Møtedato: 29. april 2015
Arkivnr.:

Saksbeh/tlf:
Hilde Rolandsen/Oddvar Larsen

Sted/Dato:
Bodø, 17.4.2015

Styresak 46-2015/3 Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013. Dokument 3:2 (2014-2015). Del II, sak 2 og 3: Helseforetakenes beredskap innen IKT, vann, strøm og styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler

Formål
Riksrevisjonens utvidede kontroll for 2013 har bl.a. omfattet de fire RHF-enes beredskap på områdene IKT, vann og strømforsyning, og til styring og kontroll av tilgang til helseopplysinger i elektroniske pasientjournaler. Riksrevisjonen har funnet grunnlag for merknader.

Formålet med å legge frem saken for styret i Helse Nord RHF er å orientere om status og fremdrift for å korrigere de avvik som er kommet frem i Riksrevisjonens rapport. Det vises spesielt til:

- Kap 2, Sak 2 (side 19), og til vedlegg 2.3 (side 119) som gjelder beredskap innen IKT, strøm og vannforsyning.
- Kap 2, Sak 3 (side 23), og til vedlegg 2.3 (side 131) som gjelder styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler

Om beredskap innen IKT strøm og vannforsyning - hovedfunn
Riksrevisjonens rapport og oppfølging av denne er et viktig underlag i gjennomføringen av plan 2015-2018, kap. 1.3.12 om at Helse Nord skal ha oppdaterte beredskapsplaner for kriser og katastrofer på alle nivå. Det vises også til kap. 11 om risikostyring og internkontroll, der det heter *bruke metodikken i risikostyring som grunnlag for å identifisere, vurdere og håndtere potensiell risiko ved hjelp av en strukturert tilnærming*.

Riksrevisjonens sentrale funn
For de områder denne saken omhandler, heter det i rapporten;
Helseforetakene mangler eller har mangelfulle risiko- og sårbarhetsanalyser og beredskaps-planer for ikt, vann og strøm. Disse innsatsfaktorene er avgjørende for sykehusdriften. Helseforetakene gjennomfører få beredskapsøvelser, og ledelsen i helseforetakene følger i liten grad opp dette arbeidet. Videre er helseforetakene lite bevisst sin rolle som eier av dataene og databehandlingsansvarlig. Selv om Helse-og

omsorgsdepartementet (HOD) og de regionale helseforetakene har lagt til rette for beredskapsarbeidet har oppfølgingen vært for svak.

Riksrevisjonens rapport bygger på innhentet skriftlig informasjon fra helseforetak og regionale helseforetak og i egne møter. I sluttarbeidene med rapporten har Helse Nord RHF hatt dialog med Helse- og omsorgsdepartementet (HOD) som har ivaretatt dialogen med Riksrevisjonen.

HOD understreker at helseforetakene i fremtiden vil arbeide for å ha gode helhetlige beredskapsplaner i samarbeid med relevante aktører, og viser til at kravene til beredskap for kritisk infrastrukturer er gjentatt i protokollene fra foretaksmøtene i 2014.

Helse Nord RHF har gitt uttrykk for at rapportens påpekning av mangler innenfor beredskapsområdet også er tilfelle i Helse Nord, dog med noe innbyrdes variasjon mellom helseforetakene.

Oppfølging i Helse Nord
I arbeidet med oppdatering av beredskapsplaner er overordnede scenariouavhengige beredskapsplaner prioritert. Alle helseforetak arbeider nå med underliggende planer, herunder kritisk infrastruktur.

Dette har vært nødvendig og ønskelig for å sikre en overordnet og helhetlig beredskap. Flere reelle hendelser har bekreftet dette. Det vises også til Riksrevisjonens rapport, side 20, der det heter: *Riksrevisjonen har merket seg at der det har vært hendelser med ikt, strøm og vann, har disse blitt taklet tilfredsstillende av helseforetakene. Riksrevisjonen mener likevel at omfanget av faktiske hendelser, og de alvorlige konsekvenser disse hendelsene kan få for pasient-behandlingen, gjør det nødvendig å øve personalet og organisasjonene i beredskapsarbeid.*

Flere hendelser den senere tid som gjelder IKT-svikt og strømbrudd har imidlertid vist behovet for å gjennomføre ROS-analyser og utarbeide konkrete beredskapsplaner.

Helse Nord RHF har innhentet informasjon om status i planer i helseforetakene og Helse Nord IKT. Felles dialog om planer og erfaringer fra hendelser gjøres i Regionalt beredskapsutvalg (REBU).

I dialogen med HOD har Helse Nord RHF informert om oppfølgingen, slik:
1. Utarbeide en samlet fremstilling som viser fremdriften i dette arbeidet.
2. Påse at planverket samordnes med lokale myndigheter/nødetater.
3. Påse at det utarbeides øvingsplaner på to til fire års horisont som sikrer at enhetene systematisk trener større deler av organisasjonen, og dekker flere funn fra ROS-analyser.
4. Sikre at vi har enhetlige rutiner i regionen (eksempel: trening på bruk av nødjournaler, testing av nødstrømsaggregater, sjekk av vannkvalitet, rutiner for forebygging av legionella).
5. Sikre at det innføres systematisk evaluering etter øvelser, og at disse tas med i forbedringsarbeidet.
6. Foreta regelmessige besøk ved helseforetakene for å sikre fremdrift i arbeidet.

Helse Nord RHF gjennomfører før sommeren 2015 egne møter med helseforetakene, Helse Nord IKT og Luftambulansetjenesten.

Om tilgang til helseopplysninger - hovedfunn
Helseforetakene har ikke i tilstrekkelig grad implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger.

