Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	23. september 2021

Sak 104-2021

Status for arbeidet med informasjonssikkerhet og regional handlingsplan for informasjonssikkerhet

Forslag til vedtak:

1. Styret tar redegjørelsen om arbeidet med informasjonssikkerhet til orientering.
2. Styret slutter seg til regional handlingsplan for arbeidet med informasjonssikkerhet.
3. Styret ber om å bli holdt løpende orientert om arbeidet med å forbedre informasjonssikkerheten i Helse Sør-Øst.

Hamar, 15. september 2021

Jan Frich
konstituert administrerende direktør

1. Hva saken gjelder

Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer ble lagt frem for styret 4. februar 2021, jf. styresak 010-2021. Styret ba om å bli holdt løpende orientert om arbeidet med å forbedre informasjonssikkerheten i regionen.

Helse- og omsorgsdepartementet ba i foretaksmøtet 14. januar 2021 om at hovedfunn, merknader og anbefalinger i Riksrevisjonens undersøkelse følges opp, og at det utvikles en regional handlingsplan for arbeidet med informasjonssikkerhet som også omfatter langsiktige tiltak. Handlingsplanen skal pre senteres i Helse- og omsorgsdepartementets felles tertialoppfølgingsmøte med de regionale helseforetakene i oktober 2021.

Denne styresaken gir en orientering om status for arbeidet med å forbedre informasjonssikkerheten i regionen. Vedlagt saken er forslag til regional handlingsplan for arbeidet med informasjonssikkerhet, og det bes om styrets tilslutning til denne.

2. Hovedpunkter og vurdering av handlingsalternativer

I Helse Sør-Øst behandles opplysninger om pasienter i mange ulike systemer. Denne behandlingen foregår både analogt og digitalt, og opplysningene behandles både muntlig og skriftlig. En rekke administrative systemer behandler annen informasjon som er nødvendig for driften av tjenestene.

I Nasjonal helse- og sykehusplan 2020–2023 omtales digitalisering som en forutsetning for pasientens helsetjeneste, og det legges vekt på bedre bruk av mulighetene teknologien gir.

Ved digitalisering av informasjon vil noen risikoer reduseres, mens andre kommer til. Digitale journaler gir enklere tilgang for helsepersonell og bedre sporbarhet for hvem som har sett opplysningene. Digitaliseringen gjør det mulig for pasienter å få tilgang til egen journal hjemmefra, noe som samtidig åpner for angrep gjennom pasientenes IKT-utstyr. Når store mengder helseopplysninger samles og gjøres tilgjengelig gjennom ulike løsninger må tiltakene tilpasses, slik at kravene til informasjonssikkerhet og personvern etterleves.

Mer krevende trusselbilde

Gjennom digitaliseringen er Helse Sør-Øst eksponert for et krevende internasjonalt trusselbilde. I følge Nasjonal sikkerhetsmyndighet er trusselbildet blitt mer krevende i 2021. Et eksempel på aktuelle hendelser hackingen av selskapet Vastaamo i Finland, et senter for psykoterapi. Hackerne presset pasientene for penger når selskapet ikke ville betale løsepenger. Et annet eksempel er hackingen av Østre Toten kommune, der datasystemene ble satt ut av spill. Da kommunen valgte ikke å betale løsepenger for å gjenopprette systemene, publiserte hackerne sensitive opplysninger fra innbruddet på internett.

Sykehuspartner HF og Helse Nord IKT har samarbeidet om å beskrive trusselbildet for regionene. I rapporten kommer det frem at det finnes statlige aktører som har kompetanse og ressurser til å kunne ta kontroll over IKT-systemer i spesialisthelsetjenesten. Rapporten

peker på at det finnes avanserte kriminelle miljøer som hele tiden leter etter en åpning for å komme inn i systemene. I tillegg til ytre aktører kan ansatte i helseforetakene ha uærlige hensikter som truer informasjonssikkerheten. Helse Sør-Øst angripes hele tiden, og noen ganger vil angriperen lykkes.

Ulike hensyn må balanseres og veies mot hverandre

Systematisk arbeid med informasjonssikkerhet handler blant annet om å finne en god balanse mellom konfidensialitet, integritet og tilgjengelighet. Skal en løsning stenges ned så snart det oppdages en sårbarhet? Kan risikoen aksepteres fordi nytten løsningen gir i pasientbehandlingen er større enn faren for at sårbarheten utnyttes? For å kunne hente ut gevinster av digitalisering vil det som oftest innebære å måtte akseptere en viss risiko Balansene mellom nytte og risiko er krevende.

