Konsernrevisjonen
Rapport 7/2022

Styring av informasjonssikkerhet i Sykehuspartner HF

19. desember 2022

Introduksjon

Helseforetakene i Helse Sør-Øst er avhengig av den felles regionale tjenesteleverandøren Sykehuspartner HF for god styring av informasjonssikkerhet.

Sykehuspartner HF har ansvar for sikring av felles IKT-infrastruktur, regionale IKT-systemer samt lokale systemer og utstyr i helseforetakene. Helseforetakene har på sin side ansvar for at systemer og utstyr brukes på en sikker måte.

Riksrevisjonens undersøkelse i 2020 avdekket flere vesentlige mangler ved helseforetakenes informasjonssikkerhetsstyring. På bakgrunn av undersøkelsen etablerte Helse Sør- Øst RHF flere tiltak, hvor av et av tiltakene var å gjennomføre en internrevisjon av Sykehuspartner HF.

Formålet med revisjonen er å vurdere tilstanden på styringen av informasjonssikkerhet i Sykehus-partner HF, samt undersøke hvordan informasjon om Sykehuspartner HFs styring inngår som et grunnlag for de øvrige helseforetakenes styring av informasjonssikkerhet.

Revisjonen baserer seg på innhentet informasjon fra Sykehuspartner HF og en spørreundersøkelse som har blitt rettet mot de øvrige helseforetakene i Helse Sør-Øst.

Rapporten er bygget opp med et innledende sammendrag som belyser de viktigste observasjonene i revisjonen. Videre fremkommer observasjoner og anbefalte tiltak i kapitlene 3 og 4.

Innholdsfortegnelse

1. Sammendrag

Revisjonen av styring av informasjonssikkerhet i Sykehuspartner HF viser at Sykehuspartner HF har etablert og vedlikeholder et ledelsessystem for informasjonssikkerhet som er basert på ISO 27001-standarden. Sykehuspartner HFs ledelsessystem bygger på Helse Sør-Østs regionale ledelsessystem som er supplert med virksomhetenes egne dokumenter.

Sykehuspartner HFs ledelse viser engasjement og har rettet stor oppmerksomhet mot ledelses-systemet. Sykehuspartner HFs ledelsessystem beskriver ulike roller og deres ansvar for informasjons-sikkerhet. Likevel forekommer det roller som ikke er tilstrekkelig konkretisert og som skaper uklar-heter i samhandlingen mellom Sykehuspartner HF og de øvrige helseforetakene.

Sykehuspartner HF har definert og benytter en prosess for risikostyring av informasjonssikkerhet. For å forbedre prosessen, er Sykehuspartner i ferd med å innføre et verktøy for å understøtte helhetlig styring av både risiko og tiltak.

ISO 27001-standarden anbefaler at en virksomhet har et bestemt sett med styrende dokumenter. Sykehuspartner HFs ledelse har etablert flere prosesser for overvåking, måling og evaluering av informasjonssikkerhet som dekker store deler av ledelsessystemet, men det gjenstår både å utarbeide og oppdatere noen sentrale styrende dokumenter.

Helse Sør-Øst RHF og Sykehuspartner HF har opprettet samhandlingsarenaer med de øvrige helse-foretakene, Regionalt sikkerhetsfaglig råd (RSR) og Regionalt sikkerhetsvurderingsteam (RSV).

Sykehuspartner HF har etablert en prosess for styring av informasjonssikkerhetsrisiko som er godt forankret i regionen. Til tross for dette fremkommer det at samhandlingen i prosessen for risiko- og sårbarhetsanalyse (ROS) ikke fungerer tilfredsstillende. Problemet er erkjent av Sykehuspartner HF som er i ferd med å iverksette tiltak for å evaluere og forbedre prosessen.

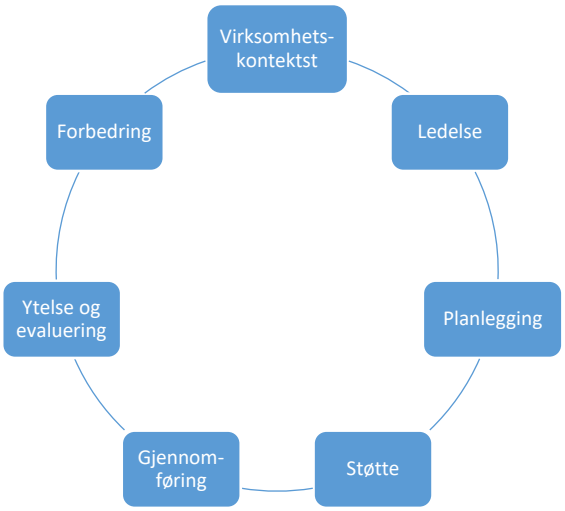
Videre viser revisjonen at Sykehuspartner HF har innført tiltak for å heve kompetanse og bevissthet innen informasjonssikkerhet i helseforetakene. I tillegg vurderer Sykehuspartner HF at informasjon fra foretaksgruppens responsmiljø (CERT) for hendelser i større grad kan deles for å skape en bedre situasjonsforståelse og bevissthet hos helseforetakene.

