Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	26. april 2024

Sak 036-2024

Status og regional handlingsplan for arbeidet med informasjonssikkerhet

Forslag til vedtak:

1. Styret tar status for arbeidet med informasjonssikkerhet til orientering.

2. Styret slutter seg til regional handlingsplan for arbeidet med informasjonssikkerhet.

Hamar, 19. april 2024

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Styret har bedt om å bli holdt orientert om arbeidet med å styrke informasjonssikkerheten, jamfør styresak 123-2023. I tillegg ba Helse- og omsorgsdepartementet i foretaksmøtet den 17. januar 2023 de regionale helseforetakene om å oppdatere de regionale handlingsplanene for det systematiske arbeidet med å styrke informasjonssikkerheten. Oppdateringen skal skje innen 1. mai hvert år, og det skal rapporteres fra forbedringsarbeidet.

Denne styresaken gir en orientering om status for arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst. Vedlagt saken er forslag til oppdatert handlingsplan for arbeidet med informasjonssikkerhet.

2 Hovedpunkter og vurdering av handlingsalternativer

Behandling av pasientjournaler, kvalitetsregistre, forskningsdata og andre opplysninger er en vesentlig del av det å yte gode helsetjenester. Informasjonssikkerhet handler om konfidensialitet, integritet og tilgjengelighet. Dette inngår i større eller mindre grad i alle ansattes arbeid og handler om å kunne levere helsetjenester selv om for eksempel flom, brann eller angrep påvirker IKT-systemene. I dette inngår blant annet å håndtere digitale angrep, bygge en kultur der ansatte behandler opplysninger fortrolig, og at digitale systemer gjengir opplysninger uforandret. Ikke minst handler informasjonssikkerhet om at opplysninger om pasienter skal være tilgjengelig for helsepersonell når de trenger dem.

Helse Sør-Øst RHF orienterte om status for arbeidet med informasjonssikkerhet i styresak 123-2023. Etter denne rapporteringen har det ikke inntruffet noen hendelser i foretaksgruppen innen informasjonssikkerhet som Helse Sør-Øst RHF har måttet håndtere.

2.1. Trusler og trusselaktører

Det digitale trusselbildet for spesialisthelsetjenesten i 2023 er beskrevet i felleskap mellom helseregionene og Norsk helsenett SF. Trusselvurderingen er publisert offentlig[1]. Organiserte kriminelle og enkelte statlige aktører vurderes å utgjøre den største trusselen for tilsiktede handlinger mot våre digitale løsninger.

Politiets sikkerhetstjeneste har i sin nasjonale trusselvurdering for 2024 skrevet at organisasjoner i helsesektoren er blant statlige cyberaktørers hovedmål i Norge. Både Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste mener problematikken med innsidevirksomhet er mer aktuell, og at det fra statlige aktører er forventet økt innsats for å rekruttere innsidere i Norge.

Trusselaktørers bruk av ny teknologi som kunstig intelligens forventes å gjøre det mer krevende å stoppe phishing, sosial manipulering og andre angrep.

[1] Trusselvurdering 2023 - Sykehuspartner HF

Skillet mellom ekte og falsk informasjon antas å bli mer krevende for pasienter, pårørende og ansatte fremover. I spesialisthelsetjenesten er det et par hundre nettsteder utenfor felles nettløsning for spesialisthelsetjenesten[2]. Det er ikke enkelt å avgjøre om et nettsted er fra en troverdig kilde. Påvirkningsaksjoner i grensen mellom ekte og falsk informasjon kan bli krevende å håndtere. Påvirkningsaksjoner kan justere befolkningens generelle oppfatning i negativ retning, og vil kunne bli en utfordring også for helsetjenesten. Tillitssamfunnet er viktig for å kunne opprettholde helsetjenestens funksjon som i dag. Helseregionene har satt i gang et felles arbeid for bedre kontroll med nettsteder. Det bærende prinsippet i arbeidet er å samle helseforetakenes kommunikasjon på de offisielle nettsidene dvs på felles nettløsning for spesialisthelsetjenesten. Med det oppnås at det blir enklere for brukerne å bekrefte ektheten av et nettsted, og det kan gis redaksjonell støtte i tråd med retningslinjer.

2.2. Systematisk arbeid for å håndtere trusler og farer

Digitalisering vil redusere og fjerne noen risikoområder, mens nye risikoer kommer til. Det er viktig å arbeide systematisk med risikostyring og ha et bevisst forhold til utvikling i trussel- og sårbarhetsbilde. Både tilsiktede og utilsiktede handlinger kan utløse hendelser som svekker måloppnåelsen i Helse Sør-Øst. Som eksempler kan blant annet menneskelige feil, tekniske feil, naturkatastrofer og tilsiktede angrep føre til at informasjon ikke er tilgjengelighet eller at krav om integritet og konfidensialitet ikke oppfylles. Resultatet kan være at kvaliteten i pasientbehandlingen reduseres. God informasjonssikkerhet er en forutsetning for god pasientbehandling.

Ansattes holdninger og handlinger er viktige for hvordan informasjonssikkerheten ivaretas. Digital sikkerhetskultur er målt årlig i foretaksgruppen siden i 2021 og vil måles igjen i 2024. Resultatene følges opp i hvert enkelt helseforetak.