Helse Sør-Øst benytter risikovurderinger, revisjoner, øvelser, angrepssimuleringer, registrerte avvik og faktiske hendelser til læring og forbedring. Riksrevisjonen har i perioden 2018 til 2020 gjennomført en undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. Resultatet av undersøkelsen ble publisert i desember 2020. Undersøkelsen har gitt et godt grunnlag for det videre arbeid med informasjonssikkerhet i regionen., Noen av funnene ble gjort kjentunderveis i undersøkelsen, slik at de aktuelle helseforetakene tidlig kunne starte arbeidet med å håndtere disse. Riksrevisjonens undersøkelsen har vært styrebehandlet i Helse Sør-Øst RHF og Sykehuspartner HF. Status og tiltak ble behandlet i Helse Sør-Øst RHF i styresak 010-2021.

Helse Sør-Øst RHF har styrket ledelse og styring innen informasjonssikkerhet. Beslutninger om risiko skal tas i ledelseslinjen, der ulike hensyn kan veies mot hverandre. Informasjonssikkerhetsmiljøet skal beskrive risiko forbundet med informasjonssikkerhet som en del av underlaget lederne benytter for å kunne ta helhetlige beslutninger som avveier hensyn til pasientsikkerhet, økonomi, personvern med mer.

Helse Sør-Øst RHF har gitt regionale føringer for ivaretagelse av informasjonssikkerhet. Helseforetakene må legge frem eventuelle avvik fra føringene for eget styre før saken løftes til Helse Sør-Øst RHF. Sykehuspartner HF er gitt ansvar for infrastrukturen, og deres rolle er dermed blitt tydeligere. og. Sykehuspartner HF har videre mulighet for å sette bruksvilkår som helseforetakene må følge. Gjennom bruksvilkår kan det for eksempel stilles krav til utstyret som skal kobles på infrastrukturen for å unngå at et helseforetak utsettes for angrep på grunn av sårbarheter i et annet helseforetak. Eldre utstyr og proprietære systemer som ikke har tilstrekkelig sikkerhet eller som ikke støtter moderne sikkerhetsmekanismer representerer en utfordring. I noen tilfeller må sikkerheten i hele nettverket reduseres for at utstyret skal kunne benyttes, noe som spesielt gjelder en del medisinsk-teknisk utstyr.

Rapporteringen om risiko er forbedret

Risiko forbundet med informasjonssikkerhet og personvern inngår i risikorapporteringen til styret i Helse Sør-Øst RHF. Sykehuspartner HF rapporterer på risiko forbundet med informasjonssikkerhet både til eget styre og til Helse Sør-Øst RHF. Rapporteringen fra Sykehuspartner HF er blitt mer detaljert enn tidligere, hvor risiko brytes ned og angis med konsekvens og sannsynlighet for de største enkeltrisikoer innen informasjonssikkerhet. Sykehuspartner HF følges opp tett innen informasjonssikkerhet.

I oppdrags- og bestillingsdokumentene fra det regionale helseforetaket er helseforetakene gitt i oppdrag å rapportere om risiko, tilstand og avvik innen informasjonssikkerhet i den ordinære tertialrapporteringen. Første rapportering er mottatt. Helseforetakene beskriver sårbarheter og deres potensiale for alvorlige konsekvenser, mens risikoen knyttet til sårbarhetene omtales i mindre grad. Flere helseforetak melder om at det er satt i gang prosesser for å få bedre oversikt over risikobildet. Rapporteringen gir Helse Sør-Øst RHF økt innsikt i risikoen i helseforetakene og dermed bedre kvalitet i risikorapporteringen til styret. Rapporteringen gir også Helse Sør-Øst RHF et bedre underlag for beslutninger på informasjonssikkerhetsområdet.

Utvalgte oppdrag for styrket informasjonssikkerhet fra foretaksmøtet

I foretaksmøtet 14. januar 2021 fikk de regionale helseforetakene i oppdrag å delta i et samarbeidsforum med de andre regionale helseforetakene, Direktoratet for e-helse og Norsk helsenett SF. Arbeidet i forumet skal bidra til erfaringsoverføring på tvers, og identifisere egnede nasjonale og interregionale tiltak for å øke informasjonssikkerheten i helseforetakene og forebygge angrep mot IKT-systemene. Helse Sør-Øst RHF har tatt initiativ overfor de andre aktørene. Samarbeidsforumet er blitt etablert og har hatt sine første møter.

I foretaksmøtet 14. januar 2020 ble helseregionene bedt om å arbeide systematisk med innføring av Nasjonal sikkerhetsmyndighets grunnprinsipper for informasjonssikkerhet. Oppdraget ble gjentatt i foretaksmøte 14. januar 2021. Nasjonal sikkerhetsmyndighets grunnprinsipper er lagt til grunn i arbeidet som gjennomføres i regionen. I arbeidet gjennomgås anbefalte tiltak og det utarbeides indikatorer for å følge opp at tiltakene gir ønsket effekt over tid.