Det er gitt anbefalinger innen områdene virksomhetskontekst, ledelse, risikostyring, gjennomføring, samt ytelse og evaluering. Anbefalingene oppsummeres i tabellen under.

	Delområder	**Anbefaling**
Del 1	Virksomhets-kontekst	Sykehuspartner HF bør inkludere informasjonssikkerhetsmessige risikoer ved gjennomgang og oppfølging av avtaler med helseforetakene.
	Ledelse	Sykehuspartner HF bør systematisk revidere og oppdatere sine styrende dokumenter i sitt ledelsessystem for informasjonssikkerhet.
	Risikostyring	Sykehuspartner HF bør fortsette forbedring av prosessene som ledelsen bruker for å følge opp og ha oversikt over helseforetakets egne risikoreduserende tiltak.
	Gjennomføring	Sykehuspartner HF bør fortsette med å styrke prosesser og praksis som gir en helhetlig tilnærming ved ledelsens gjennomgang av styringen av informasjons-sikkerhet.
	Ytelse og evaluering	Sykehuspartner HF bør vurdere tiltak som bidrar til en helhetlig intern rapportering av sikkerhetstilstanden.
Del 2	Virksomhets-kontekst	Sykehuspartner HF og de øvrige helseforetakene bør utvikle en målrettet og risikobasert rapportering til helseforetakene som bidrar til nødvendig trygghet for helseforetakenes egen styring.
	Ytelse og evaluering	Sykehuspartner HF bør vurdere å dele sentrale funn og erfaringer fra rapporter og CERT med de øvrige helseforetakene, forutsatt at helseforetakene håndterer fortrolig informasjon på en forsvarlig måte.

2. Revisjonens tilnærming

Det er to sentrale problemstillinger for denne revisjonen. Den første går ut på å vurdere styringen av informasjonssikkerhet i Sykehuspartner HF. Den andre problemstillingen handler om å undersøke hvordan informasjon om Sykehuspartner HFs styring inngår som et grunnlag for de øvrige helseforetakenes styring av informasjonssikkerhet. De to problemstillingene besvares i de to neste kapitlene og følger strukturen i ISO 27001-standarden for informasjonssikkerhet som er brukt som grunnlag i revisjonen. I figuren under vises delområdene som starter med *virksomhetskontekst.*



Figur 1: Delområder i ISO 27001-standarden

3. I hvilken grad har Sykehuspartner HF etablert et ledelsessystem for informasjons-sikkerhet?

Dette kapitlet oppsummerer revisjonens første del. Videre inneholder kapitlet anbefalinger og konklusjoner som er basert på revisjonens observasjoner.

3.1 Oppsummering

Sykehuspartner HF har etablert og innført et ledelsessystem for informasjonssikkerhet, og jobber kontinuerlig med forbedring og vedlikehold av systemet. Ledelsessystemet innbefatter også regionale bruksvilkår som virksomhetene i regionen må etterleve slik det fremkommer styresak 107-2019 i det regionale helseforetaket. Sykehuspartner HFs ledelse viser engasjement og har stor oppmerksomhet rettet mot styringssystemet. Ledelsen har sikret at ansvar og myndighet for roller innen informasjonssikkerhet er tildelt og kommunisert internt. Likevel er det identifisert noen utfordringer ved den regionale styringsmodellen for informasjonssikkerhet som gjør omfanget av Sykehuspartner HFs ansvar for informasjonssikkerhet uklart i foretaksgruppen.

Helseforetaket har definert og benytter en prosess for risikostyring av informasjonssikkerhet, men mangler et verktøy for å understøtte helhetlig styring av både risiko og tiltak.