Ansatte i helseforetakene har tilgang til helseopplysninger utover tjenstlig behov. Helseforetakene har ingen systematisk kontroll og oppfølging av ansattes tilganger til EPJ[1]. Helseforetakene har mangelfull internkontroll av tilgangsstyringen i EPJ.

Riksrevisjonen anbefaler at:

- Helse- og omsorgsdepartementet pålegger de regionale helseforetakene å forsikre seg om at alle helseforetakene etterlever gjeldende regelverk for informasjonssikkerhet og behandling av helseopplysninger.

- Helse- og omsorgsdepartementet sørger for at pålegg i regelverket om føring av journalansvarlig person og gjennomføring av sikkerhetsrevisjoner blir tolket og praktisert ensartet.

- Helse- og omsorgsdepartementet og de regionale helseforetakene følger opp at helseforetakene har en hensiktsmessig tildelingspraksis som balanserer EPJ-systemets standardisering etter rolle og regelverkets pålegg om at tilgang skal være basert på individuelt tjenstlig behov.

- Helse- og omsorgsdepartementet og de regionale helseforetakene sørger for at det blir utviklet verktøy og iverksatt tiltak som er egnet for å oppdage urettmessig tilegnelse av helseopplysninger.

- De regionale helseforetakene følger opp at helseforetakene etablerer systematisk kontroll og oppfølging av ansattes tilganger, og at det etableres en tilstrekkelig internkontroll av tilgangsstyringen.

- Helseforetakene iverksetter tiltak som sikrer økt kunnskap om gjeldende regelverk og interne rutiner om behandling av helseopplysninger.

Statsråden har kommentert forholdet slik:
… Når det gjelder anbefalingen om at departementet og de regionale helseforetakene følger opp at helseforetakene har en hensiktsmessig tildelingspraksis, viser statsråden til at de regionale helseforetakene vil følge opp at tildelingen balanserer EPJ-systemets standardisering og vurdering av det enkelte helsepersonellets behov.

Statsråden påpeker at pasienter med sammensatte lidelser, endringer i pasientforløpene, økt spesialisering og samhandling er forhold som innebærer at flere virksomheter er involvert i pasientbehandlingen enn tidligere, og at mange ansatte må ha tilgang til opplysninger, også på tvers av grensen mellom psykiatri og somatikk.

[1] EPJ: Elektronisk pasientjournal

Statsråden opplyser at de regionale helseforetakene må arbeide videre med forbedring av systematisk kontroll og oppfølging av ansattes tilganger, og etablering av tilstrekkelig internkontroll av tilgangsstyringen. Ifølge statsråden vil Nasjonal IKT HF kunne ha en sentral rolle i dette arbeidet.

Oppfølging i Helse Nord
Gjennom FIKS-prosjektet vil flere av de svakheter som er påpekt i rapporten fra Riksrevisjonen bli løst. I tillegg til den tekniske delen av prosjektet pågår det en parallell prosess med innføring av nye rutiner og standarder, jf. delprosjekt Harmonisering og Samordning (HOS).

Kontroll på informasjonssikkerhet er et vilkår for å dele journalopplysninger, hvilket er en sentral del av målsettingen med kvalitets- og IKT-strategien. Vilkår for, og foreløpige avtaler om deling av helseopplysninger har vært behandlet i som egen sak i styringsgruppen i FIKS-prosjektet.

Informasjonssikkerhetsforum planlegger å gjennomføre en GAP-analyse 2. halvår 2015. Dette etter bestilling fra Helse Nord RHF.

Saken behandles i styringsgruppen til Helse Nord IKT 16. april 2015 (sak 22-2015) med særlig vekt på status for RoS-analyser og Helse Nord IKTs arbeid med beredskapsplan, samt helseforetakenes interne håndtering av rapporten. Følgende innstilling til vedtak foreligger:
1. *Styringsgruppen tar diskusjonen til orientering.*
2. *Saken følges opp i formelle styringslinjer, jfr Oppdragsdokument*
3. *Styringsgruppen gir sin tilslutning til at Informasjonssikkerhetsforum iverksetter en GAP-analyse.*

Adm. direktørs vurdering/konklusjon
Det er en felles erkjennelse i foretaksgruppen om forbedringsbehovet både innenfor beredskaps- og informasjonssikkerhetsområdet. Det er derfor tatt inn som eget punkt i Oppdragsdokumentet for 2015 at helseforetakene skal:
- Gjennomføre risiko- og sårbarhetsanalyse på kritisk infrastruktur. Gjennomføres for vann og strøm hver for seg.
- Området informasjonssikkerhet med tilhørende status på ROS-analyser skal behandles særskilt av helseforetakenes styrer innen 01.06.15. Styresaken skal beskrive om databehandler oppfyller de krav i lover og forskrifter som er tillagt databehandlerrollen og om nødvendige krav er nedfelt i leveranseavtaler. Eventuelle avvik skal være lukket innen 31.12.15.

Adm. direktør forventer at foretaksgruppen i løpet av 2016 har lukket de svakheter som Riksrevisjonen har påpekt i sin rapport.

Adm. direktør vil innen 1. september 2016 legge frem en nærmere redegjørelse for styret i Helse Nord RHF om status innenfor begge områdene.

Vedlegg: Kopi av RR rapport side 1-11, 19-27. 109-151

Vedlegget er lagt ut på Helse Nord RHFs nettside - se her:
Styremøte i Helse Nord RHF 29. april 2015

Referanseliste: Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013
www.riksrevisjonen.no

HOS, regionale føringer og standarder - Brukertilganger - Januar 2014