Sykehuspartner HF har fått i oppdrag å måle informasjonssikkerhetskulturen i helseforetaksgruppen. Arbeidet er startet og resultatet vil foreligge i oktober 2021. Resultatene fra undersøkelsen vil bli benyttet i helseforetakenes arbeid med informasjonssikkerhet.

Helse Sør-Øst RHFs styring og kontroll med informasjonssikkerhetsområdet er bedret blant annet gjennom følgende beslutninger:

- Risikostyring innen informasjonssikkerhet følger den ordinære risikostyringen i helseforetakene (styresak 046-2021)
- Helse Sør-Øst RHF kan gi føringer for ivaretakelsen av informasjonssikkerhet i regionen. Avvik fra regionale føringer legges frem for eget styre (styresak 046-2021)
- Sykehuspartner HF skal være foretaksgruppens kompetansemiljø for informasjons-sikkerhet (oppdrag og bestilling for Sykehuspartner HF 2020 og 2021)
- Sykehuspartner HF skal ha et helhetlig ansvar for informasjonssikkerhet i infra-strukturen (oppdrag og bestilling for Sykehuspartner HF 2020 og 2021)
- Helseforetakene må akseptere de bruksvilkårene som Sykehuspartner HF definerer for de tjenestene som helseforetakene bruker (styresak 107-2019)
- Hovedregelen er at IKT-utstyr skal være plassert i sentrale datarom (styresak 107-2019)

- Helseforetakene skal rapportere om risiko, tilstand og avvik innen informasjonssikkerhet til Helse Sør-Øst RHF (oppdrag og bestilling for Sykehuspartner HF og øvrige helseforetak 2021)
- Helseforetakene skal arbeide med systematisk innføring av Nasjonal sikkerhets-myndighets grunnprinsipper for IKT-sikkerhet (oppdrag og bestilling for Sykehuspartner HF og øvrige helseforetak 2021)
- Måling av informasjonssikkerhetskulturen (oppdrag og bestilling for Sykehuspartner HF 2021)

En plattform for å oppdage og håndtere sikkerhetshendelser

I Helse Sør-Øst oppdages nye sårbarheter og det er til enhver tid både kjente og ukjente sårbarheter som ikke er lukket. Noen sårbarheter kan lukkes raskt, mens andre sårbarheter har avhengigheter som gjør at risikoen må håndteres på annen måte. Det kan for eksempel være medisinsk-teknisk utstyr som er avhengig av gamle sårbare versjoner av programvare (f.eks. Java). For å ha tilstrekkelig kontroll med risikoen må det etableres flere barrierer for å hindre at en angriper kan utnytte en sårbarhet. I tillegg er det viktig med overvåking for å oppdage når en sårbarhet blir utnyttet.

Sykehuspartner HF har etablert Sykehuspartner CERT (Computer Emergency Response Team), et responsmiljø for sikkerhetshendelser, som skal oppdage og håndtere digitale angrep. Sykehuspartner CERT samarbeider med både private og offentlige aktører, og spesielt med HelseCERT ved Norsk helsenett SF, som er helsesektorens responsmiljø. HelseCERT samarbeider med Nasjonalt cybersikkerhetssenter (NCSC) ved Nasjonal sikkerhetsmyndighet, som er det nasjonale responsmiljøet for alle sektorer. NCSC samarbeider videre med det europeiske responsmiljøet, CERT-EU. Helse Sør-Øst er også knyttet til Nasjonal sikkerhetsmyndighets nasjonale varslingssystem for digital infrastruktur.

Sykehuspartner CERT er døgnbemannet. Sensorer i nettverkene, logger fra utstyr og programmer, og varsler fra samarbeidspartnere analyseres og følges opp fortløpende. Riksrevisjonens simulerte angrep ble oppdaget av Sykehuspartner CERT, og Riksrevisjonen fikk ikke kontroll med sentral infrastruktur i Helse Sør-Øst. Sykehuspartner HFs plattform for å oppdage og håndtere digitale angrep er adaptiv og videreutvikles fortløpende for å oppdage nye trusler.