Sykehuspartner HF har etablert prosesser for overvåkning, måling og evaluering av informasjonssikkerhet som dekker store deler av styringssystemet, men det gjenstår både å utarbeide og oppdatere noen få sentrale dokumenter. Videre oppfattes Sykehuspartner HF å ha en kultur for å oppdage, rapportere og dokumentere avvik i systemet. Til tross for dette kunne Sykehuspartner HF i større grad dele informasjon fra risiko- og tiltaksregistrene, fra CERT og generelt om sikkerhetstilstanden med de øvrige helseforetakene.

3.2 Observasjoner og anbefalinger

Virksomhetskontekst

Sykehuspartner HF ivaretar hensynet til leveranserelaterte risikoer gjennom regionalt ledelsessystem for informasjonssikkerhet med supplerende lokale tilpasninger. Sykehuspartner HFs egne risikoer håndteres med utgangspunkt i policy for risikostyring. Ansvaret Sykehuspartner HF har for informasjonssikkerhet som tjenesteleverandør beskrives gjennom tjenesteavtaler med helseforetakene. Videre benytter Sykehuspartner HF seg av to faste møterekker med Regionalt sikkerhetsfaglig råd (RSR) og Regionalt sikkerhetsvurderingsteam (RSV) samt med flere uformaliserte samhandlingsmøter.

Sykehuspartner HF har dermed etablert og innført et ledelsessystem for informasjonssikkerhet. Sykehuspartner HF arbeider kontinuerlig med forbedring og vedlikehold av systemet, men har foreløpig ikke utarbeidet dokumentet som formaliserer omfanget av ledelsessystemet.

Databehandleravtaler med eksterne leverandører er ikke systematisk gjenstand for oppfølging eller revisjon. Sykehuspartner HF rapporterer ikke til helseforetakene om egen etterlevelse av kravene som fremkommer i avtaler. Dette er ikke et krav i ISO-standarden, men skulle det være et behov for slik rapportering i de øvrige helseforetakene, bør dette i så fall avtales med Sykehuspartner HF.

Konsernrevisjonen anbefaler at Sykehuspartner HF inkluderer informasjonssikkerhetsmessige risikoer ved gjennomgang og oppfølging av avtaler med helseforetakene. Videre kunne Sykehuspartner HF vurdere behovet for rapportering fra eksterne leverandører på etterlevelse av avtaler, for eksempel ved bruk av samsvarserklæringer.

Ledelse

Sykehuspartner HFs ledelse viser engasjement og har oppmerksomhet på foretakets ledelsessystem for informasjonssikkerhet. Sykehuspartner HFs ledelse har sikret at ansvar og myndighet for Sykehuspartner HFs roller relevant for informasjonssikkerhet, er tildelt og kommunisert internt.

Til tross for dette opplever Sykehuspartner HF uklarheter ved sitt totalansvar for informasjonssikkerhet. Her peker Sykehuspartner HF på et forbedringspotensial i ledelsessystemet med en tydeligere forankring av hvilket ansvar foretaket har for informasjonssikkerhet, fordi delt ansvar i foretaksgruppen skaper noen utfordringer.

Sykehuspartner HF har etablert policy for informasjonssikkerhet og personvern. Policy-en har ikke blitt revidert siden mai 2019.

Konsernrevisjonen anbefaler at Sykehuspartner HF systematisk reviderer og oppdaterer sine styrende dokumenter i sitt ledelsessystem for informasjonssikkerhet. Helse Sør-Øst RHF kunne med

fordel ta initiativ til en gjennomgang med Sykehuspartner HF og helseforetakene for å konkretisere og sørge for konsensus rundt rollene og ansvarsfordelingen i regionen.

Risikostyring

Sykehuspartner HF har definert og benytter en prosess for risikostyring og risikovurdering for informasjonssikkerhet. Sykehuspartner HF har ikke hatt verktøystøtte for helhetlig risikostyring, men planlegger å anskaffe et verktøy som understøtter en slik tilnærming.

Sykehuspartner HF har definert en prosess for behandling av informasjonssikkerhetsrisiko. Sykehuspartner HF har en prosess for ROS-vurderinger og risikoreduserende tiltak utarbeides for identifiserte risikoer. Tiltakene tildeles en tiltakseier. Tiltak som eies av Sykehuspartner HF, følges opp av tiltakseiere i foretaket. Sykehuspartner HF har ikke et sentralt verktøy for å håndtere identifiserte risikoer og planlagte tiltak. Dette betyr at Sykehuspartner HF ikke har en helhetlig oversikt som viser om tiltakene er gjennomført.