Felles kriterier for å beskrive og akseptere informasjonssikkerhetsrisiko er innført i Helse Sør-Øst. I kriteriene ligger blant annet en tydeliggjøring av at risikoeier skal akseptere og beslutte håndtering av restrisiko. Utarbeidelse av beslutningsgrunnlag og implementering av nye saksbehandlingsprosesser er krevende. Tilpasning pågår fortsatt.

Kunstig intelligens er tatt i bruk pasientbehandlingen og har gitt gevinster både for helse-foretak og pasienter. Helse Sør-Øst regner med at dette området vil bli viktigere framover. Det er stor variasjon innen kunstig intelligens, fra spesialtilpassede løsninger til generiske språkmodeller. Risikoen varierer, blant annet etter type løsning og hva den benyttes til. Det er viktig å fange opp informasjonssikkerhetsrisikoene i slike løsninger, som for andre løsninger som er avhengige av informasjonsbehandling.

Riksrevisjonen publiserte i desember 2020 undersøkelsen av helseforetakenes forebygging av angrep mot sine IKT-systemer. I år vil Riksrevisjonen gjennomføre en treårsoppfølging av undersøkelsen. Denne gangen vil undersøkelsen fokusere på Helse Nord og Helse Sør-Øst.. I Helse Sør-Øst vil Sykehuspartner HF, Sykehuset Innlandet HF og Helse Sør-Øst RHF under-søkes nærmere.

De regionale helseforetakene har i felleskap tatt initiativ til oppfølging av IKT og informasjonssikkerhet i de felleseide helseforetakene. Status på arbeidet ble lagt frem i det interregionale møtet for administrerende direktører (sak 151-2023). Det ble klargjort at de

[2] Forside - Felles nettløsning for spesialisthelsetjenesten (fnsp.no)

felleseide helseforetakene selv er ansvarlige for sin informasjonssikkerhet. De felleseide helseforetakene får flere av sine IKT-tjenester levert fra helseregionenes IKT-selskaper. Ansvaret til driftsleverandøren reguleres i avtaler og er i stor grad i samsvar med det ansvaret driftsleverandøren har ovenfor øvrige helseforetak de leverer tjenester til.

2.3. Identifiserte sårbarheter og risikoer

Det er viktig å arbeide med sårbarheter og risikoer og å håndtere disse, både for å unngå alvorlige enkelthendelser, og for å unngå mange mindre uønskede hendelser som samlet gir vesentlig skade. Det kan for eksempel være tid som brukes på unødvendige steg for å hente informasjon en har tjenstlig behov for.

Helseforetakene har i sin rapportering omtalt de største risikoene. Et utvalg av disse er knyttet til løsepengevirus, usikkerhet rundt bruk av skytjenester, gamle domener og utdatert programvare, medisinsk-teknisk utstyr og manglende tilgjengelighet til IKT-systemer. Eksempler på informasjonssikkerhetsbrudd som er rapportert fra helseforetak, er bortfall av varslingssystemet på et rom, slik at pasienten ikke fikk kontakt med personalet, registrering av helseopplysninger på feil pasient og brudd på taushetsplikt.

I henhold til pasientjournalloven skal behandlingsrettede helseregistre understøtte pasientforløp i klinisk praksis og være lett å bruke og å finne frem i. I henhold til helse-personelloven skal helsepersonell gis nødvendige og relevante helseopplysninger når det er nødvendig for å gi forsvarlig helsehjelp. Dette gjelder også på tvers av helseforetak og mellom helsetjenestenivåene. Svikt vil typisk være i forbindelse med samhandling og ansvarsoverganger. I styresak 123-2023 ble et scenario beskrevet med redusert kvalitet i pasientbehandlingen grunnet manglende registrering i kjernejournal. Regjeringen varsler i Nasjonal helse- og samhandlingsplan 2024-2027[3]at den vil prioritere et tiltak som tar ned denne risikoen: Personell skal kunne registrere opplysningene i eget fagsystem, samtidig som opplysningene overføres automatisk til kjernejournalen.

Vurderingen fra Helse Sør-Øst RHF er at det innen informasjonssikkerhet ikke er høye risikoer, på en skala med lav, moderat og høy risiko. Det vil si at det ikke er høy sannsynlighet for at alvorlige hendelser inntreffer.

Det er derimot noen moderate risikoer. Som illustrasjon beskrives to utvalgte risiko-scenarier, med beskrivelse av konsekvens og tilhørende årlig sannsynlighet for at scenariet skal inntreffe med angitt konsekvens:

- Et scenario er redusert kvalitet i pasientbehandlingen fordi relevant informasjon ikke er tilgjengelig. Helseforetak er involvert i en rekke samhandlinger om pasient-forløp eller ansvarsoverganger i pasientforløp. Det kan være krevende å hente opplysninger fra andre helseforetak og fra primærhelsetjenesten. I tillegg rapporterer noen helseforetak om manglende tilgjengelighet til IKT-systemer. Hendelser knyttet til informasjonssikkerhetsbrudd med liten konsekvens er meget sannsynlige og skjer flere ganger hvert år. Det utgjør en moderat risiko.

