HELSE SØR-ØST

Regional handlingsplan for arbeidet med informasjonssikkerhet

1 Innledning

Informasjonsbehandling er en sentral og integrert del av helsetjenesten. Informasjonssikkerhet skal sørge for at informasjon er tilgjengelig ved behov, ikke blir endret enten utilsiktet eller av uvedkommende, eller at informasjon blir kjent for uvedkommende.

I foretaksmøtet den 17. januar 2023 ble Helse Sør-Øst RHF bedt om å: «*oppdatere de regionale handlingsplanene for det systematiske arbeidet med å styrke informasjonssikkerheten og med å lukke de sårbarhetene som Riksrevisjonens undersøkelse avdekket. Oppdatering skal skje innen 1. mai hvert år og det skal rapporteres fra forbedringsarbeidet*».

Denne handlingsplanen omfatter tiltak basert på mål og strategi for informasjonssikkerhet i Helse Sør-Øst, revisjoner, øvelser, angrepssimuleringer, avvik og faktiske hendelser. Det utføres i tillegg mange risikovurderinger i Helse Sør-Øst hvor risikoreduserende tiltak identifiseres. Dette kan eksempelvis være risikovurderinger knyttet til innføring av nye digitale løsninger. De enkelte helseforetakene har et selvstendig ansvar for å akseptere risiko, herunder om risikoreduserende tiltak skal iverksettes. Disse tiltakene inngår i de ulike risikovurderingene og er ikke tatt med i handlingsplanen.

Gjennomførte tiltak fra forrige versjon av handlingsplanen er tatt ut. Alle øvrige tiltak videreføres, med oppdatert status. Nye tiltak er lagt til.

2 Mål

Helse Sør-Øst har en risikobasert tilnærming til informasjonssikkerhet der tiltak mot de største risikoene vurderes og iverksettes slik at egnet informasjonssikkerhet opprettholdes. Arbeidet med informasjonssikkerhet er et kontinuerlig arbeid, blant annet fordi både trusselbildet, organisering og oppgaveløsning endres over tid.

Målet med tiltakene er å opprettholde egnet informasjonssikkerhet i foretaksgruppen.

3 Tiltak

Handlingsplanen har tiltak innen seks områder som følger. Status per 3. mars 2023 er beskrevet for hvert tiltak.

3.1 Roller og ansvar

Kriterier for vurdering og aksept av risiko beskriver hvordan beslutning om risiko skal være helhetlig og tas i ledelseslinjene.

Sykehuspartner HF er bedt om å tilpasse egne prosesser for risikostyring innen informasjonssikkerhet i henhold til mål og strategi for informasjonssikkerhet og kriterier for vurdering og aksept av risiko innen informasjonssikkerhet, og legge disse frem for Direktørmøtet.

Forbedret risikostyring
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Tilpasse prosesser for beslutning om aksept av risiko, slik at helhetlige beslutninger kan tas i ledelseslinjene.
Status: Pågår

3.2 Oversikt, rapportering og oppfølging

Helseforetakene har opplysninger og systemer som er viktig for pasientbehandlingen og annen måloppnåelse. En trusselaktør kan ha ønske om å skade disse verdiene. Helseforetakene har derfor fått oppdrag om å ha bedre oversikt over verdiene.

Oversikt over verdier
Ansvarlig: Helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Informasjonssikkerhet handler om å sikre informasjonsbehandlingen som inngår i systemer og ansattes arbeid. Helseforetaket skal ha oversikt over sine viktigste verdier og risikoer, slik at ikt-systemer og tjenester bestilles med egnet sikkerhetsnivå. Helseforetaket skal gjøre Sykehuspartner HF kjent med verdiene og relevante endringer som påvirker informasjons-sikkerheten
Status: Oppdrag gitt i oppdrags- og bestillingsdokumenter for 2023 til helseforetakene.

For å kunne ha oversikt, rapportering og oppføling av gradert informasjon er det nødvendig å ha egnede kommunikasjonssystemer. Det er gitt oppdrag i foretaksmøtet 17. januar 2023 om utbredelse av nasjonalt begrenset nett til helseforetakene.

Etablere nasjonalt begrenset nett (NBN) i helseforetakene
Ansvarlig: Helseforetakene
Relevant for: Helseforetakene
Tidsperiode: 2023

Beskrivelse: Etablere nasjonalt begrenset nett (NBN) (tekst og tale) i underliggende helseforetak og utpekte virksomheter i spesialisthelsetjenesten i samarbeid med Norsk helsenett SF.
Status: Helseforetakene har fått i oppdrag å etablere NBN. Sykehuspartner HF har fått oppdrag om å bistå.

Oppfølging av skjermingsverdige verdier i henhold til foretaksmøtet 17. januar 2023.