Sykehuspartner HF har et styrende dokument med 15 sikkerhetsmål. Det er ikke utarbeidet en detaljert plan for å oppnå sikkerhetsmålene. Mye av målingen skjer på enkeltkomponenter og dekker ikke alle de etablerte sikkerhetsmålene. Sykehuspartner HF opplyser at de i løpet av revisjonen har oppdatert sikkerhetsmålene.

Konsernrevisjonen anbefaler at Sykehuspartner HF fortsetter forbedring av prosessene som ledelsen bruker for å følge opp og ha oversikt over helseforetakets egne risikoreduserende tiltak.

Støtte

Sykehuspartner HF har i all hovedsak tilgang til tilstrekkelig med informasjonssikkerhetsressurser. Hvis nødvendig kan ledelsen gi informasjonssikkerhetsleder i Sykehuspartner HF tilgang til ekstra ressurser. Interne roller og ansvar er definert dokumentert i styrende dokumenter. Sikkerhetsbevissthet er et sentralt element i styringen av Sykehuspartner HFs virksomhet. For å bevisstgjøre medarbeiderne om viktigheten av informasjonssikkerhet, gjennomføres det årlige sikkerhetssamtaler, kampanjer og annen opplæring.

Det meste av ledelsessystemet er dokumentert, men Sykehuspartner HF har ikke utarbeidet en erklæring av relevans (*Statement of Applicability – SoA*) og et dokument som definerer omfanget av ledelsessystemet i henhold til standarden.

Gjennomføring

Sykehuspartner HF har definert og benytter en prosess for behandling av informasjonssikkerhetsrisiko. I henhold til prosessen skal identifisert risiko håndteres på en hensiktsmessig måte. Slike risikovurderinger er et fast punkt i ledelsens gjennomgang hvert tertial. Selv om Sykehuspartner HF har mange elementer på plass i sitt ledelsessystem, har foretaket ikke en tilstrekkelig systematisk tilnærming til innholdet ved ledelsens gjennomgang av informasjonssikkerhetsprosesser.

Konsernrevisjonen anbefaler at Sykehuspartner HF fortsetter med å styrke prosesser og praksis som gir en helhetlig tilnærming ved ledelsens gjennomgang av styringen av informasjonssikkerhet.

Ytelse og evaluering

Sykehuspartner HF overvåker, måler og evaluerer deler av ledelsessystemet. For å forbedre av oppfølgingen av etterlevelse er Sykehuspartner HF i ferd med å etablere nye KPI-er. Videre har Sykehuspartner HF identifisert et behov for å lage et system som bidrar til å måle og dokumentere sin etterlevelse med hensyn til NSMs grunnprinsipper. I tillegg gjennomfører Sykehuspartner HF revisjon av én leverandør i året, primært rettet mot hovedleverandørene.

Ledelsens gjennomgang gjennomføres hvert tertial ved innrapporteringer fra virksomhetsområder. Innholdet i Sykehuspartner HFs rapportering er ikke like systematisk og har et forbedringspotensial for å kunne presentere status for foretakets samlede arbeid innen informasjonssikkerhet.

Konsernrevisjonen anbefaler at Sykehuspartner HF vurderer tiltak som bidrar til en helhetlig intern rapportering av sikkerhetstilstanden.

Forbedring

Konsernrevisjonen oppfatter at Sykehuspartner HF har en kultur for å oppdage, rapportere og dokumentere avvik. Dagens avvikssystem beskrives av Sykehuspartner HF er ikke så godt egnet til oppfølging, og Sykehuspartner HF er i ferd med å ta i bruk et nytt støtteverktøy for avvikshåndtering. Videre har Sykehuspartner HF fokus på kontinuerlig forbedring av ledelsessystemet gjennom Information Security Management Board (ISMB) som jevnlig vurderer styrende dokumenter.

4. I hvilken grad skaper Sykehuspartner HFs system for styring av informasjonssikkerhet et godt grunnlag for at de øvrige helseforetakene kan ivareta sitt selvstendige ansvar for informasjonssikkerhet?

Dette kapitlet oppsummerer revisjonens andre del. Videre inneholder kapitlet anbefalinger og konklusjoner basert på en risikovurdert prioritering av observasjonene.

4.1 Oppsummering

Sykehuspartner HFs ledelsessystem for informasjonssikkerhet tar hensyn til interne og eksterne interessenter gjennom de etablerte faste møtearenaene hvor Sykehuspartner HF normalt deltar. I tillegg utarbeider Sykehuspartner HF periodiske virksomhetsrapporter som er åpent tilgjengelig.