Tiltak for økt informasjonssikkerhet

I arbeidet med å forbedre sikkerhetstilstanden er

- angrepsflatene redusert ved bedre kontroll med utdaterte systemer og internetteksponerte tjenester (blant annet ved at flere tjenester er stengt ned fordi tilstrekkelig sikkerhet ikke kunne dokumenteres)
- applikasjoner sanert og oppgradert
- spesialister leid inn for å gjennomføre kontinuerlig angrepssimulering (på linje med Riksrevisjonens angrepssimulering)
- sårbarhetsskanning fra HelseCERT supplert med sårbarhetsskanning i egen regi

Oppgraderinger og nye løsninger kan gi økt informasjonssikkerhet. Oppgradering til Windows 10, prosjekter i Program for standardisering og IKT-infrastrukturmodernisering (STIM), kryptert stamnett og diverse prosjekter for kliniske løsninger følges opp i ordinær rapportering og status er ikke tatt med her.
Riksrevisjonen har gjennomført en undersøkelse av styring og kontroll av tilgang i elektroniske pasientjournaler i fire helseforetak (vedlegg). Undersøkelsen ble offentliggjort i 2014. I Riksrevisjonens undersøkelse fra 2020 om IKT-angrep ble det påpekt at det fortsatt er funn fra tidligere revisjoner som ikke er håndtert. Funnene er i all hovedsak håndtert, og det arbeides videre med ytterligere forbedring for å hindre ulovlige oppslag fra ansatte, både gjennom etterfølgende kontroll ved bruk av statistisk logganalyse, og ved forbedret funksjonalitet for tilgangsstyring. Tiltakene er detaljert i regional handlingsplan for arbeidet med informasjonssikkerhet.

Riksrevisjonen har gjennomført en undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr (vedlegg). Undersøkelsen ble offentliggjort i 2015. Det gjenstående arbeidet med tydeliggjøring av ansvar og roller ble sluttført i 2021, og med det er alle funnene håndtert.

For Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer (vedlegg) er 43 av 47 identifiserte tekniske tiltak gjennomført per 31. juli 2021. Videre arbeider Helse Sør-Øst RHF med seks forbedringsområder, som ble behandlet av styret i sak 010-2021:

- Roller og ansvar
- Oversikt, rapportering og oppfølging
- Informasjonssikkerhetskultur og –kompetanse
- Informasjonssikkerhet i anskaffelser
- Applikasjoner, infrastruktur og teknisk sikkerhet
- Kontinuerlig forbedring

Disse forbedringsområdene detaljeres ytterligere i regional handlingsplan for arbeidet med informasjonssikkerhet.

3. Administrerende direktørs anbefaling

Digitaliseringen av helsevesenet skaper nye muligheter og økt tilgjengelighet av tjenester og viktig informasjon, og samtidig er god informasjonssikkerhet en forutsetning for trygg og sikker pasientbehandling.

Administrerende direktør er opptatt av risikoen forbundet med håndteringen av informasjon og har derfor løftet informasjonssikkerhet inn som et eget område i risikorapporteringen til styret. Administrerende direktør har videre forsterket oppfølgingen av Sykehuspartner HFs arbeid med informasjonssikkerhet og har skjerpet kravene til rapportering innen informasjonssikkerhet fra helseforetakene i regionen.

Administrerende direktør mener at arbeidet med informasjonssikkerhet er blitt ytterligere styrket etter Riksrevisjonens undersøkelse om helseforetakenes forebygging av angrep mot sine IKT-systemer. Administrerende direktør vil understreke betydningen av systematisk og kontinuerlig arbeid med informasjonssikkerhet og viktigheten av at både ledere og medarbeidere tar del i dette arbeidet.

De regionale helseforetakene ble i foretaksmøtet 14. januar 2021 bedt om å følge opp Riksrevisjonens hovedfunn, merknader og anbefalinger fra undersøkelsen om helseforetakenes forebygging av angrep mot sine IKT-systemer. Administrerende direktør mener arbeidet med informasjonssikkerhet i Helse Sør-Øst har hensyntatt Riksrevisjonens funn og anbefalinger. Tiltak for å bedre informasjonssikkerheten, inkludert håndtering av Riksrevisjonens funn, er detaljert i vedlagt forslag til regional handlingsplan for arbeidet med informasjonssikkerhet.

Administrerende direktør anbefaler at styret slutter seg til forslaget til handlingsplan. Administrerende direktør vil holde styret løpende orientert om arbeidet med å styrke informasjonssikkerhet i Helse Sør-Øst.

Trykte vedlegg:

- Regional handlingsplan for arbeidet med informasjonssikkerhet

Utrykte vedlegg:

- Undersøkelse av styring og kontroll av tilgang i elektroniske pasientjournaler i fire helseforetak (Del av dokument 3:2 (2014-2015)): https://riksrevisjonen.no/rapporter-mappe/no-2014-2015/undersokelse-av-helseopplysninger-i-elektroniske-pasientjournaler-i-fire-helseforetak/
- Undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr (Del av dokument 3:2 (2015–2016)). https://riksrevisjonen.no/rapporter-mappe/no-2015-2016/undersokelse-av-helseforetakenes-ivaretakelse-av-informasjonssikkerhet-i-medisinsk-teknisk-utstyr/
- Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer (Del av Dokument 3:2 (2020–2021)): https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/