[3] Meld. St. 9 (2023-2024) kapittel 9.4.1, kulepunkt om kritisk informasjon.

- Et annet scenario er der organiserte kriminelle løsepengeutpressere får tilgang til infrastrukturen og bruker tilgangen til å kryptere deler av opplysningene og gjøre systemer utilgjengelig. Konsekvensen vil være alvorlig, både for pasientenes personvern og for pasientbehandlingen. Helse Sør-Øst har en stor portefølje av applikasjoner og en kompleks infrastruktur, hvorav flere applikasjoner er utdatert. Helse Sør-Øst har hatt noen dataangrep med alvorlig konsekvens. På den andre siden har Helse Sør-Øst mange sikkerhetstiltak for å beskytte, oppdage og håndtere digitale angrep. Det vurderes som lite sannsynlig at scenarioet vil inntreffe, men på grunn av alvorlighetsgraden vil det likevel utgjøre en moderat risiko.

Som del av daglig drift gjennomføres det risikovurderinger av løsninger før de settes i produksjon. Opp mot nasjonale sikkerhetsinteresser er det gjennomført vurderinger og pekt ut objekter som er skjermingsverdige. Styrket risikovurdering innen informasjonssikkerhet sett opp mot helseforetakene som utøvere av kritiske samfunnsfunksjoner[4] er noe som vil vurderes nærmere.

Regelverk knyttet til samfunnsviktige funksjoner er i endring, blant annet skjerpes krav til rapportering og tilsyn. Stortinget har vedtatt lov om digital sikkerhet, som trer i kraft når Kongen bestemmer. Forskrifter til loven er under utarbeidelse, og det er flere EU-direktiver som venter på norsk gjennomføring.[5] Regelverkene understreker behovet for godt, risikobasert arbeid i spesialisthelsetjenesten, med særlig vekt på evnen til å opprettholde samfunnsviktige funksjoner.

2.4. Oppfølging av tiltak

Sykehuspartner HF avsluttet i 2023 oppgraderingen til Windows 10. Prosjektet har oppgradert om lag 69 000 klienter. I tillegg til at oppgraderingen øker sikkerheten gjennom å ta i bruk en mer moderne løsning, er det nå også mulig å gjennomføre jevnlige oppdateringer av maskinparken til nye versjoner. Dette sikrer en raskere og mer kostnadseffektiv oppgradering. Som et ledd i oppgradering til Windows 10 ble det vurdert hvilke applikasjoner som kan saneres. Antall unike klientapplikasjoner er redusert med 50 prosent de siste årene.

Alle helseforetak er migrert til Norsk helsenetts krypterte stamnett i henhold til plan. I tillegg er det etablert kryptering på forbindelser til noen mindre lokasjoner i Helse Sør-Østs nettverk og etablert krypterte samtrafikkpunkter for foretakene mellom Helse Sør-Øst og Norsk helsenett. Arbeidet har omfattet totalt 97 lokasjoner. Arbeidet med kryptering av nettverkene i Helse Sør-Øst er med dette ferdigstilt. Datatilsynet har blitt informert om at kravet om kryptering av nettverkene er lukket.

Arbeid med å holde et sikkerhetsnivå som er egnet i forhold til risiko, er et kontinuerlig arbeid. I den regionale handlingsplanen for arbeidet med informasjonssikkerhet vises de mest sentrale tiltakene det arbeides med i 2024. Risikoer identifisert i revisjoner har tiltak i handlingsplanen, mens mange av de tiltak som er foreslått i risiko- og sårbarhetsvurderinger for den enkelte løsning, følges opp i hver enkelt løsning, og disse er ikke tatt med i handlingsplanen.

---

[4] Jf. samfunnssikkerhetsinstruksen kap V og oversikt over kritiske samfunnsfunksjoner hvor spesialisthelsetjenesten er inkludert.
[5] NIS II- og CER-direktivene ble vedtatt i desember 2022, begge antas være EØS-relevante.

3 Administrerende direktørs anbefaling

Helseopplysninger skal være lett tilgjengelig for helsepersonell, slik at en unngår redusert kvalitet i pasientbehandlingen fordi relevant informasjon ikke er tilgjengelig. Samtidig skal informasjon beskyttes, blant annet mot menneskelige feil, statlige cyberaktører og organiserte kriminelle. Dette er en krevende balanse i et stadig skjerpet internasjonalt trusselbilde.

Det er gjennomført en rekke tiltak for styrket informasjonssikkerhet i Helse Sør-Øst, blant annet oppgradering av operativsystemer, modernisering av nettverk og sanering av applikasjoner. I handlingsplanen for arbeidet med informasjonssikkerhet er planlagte tiltak for ytterligere styrking av informasjonssikkerheten beskrevet.

Administrerende direktør anbefaler at styret slutter seg til forslaget til regional handlingsplan for arbeidet med informasjonssikkerhet.

Trykte vedlegg:

- Regional handlingsplan for arbeidet med informasjonssikkerhet

Utrykte vedlegg:

- Ingen