Sykehuspartner HF har etablert en prosess for styring av informasjonssikkerhetsrisiko som er godt forankret i regionen. Til tross for dette fremkommer det at samhandlingen i prosessen for risiko- og sårbarhetsanalyse (ROS) ikke fungerer tilfredsstillende. Problemet er erkjent av Sykehuspartner HF som er i ferd med å iverksette tiltak for å evaluere og forbedre prosessen.

Videre viser revisjonen at Sykehuspartner HF har innført tiltak for å heve kompetanse og bevissthet innen informasjonssikkerhet i helseforetakene. Likevel gir helseforetakene uttrykk for ønske om flere informasjonssikkerhetsrelaterte tjenester fra Sykehuspartner HF. I tilfelle bør helseforetakene benytte de etablerte bestillingskanalene til dette.

I tillegg vurderer Sykehuspartner HF at informasjon fra foretaksgruppens responsmiljø (CERT) for hendelser i større grad kan deles for å skape en bedre situasjonsforståelse og bevissthet hos helseforetakene. Dette må forutsette at helseforetakene som får del i slik sensitiv informasjon, korrekt håndterer den innenfor gjeldende begrensninger.

Sykehuspartner HF opplyser at for å effektivt oppfylle sitt ansvar for informasjonssikkerhet, vil det være en ubetinget fordel at de øvrige helseforetakene også har kartlagt og prioritert sine informasjonsverdier slik at dette kan inngå som grunnlag for Sykehuspartner HFs forbedringsarbeid.

4.2 Observasjoner og anbefalinger

Virksomhetskontekst

Sykehuspartner HFs ledelsessystem for informasjonssikkerhet tar hensyn til interne og eksterne interessenter gjennom de etablerte faste møtearenaene hvor Sykehuspartner HF normalt deltar. I tillegg utarbeider Sykehuspartner HF periodiske virksomhetsrapporter som er åpent tilgjengelig. Samtidig oppfatter konsernrevisjonen at interessenter i flere helseforetak savner tilstrekkelig informasjon om hvordan helseforetakenes data behandles.

Konsernrevisjonen anbefaler at Sykehuspartner HF og de øvrige helseforetakene utvikler en målrettet og risikobasert rapportering til helseforetakene som bidrar til nødvendig trygghet for helseforetakenes egen styring.

Ledelse

Ledelsen i Sykehuspartner HF har fordelt ansvaret og myndighet for informasjonssikkerhet ved bruk av sitt ledelsessystem. Samtidig opplyser Sykehuspartner HF at det er uklar ansvarsdeling mellom Sykehuspartner HF og helseforetakene på noen områder. Det er risiko for at en slik uklarhet mellom helseforetakene forplanter seg videre internt i Sykehuspartner HFs organisasjon.

Risikostyring

Sykehuspartner HF har etablert flere prosesser hvor styring av informasjonssikkerhetsrisikoer inngår. Til tross for dette opplyser interessenter i flere helseforetak at informasjon om risikoer innen informasjonssikkerhet ikke er tilstrekkelig slik at helseforetakene selv kan vurdere sannsynlighet, konsekvenser og eventuelle tiltak.

Videre anser de fleste interessentene at gjennomføringstiden for ROS-analyser blir altfor lang. Dette kan medføre at for eksempel innføring av nye informasjonssystemer på helseforetakene blir unødig tidkrevende. Deler av forklaringen til dette ligger utenfor Sykehuspartner HF. Problemet er erkjent og Sykehuspartner HF er i ferd med å evaluere prosessen for å forbedre den. Utover dette opplyser Sykehuspartner HF at det er uklart i hvilken grad tiltakene fra ROS-analysene blir fulgt opp av helseforetakene.

Støtte

Spørreundersøkelsen som ble gjennomført i revisjonen, viser at Sykehuspartner HF har innført tiltak for å heve kompetanse og bevissthet innen informasjonssikkerhet i helseforetakene. Til tross for dette gis det uttrykk for at Sykehuspartner HF kan være mer aktiv for å tilby flere kompetansehevende og bevisstgjørende tjenester til helseforetakene. Dette vil forutsette at helseforetakene for sin del blir tydeligere på hvilke behov de faktisk har innen dette området.

Ytelse og evaluering

Sykehuspartner HF CERT (*Computer Emergency Response Team*) er foretaksgruppens responsmiljø for hendelser og Sykehuspartner HF vurderer i større grad å bruke denne funksjonen for å bidra til en bedre situasjonsforståelse og bevissthet hos helseforetakene. Til slutt synliggjør spørreundersøkelsen at flere foretak ønsker tilgang til data som fanges opp gjennom CERT. Dette forutsetter at helseforetakene som får del i slik sensitiv informasjon, korrekt håndterer den innenfor gjeldende begrensninger.

