detaljert til å kunne gi styret trygghet for at fagområdet informasjonssikkerhet ivaretas tilstrekkelig, og at helseforetakene etterlever de plikter som lovverket krever.

Etter dette har alle helseforetakene utarbeidet forpliktende plan for gjennomføring av nødvendige risiko- og sårbarhetsanalyser (ROS). For kliniske systemer er status at helseforetakene følger oppsatt plan, men med mindre forsinkelser. Figuren under viser en mer detaljert oversikt pr. helseforetak. Nødvendige risiko- og sårbarhetsanalyser skal være gjennomført innen 31. desember 2016, og om fristen ikke overholdes, skal det gis skriftlig begrunnelse for dette.

Helseforetak	**Antall ROS som skal gjennomføres**	**Antall ROS som er gjennomført**	**Antall ROS som er påbegynt men ikke sluttført**	**Antall ROS som ikke er påbegynt**
Finnmarkssykehuset	12	8	4	0
UNN	27	5	6	16
Nordlandssykehuset	16	10	4	2
Helgelandssykehuset	16	13	3	0
Sykehusapotek Nord	2	1	1	0
Helse Nord IKT	16	10	5	1

Figur 1 - oversikt status for gjennomføring av risiko- og sårbarhetsanalyser per helseforetak

Status for risiko og sårbarhetsanalyser for medisin teknisk utstyr (MTU) viser at det kun er Nordlandssykehuset HF som vil kunne gjennomføre dette innen 31. desember 2016. Dette er en krevende oppgave, og helseforetakene har gitt tilbakemelding om at det er ønskelig med en regional koordinering av prosessen. God samhandling mellom Fagråd for informasjonssikkerhet (FRIS) og Fagforum medisin teknikk er en forutsetning for en helhetlig prosess. Dette arbeidet har så vidt startet og vil fortsette inn i 2017.

Rollefordelingen mellom Helse Nord IKT og helseforetakenes medisinsk-tekniske miljø er et risikoområde og skal derfor gjennomgås i 2017.

Oppfølging av Riksrevisjonens undersøkelser om helseforetakenes ivaretakelse av elektroniske pasientjournaler (EPJ) har tre ulike tilnærminger. Innsyn i egne opplysninger for den registrerte, sykehusenes eget forbedringsarbeid og mønstergjenkjenning.

I desember 2015 fikk alle pasienter i Helse Nord elektronisk tilgang til egen pasientjournal. Fra og med desember 2016 skal også pasientene i regionen få elektronisk innsyn i loggen i EPJ/PAS.

For å styrke sykehusenes eget forbedringsarbeid vil Helse Nord RHF innføre mer løpende rapportering rundt lukking av avvik. I denne sammenhengen er det viktig å fremheve at mye av arbeidet rundt lukking av avvik vil styrkes som følge av innføringen av felles kliniske system (FIKS). Tilfredsstillende informasjonssikkerhet og et godt personvern for den registrerte er en forutsetning for innføring av en felles journal.

Den tredje tilnærmingen går ut på at Helse Nord RHF sammen med de tre andre regionale helseforetakene skal etablere en nasjonal felles løsning for drift av mønstergjenkjenning i regi av Norsk Helsenett SF. Grunnet manglende finansiering er en felles nasjonal løsning utsatt til 2017. Det forventes at Helse Nord kan være første region ut.

For flere detaljer rundt oppfølging av Riksrevisjonens undersøkelser om helseforetakenes ivaretakelse av elektroniske pasientjournaler (EPJ), se vedlegg *Status Riksrevisjonens undersøkelser om helseforetakenes ivaretakelse av elektroniske pasientjournaler (EPJ)*.

Adm. direktørs vurdering
Adm. direktør viser til *styresak 157-2016/4 Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2015 - Dokument 3:2 (2016-2017), informasjon*, der informasjonssikkerhet rundt EPJ er kommentert. Det har vært en positiv utvikling, men det er fremdeles et stort behov for ytterligere forbedring. Vi forventer at Riksrevisjonen gjennomfører en oppfølgingsrevisjon på senere tidspunkt.

Økt digitalisering av tjenestene, endringer i rammebetingelser som følge av nytt regelverk og et sammensatt risikobilde gjør at Helse Nord står ovenfor store utfordringer innen fagfeltet informasjonssikkerhet.

Deling av pasientopplysninger med andre helseforetak og realisering av en felles journal forutsetter tilfredsstillende informasjonssikkerhet. Dette innebærer blant annet dokumentasjon som viser et akseptabelt risikonivå ved behandling av pasientopplysninger. I ytterste konsekvens kan manglende etterlevelse føre til begrensinger i realisering av en felles journal.

EU-parlamentet har vedtatt en ny personvernforordning. Det betyr at alle EU- og EØS-land vil få et nytt personvernregelverk som trer i kraft mai 2018. Den nye personvernforordningen vil erstatte personopplysningsloven og tilhørende forskrifter. Det nye regelverket gir virksomheter nye plikter, og personer som får sine opplysninger registrert får nye rettigheter.

Endringer i risikobildet tilsier også at trusselmetodene er i rask utvikling, og at angrepene er mer avanserte og mer komplekse enn tidligere. Et utviklingstrekk er at interessen for pasientinformasjon er blitt større. Innsamling av slike data er et mål for både kriminelle og statssponsende aktører, og sykehus er potensielle mål for slik informasjonsinnsamling.

Det er adm. direktørs vurdering at det er et økende fokus på området, men for å ha et tilfredsstillende risikonivå krever det at foretaksgruppen har kontinuerlig fokus på de prosesser som er beskrevet her. Eventuelle nye finansieringsbehov knyttet til tekniske tiltak vurderes ved rullering av langsiktig investeringsplan i 2017.

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

1. Styret i Helse Nord RHF tar informasjonen om status for arbeidet med informasjonssikkerhet i foretaksgruppen til orientering.

2. Styret ber adm. direktør om å legge frem en langsiktig plan for området informasjonssikkerhet, ved at dette blir omtalt og innarbeidet ved rullering av langsiktig plan, som legges frem i juni 2017.

3. Styret ber adm. direktør om å legge frem en egen styresak om status og handlingsplan for informasjonssikkerhet innen utgangen av 2017.

Bodø, den 8. desember 2016

Lars Vorland
Adm. direktør

Vedlegg: Status Riksrevisjonens undersøkelser om helseforetakenes ivaretakelse av elektroniske pasientjournaler (EPJ)

Vedlegget er lagt ut på Helse Nord RHFs nettsted – se her: *Styremøte i Helse Nord RHF 14. desember 2016*

Utrykt vedlegg: Status nødvendige evner for å ivareta sikkerhet - Helse Nord IKT, unntatt offentlighet, jf. Offl. § 24, 3. ledd

Utrykte vedlegg oversendes på forespørsel.