Forebyggende sikkerhetstiltak for å beskytte skjermingsverdige verdier
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Gjennomføre forebyggende sikkerhetstiltak for å beskytte skjermingsverdige verdier for å opprettholde et forsvarlig sikkerhetsnivå
Status: Gitt som oppdrag til Sykehuspartner HF i oppdrags- og bestillingsdokumentet for 2023.

3.3 Informasjonssikkerhetskultur og –kompetanse

Det er etablert et samarbeidsforum for informasjonssikkerhet mellom helseregionene. Regionalt sikkerhetsfaglig råd er et sted for utveksling av kunnskap innen informasjonssikkerhet.

Brukerutvalget mener generelt at informasjonssikkerhet i større grad må fokuseres på i det daglige arbeidet på alle nivåer av helsetjenesten, på en slik måte at det i større grad blir en naturlig og normal del av daglig drift, virksomhet og virksomhetsstyring. På denne måten integreres det som en del av kulturen i helsetjenesten.

Kjennskap til sikkerhetskulturen er viktig for å kunne iverksette eventuelle tiltak dersom det er behov for forbedring av kulturen.

Måling av informasjonssikkerhetskultur
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: Årlig
Beskrivelse: Måling av informasjonssikkerhetskultur som kan benyttes i helseforetakenes kulturarbeid.
Status: Måling av informasjonssikkerhetskultur skal gjennomføres i tredje kvartal 2023. Resultatet vil legges frem for foretaksgruppen i oktober 2023. Helseforetakene vil deretter følge opp funn og resultater i egen virksomhet.

De ansattes informasjonssikkerhetskompetanse skal styrkes gjennom felles digital opplæring. Regional delstrategi for utdanning og kompetanse har et tiltak om å bidra til å heve medarbeidernes digitale kompetanse. Informasjonssikkerhet og personvern inngår i dette.

Utarbeide opplæring for styrket digital kompetanse innen informasjonssikkerhet
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Alle ansatte i foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Utarbeidelse av digitalt opplæringsmateriell for å styrke den ansattes digitale kompetanse, inkludert kompetanse innen informasjonssikkerhet og personvern.
Status: Pågår

Økt kompetanse om trusselbildet gis gjennom en felles årlig rapport som utarbeides av helseregionene i samarbeid med Norsk helsenett SF.

Trusselvurdering
Ansvarlig: Regionale ikt-selskaper i fellesskap
Relevant for: Spesialisthelsetjenesten
Tidsperiode: Årlig
Beskrivelse: Utarbeide en årlig rapport i samarbeid med Norsk helsenett SF om trusler og trender som spesialisthelsetjenesten kan benytte i sitt arbeid med risiko- og sårbarhetsvurderinger innen 1. juni hvert år. Erfaringer fra hendelser, penetrasjonstesting og portskanningstester vil være relevant.
Status: Planlagt behandlet i Sykehuspartner HFs styre den 24. mai 2023.

For å øke kompetansen om skjermingsverdige verdier er det gitt oppdrag om øvelse i foretaksmøtet 17. januar 2023.

Øve på håndteringen av uønskede kritiske hendelser
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Øve på håndteringen av uønskede kritiske hendelser, jf. NSMs grunnprinsipper for IKT-sikkerhet. Dette skal skje i samarbeid med Norsk helsenett SF.

Status: Oppdrag gitt til Sykehuspartner HF i oppdrags- og bestillingsdokumentet for 2023.

3.4 Informasjonssikkerhet i anskaffelser

I interregionale anskaffelser bidrar Sykehuspartner HF med fagkompetanse innen informasjonssikkerhet.

Informasjonssikkerhet i produkter og tjenester som anskaffes krever også forvaltning etter anskaffelsen er ferdig. Det kan for eksempel være medisinsk-teknisk utstyr eller behandlingshjelpemidler hvor leverandøren har utviklet forbedret funksjonalitet eller rettet opp feil etter anskaffelsen er gjennomført

Forvaltning og oppfølging av leverandører
Ansvarlig: De regionale helseforetakene
Relevant for: Spesialisthelsetjenesten
Tidsperiode: 2021–2023
Beskrivelse: For nasjonale anskaffelser kan det pekes på en region for å forvalte området som en anskaffelse omfatter, slik at arbeidet med risikoanalyser og oppfølging av leverandører blir mer effektivt etter anskaffelsen er gjennomført.
Status: Det pågår et arbeid, ledet av regionenes ikt-direktører, med å lage en plan for hvordan forvaltning av ulike områder kan fordeles mellom regionene.