Sykehuspartner HF gjennomfører årlige internrevisjoner av blant annet CERT, tilganger og brannmurer. Resultatet av revisjonene deles ikke med helseforetakene, hvilket kan redusere helseforetakenes mulighet til å planlegge og gjennomføre risikobaserte bekreftelsesaktiviteter.

Konsernrevisjonen anbefaler at Sykehuspartner HF vurderer å dele sentrale funn og erfaringer fra rapporter og CERT med de øvrige helseforetakene, forutsatt at helseforetakene håndterer fortrolig informasjon på en forsvarlig måte.

5. Nærmere om grunnlaget for revisjon

Helse Sør-Øst RHF og Sykehuspartner HFs rolle og ansvar

Helse Sør-Øst RHF (Helse Sør-Øst RHF) er et regionalt helseforetak som eies av staten ved Helse- og omsorgsdepartementet (HOD). Helse Sør-Øst RHF sørger for spesialisthelsetjenester til 3,1 millioner mennesker i Innlandet, Oslo, Vestfold og Telemark, Viken og Agder. Det arbeider til sammen 81.000 medarbeidere i helseforetakene. Foretaksgruppens årsomsetning er 88 500 millioner kroner.

Regionen består av totalt elleve helseforetak, og Sykehuspartner HF er foretaket som leverer sikker og stabil drift av IKT-utstyr, nettverk, kliniske og administrative applikasjoner og IKT-infrastruktur til alle sykehusene i Helse Sør-Øst. Sykehuspartner HF eies av HSØ RHF. Det er likevel inntil videre helse-foretakene selv som er dataansvarlig for sine personopplysninger. Derfor er det viktig med en konkret fordeling og eierskap til ansvaret rundt informasjonssikkerhet mellom Sykehuspartner HF og de øvrige helseforetakene. Manglende samsvar med regelverk, informasjonssikkerhetsstandarder og god praksis kan ha gjennomgående effekt på hele foretaksgruppen og vil medføre risiko for redusert kvalitet i helsehjelpen, negative omdømmekonsekvenser og finansielle tap.

Revisjon utført av Riksrevisjonen i 2020

Riksrevisjonen gjennomførte en revisjon og publiserte dokument ((3:2) i 2020), der det ble påpekt flere vesentlige svakheter i helseforetakene knyttet til informasjonssikkerhetsstyringen.

Riksrevisjonens rapport viser at helseregionene har satt i verk flere forbedringstiltak for å styrke informasjonssikkerheten. Likevel påpekte Riksrevisjonen en rekke utfordringer med å gjennomføre forbedringstiltak. De mest sentrale utfordringene var relatert til kompleksitet og omfang av utstyr, systemer og programvare, manglende opprydding, uklar ansvars- og oppgavefordeling, og ansattes uheldige sikkerhetsatferd.

Rammeverket for informasjonssikkerhetsledelse: ISO 27001 og viktigheten av god informasjonssikkerhetsledelse

Informasjon og data er ofte en av virksomhetens viktigste verdier, spesielt for en virksomhet som Sykehuspartner HF, som behandler store mengder sensitive opplysninger. Sensitiv informasjon som eventuelt mistes, stjeles eller skades kan derfor få alvorlige konsekvenser i og utenfor foretaks-gruppen.

ISO 27001 er en internasjonal standard for implementering av et styringssystem for informasjons-sikkerhet. Hensikten med styringssystemet er å beskytte bedriftens informasjonsverdier og standarden kan bidra til informasjonssikkerhetsarbeid som er enklere å håndtere, måle og forbedre. ISO 27001 synliggjør ledende praksis, og definerer styringsledelse for en helhetlig og strukturert tilnærming til informasjonssikkerhet.

Sykehuspartner HFs ledelsessystem er basert på ISO 27001. Sykehuspartner HF er likevel ikke sertifisert i henhold til standarden, og er ikke forpliktet til å følge kravene i standarden.

6. Metode

Revisjonsarbeidet har i hovedsak bestått av tre faser som beskrevet under.

Utarbeiding av oppdragsplan

Det ble først utarbeidet en oppdragsplan for den forestående revisjonen. Planen beskriver formål og problemstillinger, revisjonskriterier og metodisk tilnærming. Planleggingen har tatt utgangspunkt i en risikobasert tilnærming, innhenting av informasjon fra sentrale nøkkelpersoner, samt eventuelle tidligere revisjoner og funn for å identifisere utfordringer og viktige fokusområder.

