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.

Regional handlingsplan for arbeidet med informasjonssikkerhet oppdateres innen 1. mai hvert år, i henhold til krav i foretaksmøtet den 17. januar 2023.

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 1. april 2024 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.

Forbedret risikostyring
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2024

Beskrivelse: Tilpasse prosesser for beslutning om aksept av risiko, slik at helhetlige beslutninger kan tas i ledelseslinjene.
Status: Sykehuspartner har tilpasset egne prosesser: • NO-52 veileder til NO-05 – Kriterier for vurdering og aksept av risiko, • NO-53 Informasjonsklassifisering og verdimodell, og • NO-54 ROS-prosess informasjonssikkerhet. Helseforetakene ble orientert om prosessen i juni 2023. Bruk av prosessene er nå under operasjonalisering, inkludert kursing av risikoeiere og ledere for å styrke kompetansen i linjen.

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: 2024
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, med frist innen utgangen av 2023. Noen helseforetak har kvittert ut i årlig melding at de har oversikt over sine viktigste verdier, mens andre har skrevet at dette først vil fullføres i 2024.

For å kunne ha oversikt, rapportering og oppfølging 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: 2024
Beskrivelse: Etablere nasjonalt begrenset nett (NBN) (tekst og tale) i underliggende helseforetak og utpekte virksomheter i spesialisthelsetjenesten i samarbeid med Norsk helsenett SF.

Status: For Helse Sør-Øst, inkludert Pasientreiser HF og Helsetjenestenes driftsorganisasjon HF, er alle helseforetak, unntatt Sunnaas sykehus HF og Sykehusapotekene HF, tilkoblet NBN. Sunnaas sykehus HF og Sykehusapotekene HF vil kobles på i løpet av 2024.

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

Forebyggende sikkerhetstiltak for å beskytte skjermingsverdige verdier
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2024
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. Arbeidet går i henhold til Sykehuspartner HFs plan. Arbeidet fortsetter i 2024.

I tiden fremover er det forventet å bli mer krevende å skille ekte og falsk informasjon. Kunstig intelligens har gjort det enklere for en trusselaktør å lage troverdige nettsteder med feilinformasjon. Nasjonalt systemeierforum for Felles nettløsning i spesialisthelsetjenesten (FNSP) har behandlet felles nasjonale prinsipper for nettsteder i spesialisthelsetjenesten i Norge, etter initiativ fra helseforetak i hele landet. Et bærende prinsipp er å samle foretakets kommunikasjon på det offisielle nettstedet. Da blir det enklere for brukerne å bekrefte ektheten av informasjonen.

Kartlegge nettsteder og samle innhold på helseforetakenes offisielle nettside
Ansvarlig: Helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2025
Beskrivelse: Helseforetaket, med underliggende virksomheter, skal som hovedregel ha nettstedene sine på Felles nettløsning for spesialisthelsetjenesten (FNSP). Det vil sikre deling av innhold nasjonalt, krav til personvern, universell utforming og informasjonssikkerhet. Helseforetaket skal kartlegge og vurdere risikoen ved nettsteder som har andre publiseringsløsninger enn FNSP. Dersom det er nettsteder som inneholder informasjon til pasienter og pårørende, skal disse flyttes til FNSP. Helseforetaket skal også prioritere å flytte nettsteder med innhold som kan styrke spesialisthelsetjenestens og helseforetakets posisjon som attraktiv arbeidsgiver og som ledende aktør innen helseforskning, utdanning og opplæring av helsepersonell. Eventuelle unntak skal avklares med lokal kommunikasjonsdirektør.
Status: Gitt som oppdrag til helseforetakene i 2024.

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 ha oppmerksomhet om 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 og virksomhetsstyring. På denne måten integreres det som en del av kulturen i helsetjenesten.

Kjennskap til ansattes kunnskap, erfaring, atferd og holdninger er viktig for å kunne identifisere gode/egnede tiltak for å håndtere informasjonssikkerhetsrisikoer; slike tiltak kan eksempelvis handle om forbedret opplæring eller bedre tilrettelagte tekniske løsninger. Den digitale sikkerhets-kulturen har vært kartlagt årlig siden 2021.

Måling av informasjonssikkerhetskultur
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: Årlig
Beskrivelse: Måling av informasjonssikkerhetskultur for 2024 som kan benyttes i helseforetakenes kulturarbeid.
Status: Pågår

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: 2024
Beskrivelse: Utarbeidelse av digitalt opplæringsmateriell for å styrke den ansattes digitale kompetanse, inkludert kompetanse innen informasjonssikkerhet og personvern.
Status: Pågår

Oppdatert kunnskap om trusselbildet fremmes gjennom en felles årlig rapport som utarbeides av helseregionene i samarbeid med Norsk helsenett SF. En rapport med beskrivelse av trusselbildet har vært utarbeidet årlig siden 2021.

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: Trusselrapport for 2024 er under arbeid.

3.4 Informasjonssikkerhet i anskaffelser

I interregionale anskaffelser bidrar Sykehuspartner HF med fagkompetanse innen informasjons-sikkerhet.

Informasjonssikkerhet i produkter og tjenester som anskaffes krever også forvaltning etter anskaffelsen er ferdig. Det kan for eksempel være medisinsk-teknisk utstyr eller behandlings-hjelpemidler 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: 2021–2024
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 oppmerksomhet om 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: 2024
Beskrivelse: Helseforetakene har i styresak 107-2019 blitt bedt om å bidra aktivt til sanering av applikasjoner.
Status: Mange applikasjoner er sanert, og det pågår fortsatt 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 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.

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

Statistisk logganalyse
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: 2025.
Beskrivelse: Det er et krav om å ha tilgangsstyring, logging og etterfølgende kontroll for å hindre urettmessig tilgang til journaler. Statistisk logganalyse vil identifisere uvanlige oppslag som kan følges opp manuelt.
Status: Porteføljestyret besluttet 15. februar å utvikle en egen løsning ved bruk av regional data- og analyseplattform (RDAP).

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: 2024
Beskrivelse: Forbedret oversikt over tiltak som er identifisert i risiko- og sårbarhetsvurderinger.
Status: Sykehuspartner HF har pilotert et verktøy, men det viste seg ikke å fungere godt for alle områder. Det arbeides videre med å forbedre prosessen, slik at alle tiltak fanges opp uavhengig av størrelse og kompleksitet i risiko- og sårbarhetsvurderingen.