3.5 Applikasjoner, infrastruktur og teknisk sikkerhet

Helse Sør-Øst har mange applikasjoner, systemer og en kompleks infrastruktur som inkluderer utdatert maskinvare og gamle domener med ulikt oppsett. Dette hindrer samhandling og flyt av opplysninger mellom systemer, og det gjør at Helse Sør-Øst er mer utsatt for dataangrep. Det er sentralt å unngå duplisering og uønsket variasjon av ikt-løsninger.

Brukerutvalget er også opptatt av at planene framover gjennomføres, med fokus på oppgraderinger, innføring av felles/like systemer og forbedret informasjonsflyt og -deling. Dette vil etter brukerutvalgets oppfatning forenkle oppfølgingen av informasjonssikkerhet i regionen.

Sanering av applikasjoner, systemer og infrastruktur
Ansvarlig: Helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Helseforetakene har i styresak 107-2019 blitt bedt om å bidra aktivt til sanering av applikasjoner.

Status: Det pågår et arbeid med sanering.

Riksrevisjonen har gjennomført en undersøkelse av styring og kontroll av tilgang i elektroniske pasientjournaler i fire helseforetak[1]. Undersøkelsen ble offentliggjort i 2014. Funn i Riksrevisjonens undersøkelse er i all hovedsak håndtert i Helse Sør-Øst. Det er identifisert to forbedringspunkter hvor det ene handler om tilgangsstyring.

Bedre tilgangsstyring er selvsagt en viktig innsats for å oppnå og ivareta godt og sikkert personvern. Samtidig bemerker brukerutvalget at tilgangsstyring må utformes på en slik måte at det både ivaretar det ønskede personvernet, og muliggjør effektive og hensiktsmessige arbeidsrutiner for helsepersonellet. Tilgangsstyring må ikke bli slik at det medfører unødig stort ressursforbruk, som f.eks. uforholdsmessig tidsbruk og kompetansekrav for personellet, og dermed medføre mindre tid til pasienter og behandling. Det er viktig at man hele tiden også har pasientsikkerhet i fokus når man utformer systemer og grader av tilgangsstyring.

Forbedret tilgangsstyring i journalsystemer
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: Vil følge innføringsplanen for DIPS Arena.
Beskrivelse: Innføre DIPS Arena med bedre funksjonalitet for tilgangsstyring.
Status: Det pågår et arbeid med innføring av DIPS Arena.

Det andre forbedringspunktet etter Riksrevisjonen undersøkelse om journalsystemer handler om etterfølgende kontroll av logger.

Statistisk logganalyse
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: Følger innføringsplanen for statistisk logganalyse og vil være innført i Helse Sør-Øst innen første halvdel av 2023.
Beskrivelse: Det er et krav om å ha tilgangsstyring, logging og etterfølgende kontroll for å hindre urettmessig tilgang til journaler. Antallet oppslag i journal er så stort at manuelle rutiner for etterfølgende kontroll i helseforetaket er krevende. Statistisk logganalyse vil identifisere uvanlige oppslag som kan følges opp manuelt.

[1] Undersøkelse av helseopplysninger i elektroniske pasientjournaler i fire helseforetak (riksrevisjonen.no)

Status: Prosjektet er satt på pause ut 2023, blant annet grunnet utfordringer med å etablere drift av løsningen.

Flere helseforetak i foretaksgruppen har publisert helseopplysninger i offentlig postjournal, selv om det er flere ledd med manuelle kontroller for å forhindre at dette skjer.

Innføre automatisert kvalitetskontroll i offentlig journal
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Systemstøtte for å oppdage helse- og personopplysninger i dokumentene som skal publiseres i offentlig postjournal.
Status: Pågår.

3.6 Kontinuerlig forbedring

Kontinuerlig forbedring er en viktig del av arbeidet med informasjonssikkerhet.

I risikovurderingene fremkommer det mange forslag til tiltak, hvor noen besluttes gjennomført. Oversikten over status på tiltak er vanskelig tilgjengelig, og det pågår derfor et arbeid i Sykehuspartner HF med bedre oversikt over status på identifiserte tiltak.

Oversikt over tiltak fra risikovurderinger
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2023
Beskrivelse: Forbedret oversikt over tiltak som er identifisert i risiko- og sårbarhetsvurderinger.
Status: Pågår

I foretaksmøtet 17. januar 2023 ble det gitt oppdrag om å gjennomgå beredskapsplanverket.

Gjennomgå beredskapsplanverk innen ikt
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen

Tidsperiode: 2023
Beskrivelse: Gjennomgå eget beredskapsplanverk og vurdere behovet for å iverksette ytterligere forebyggende tiltak og tiltak for å håndtere og gjenopprette funksjon etter tilsiktede eller utilsiktede hendelser mot egen infrastruktur, ikt-systemer og viktige verdier.
Status: Pågår