Gjennomføring av revisjonen

For å vurdere tilstanden på styringen av informasjonssikkerhet i Sykehuspartner HF og hvordan dette inngår som grunnlag for de øvrige helseforetakene, er revisjonens undersøkelser basert på standard ISO 27001 som er grunnlaget for regionens ledelsessystem for informasjonssikkerhet. Standarden består av delområdene virksomhetskontekst, ledelse, planlegging, støtte, gjennomføring, ytelse og evaluering, og forbedring.

Innsamling av data for å vurdere tilstanden på styring av informasjonssikkerhet i Sykehuspartner HF er basert på intervjuer, spørreundersøkelse og dokumentanalyse. Spørreundersøkelsen er gjennomført for å undersøke hvordan informasjon om Sykehuspartner HFs styring inngår som et grunnlag for de øvrige helseforetakenes styring av informasjonssikkerhet. Basert på spørreundersøkelsen ble det i tillegg gjennomført intervju i et helseforetak.

Reviderte enheter

For å innhente relevant informasjon og undersøke problemstillingene, er det valgt ut sentrale medarbeidere både fra Sykehuspartner HF, de øvrige helseforetakene og det regionale helseforetaket. Spørreundersøkelsene ble utsendt til representanter for samtlige helseforetak i regionen, med unntak av Sykehuspartner HF og Sykehusapotekene HF. Spørreundersøkelsens respondenter er administrerende direktører, fagdirektører, informasjonssikkerhetsledere og IT-direktører, teknologidirektør. Intervjuobjektene i Sykehuspartner HF og Sykehuset i Vestfold fremgår av listen i vedlegg 2.

7. Vedlegg

Tabell 1: Informasjonsgrunnlag

Dokumentasjon	
Sykehuspartner HF Policy for informasjonssikkerhet og personvern i Sykehuspartner HF, 15.05.19	Sykehuspartner HF Ledelsens gjennomgang: Årlig melding 2021
Sykehuspartner HF Policy for Risikostyring, 17.11.20	Sykehuspartner HF Revisjonsrapporter fra 2016-2022
Sykehuspartner HF Beredskapspolicy, 11.11.20	Sykehuspartner HF ROS-analyser, 3 versjoner fra 2022
Sykehuspartner HF Fullmaktstruktur, 03.05.22	Sykehuspartner HF-09 – Sikkerhetssamtale 2022
Sykehuspartner HF Mandat Security Governance Board (SGB), 12.01.21	Sykehuspartner HF NO-13 Sikkerhetsinstruks, 14.03.22
Sykehuspartner HF Mandat Regionalt Sikkerhetsvurderingsteam (RSV), 02.01.17	Sykehuspartner HF NO-16 Regional autentiseringspolicy for Helse Sør-Øst, 23.09.22
Sykehuspartner HF Mandat Information Security Management Board (ISMB), 20.05.20	Sykehuspartner HF NO-30 – Regionale sikkerhetsprinsipper og –krav for skytjenester, 23.03.22
Sykehuspartner HF Lover, forskrifter og rammer, 16.11.22	Sykehuspartner HF NO-31 Regional Sikkerhetspolicy for Sikkerhetstjenester, 08.04.21
Sykehuspartner HF Sikkerhetsmål for Sykehuspartner, 10.08.15	Sykehuspartner HF NO-45 – Sikkerhetsoppdateringer og IKT-sårbarheter i Helse Sør-Øst, 14.04.22
Sykehuspartner HF Revisjonsprogram for Sykehuspartner HF 2022	HSØ Oppdrag og bestilling (OBD) 2022
Sykehuspartner HF Rollekatalog og beskrivelser	HSØ Revisjonsplan for HSØ 2022
Sykehuspartner HF Risikovurdering 2022 T2	HSØ Mål og strategi for informasjonssikkerhet i Helse Sør-Øst, 22.04.21
Sykehuspartner HF NSM grunnprinsipper kartlegging, 05.11.21	HSØ NO-1 - Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet og personvern, 23.10.18
Sykehuspartner HF CERT – vaktrapporter 2022	HSØ NO-2 – Sikkerhetsregulerende lovverk gjeldende for foretaksgruppen, 23.10.2018
Sykehuspartner HF Trusselvurdering 2022	HSØ NO-4 – Organisering av personvern- og informasjonssikkerhetsarbeidet, 09.12.21
Sykehuspartner HF Rapport inntrengingstest, september 2021	HSØ NO-5 – Kriterier for vurdering og aksept av risiko innen informasjonssikkerhet, 03.11.22
Sykehuspartner HF Sikkerhetsnytt, 3 versjoner fra 2022	HSØ NO-6 – Sikkerhetsstrategi, 23.10.18
Sykehuspartner HF Direktørmøte - Hoxhunt	HSØ NO-8 – Bruk av databehandler – Behandling av personopplysninger hos annen juridisk enhet, 23.10.18
Sykehuspartner HF Ledelsens gjennomgang	HSØ Mandat – Regionalt sikkerhetsfaglig råd (RSR), 30.02.2022
Sykehuspartner HF Tjenestekatalog, oppdateres løpende	Spørreundersøkelse for helseforetakene i HSØ
Sykehuspartner HF Referat ledermøte, 25.10.22	
Sykehuspartner HF Virksomhetsrapport 2022	
Sykehuspartner HF Leverandøroppfølging, oppdateres løpende på Sykehuspartner HFs intranett	
Sykehuspartner HF Læringsportal	

Tabell 2: Gjennomførte intervjuer

Dato	Navn og stilling/funksjon
27.09.22	Christian Jacobsen, Informasjonssikkerhetsleder, Sykehuspartner HF - Del 1
07.10.22	Christian Jacobsen, Informasjonssikkerhetsleder, Sykehuspartner HF - Del 2
12.10.22	Olav S. Ulvund, IKT-direktør, Sykehuspartner HF
14.10.22	Hanne T. Nilsen, Administrerende direktør, Sykehuspartner HF
18.10.22	Thomas Erstad, Kundeansvarlig, Sykehuspartner HF
24.10.22	Jan Ottar Holt, ROS-ansvarlig, Sykehuspartner HF
25.10.22	Thomas Djupvik, Seksjonsleder Identitet og Tilgang, Sykehuspartner HF
27.10.22	Bård A. Hansen, Chief Risk Officer (CRO), Sykehuspartner HF
28.10.22	Anne Thea Hval, Leder for virksomhetsstyring, Sykehuspartner HF
31.10.22	Solveig Tolleshaug, ansvarlig for CERT, Sykehuspartner HF
08.11.22	Thor A. Pedersen, Informasjonssikkerhetsleder for Sykehuset i Vestfold

Om konsernrevisjonen i Helse Sør-Øst

Konsernrevisjonen er organisert direkte under styret i Helse Sør-Øst RHF og rapporterer funksjonelt til styrets revisjonsutvalg og administrativt til administrerende direktør i det regionale helseforetaket. Konsern-revisjonens rapporter behandles av styret i det reviderte helseforetak.

Konsernrevisjonen ble etablert i 2005, og er fra 1. januar 2013 hjemlet i helseforetaksloven §37a.

Konsernrevisjon skal på vegne av styret i Helse Sør-Øst bidra til forbedring i risikostyring, internkontroll og virksomhetsstyring i Helse Sør-Øst RHF og underliggende helseforetak.

Vår visjon

Konsernrevisjonen skal være en etterspurt bidragsyter til læring og forbedring i Helse Sør-Øst.

Dette skal vi oppnå gjennom:

- Relevante revisjons- og rådgivningsoppdrag som skaper innsikt
- Effektiv kommunikasjon og godt samarbeid
- Deling av erfaringer og læringspunkter på tvers av helseforetakene

Om revisjonsprosjektet

Revisjonsperiode: August-november 2022
Virksomhet: Sykehuspartner HF
Oppdragsgiver: Konsernrevisjonen i Helse Sør-Øst RHF

Revisjonsteamet:

- Espen Anderssen (Oppdragseier - Konsernrevisor)
- Esa Leporanta (Konsernrevisjonen)
- Anders Blix (Konsernrevisjonen)
- Bjørn Jonassen (Eksternt medlem av revisjonsteamet)
- Svein Bekkevold (Eksternt medlem av revisjonsteamet)
- Marit Sommerseth Schiefloe (Eksternt medlem av revisjonsteamet)
- Marius Aune (Eksternt medlem av revisjonsteamet)

Rapporten er oversendt til:

- Styret i Sykehuspartner HF
- Administrerende direktør i Sykehuspartner HF
- Revisjonsutvalget i Helse Sør-Øst RHF
- Administrerende direktør i Helse Sør-Øst RHF

Konsernrevisjonens rapporter

Rapporter er tilgjengelig på følgende web-adresse:
https://www.helse-sorost.no/om-oss/styret/konsernrevisjonen