HELSE SØR-ØST

Regional handlingsplan for arbeidet med informasjonssikkerhet

Versjon	**Dato**	**Behandling/endring**	**Godkjent av**
0.99	12.9.2021		Jan Frich

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 i Helse Sør-Øst RHF den 14. januar 2021 ble det regionale helseforetaket gitt i oppdrag å: «*utvikle en regional handlingsplan for arbeidet med informasjonssikkerhet som også omfatter langsiktige tiltak. Planen presenteres på felles tertialoppfølgingsmøte i oktober 2021*».

Denne handlingsplanen omfatter tiltak basert på mål og strategi for informasjonssikkerhet i Helse Sør-Øst[1], 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 den gjenværende risikoen etter at tiltak er iverksatt. Disse tiltakene inngår i de ulike risikovurderingene og er ikke tatt med i handlingsplanen.

Riksrevisjonen har gjennomført en undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer[2]. Undersøkelsen ble offentliggjort i 2020. Tiltak for å følge opp Riksrevisjonens undersøkelse ble behandlet i styret i Helse Sør-Øst RHF den 4. februar 2021 (styresak 10-2021). Forbedringsområdene detaljeres ytterligere i denne handlingsplanen.

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. september 2021 er beskrevet for hvert tiltak.

3.1 Roller og ansvar

Både eForvaltningsforskriften og Nasjonal sikkerhetsmyndighet anbefaler informasjonssikkerhet som en integrert del av ordinær virksomhetsstyring. I mål og strategi for informasjonssikkerhet i Helse Sør-Øst stilles det krav om at ledelsessystemet for informasjonssikkerhet skal være en del av interkontrollen for helhetlig risikostyring i helseforetakene.

[1] https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

[2] https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/

Informasjonssikkerhet som del av ordinær virksomhetsstyring
Ansvarlig: Helseforetakene
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2022
Beskrivelse: Informasjonssikkerhet skal bli en mer integrert del av den ordinære virksomhetsstyringen der beslutninger om risiko tas i de ordinære ledelseslinjene. Mål og strategi for informasjonssikkerhet i Helse Sør-Øst stiller krav om at kriterier for å akseptere risiko utarbeides og tas i bruk i arbeidet med vurdering av og beslutning om risiko.
Status: Et utkast til kriterier for å vurdere og akseptere risiko er utarbeidet av regionalt sikkerhetsfaglig råd, bestående av alle informasjonssikkerhetslederne i regionen. Utkastet er behandlet av de administrerende direktørene vel helseforetakene, som ga sin tilslutning til å prøve ut kriteriene i en pilotperiode.

Svakheter ved ansvar og roller tilknyttet medisinsk-teknisk utstyr har vært påpekt av Riksrevisjonen i 2015 i undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr[3].

Samhandling for medisinsk-teknisk utstyr
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2021
Beskrivelse: For medisinsk-teknisk utstyr (MTU) skal ansvarsforholdet mellom leverandør, helseforetak og IKT-leverandør være avklart.
Status: En modell for samhandling som avklarer ansvarsforhold er presentert for de administrerende direktører i helseforetakene som har gitt sin tilslutning til modellen.

Riksrevisjonens undersøkelse om IKT-angrep har påpekt at roller og ansvar bør tydeliggjøres.

Revidere beskrivelser av ansvar og roller
Ansvarlig: Helse Sør-Øst RHF og helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2021–2022
Beskrivelse: I ledelsessystemet for informasjonssikkerhet skal beskrivelsene av ansvar og roller revideres.

[3] https://riksrevisjonen.no/rapporter-mappe/no-2015-2016/undersokelse-av-helseforetakenes-ivaretakelse-av-informasjonssikkerhet-i-medisinsk-teknisk-utstyr/

Status: Det er gjennomført innledende møter i regionalt sikkerhetsfaglig råd. Arbeidet med å revidere beskrivelser av ansvar og roller er startet opp høsten 2021.

3.2 Oversikt, rapportering og oppfølging

Helse Sør-Øst RHF har «risiko forbundet med informasjonssikkerhet og personvern» som et eget område i risikorapporteringen til styret.

Helse Sør-Øst RHF har i løpet av høsten 2020 etablert en tettere oppfølging av Sykehuspartner HF innen informasjonssikkerhet.

Riksrevisjonens undersøkelse om IKT-angrep påpeker at ledelsen i helseforetakene og det regionale helseforetaket ikke har tilstrekkelig beslutningsunderlag innen informasjonssikkerhet.

Rapportering av risiko, tilstand og avvik innen informasjonssikkerhet
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: 2021
Beskrivelse: Den ordinære rapporteringen om informasjonssikkerhet fra helseforetakene, og spesielt fra Sykehuspartner HF, skal styrkes, slik at Helse Sør-Øst RHF og styret får bedre styringsinformasjon innen informasjonssikkerhet og bedre innsikt i risikobildet.
Status: Helseforetakene har i oppdrags- og bestillingsdokumenter fått i oppdrag å rapportere risiko, tilstand, avvik og hendelser innen informasjonssikkerhet. Rapporteringen skal gjøres i ordinær tertialrapportering. Rapportering fra første tertial er mottatt. Helseforetakene beskriver sårbarheter og deres potensiale for alvorlige konsekvenser, mens risikoen knyttet til sårbarhetene omtales i mindre grad. Flere foretak melder om prosesser for å få bedre oversikt over risikobildet.

Trusselvurderinger er en viktig del av beslutningsunderlaget innen informasjonssikkerhet. Bruk av trusselvurderinger er et oppdrag Helse Sør-Øst RHF har mottatt i foretaksmøtet 14. januar 2021.

Utarbeide og benytte trusselvurderinger
Ansvarlig: Sykehuspartner HF og øvrige helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2021
Beskrivelse: Sykehuspartner HF skal utarbeide årlige trusselvurderinger i samarbeid med relevante aktører fra både privat og offentlig sektor. Helseforetakene skal benytte denne og andre kilder i sitt arbeid med informasjonssikkerhet.
Status: Sykehuspartner HF har sammen med Helse Nord IKT utarbeidet en trusselvurdering. Trusselvurderingen har blitt oversendt til og presentert for helseforetakene.

3.3 Informasjonssikkerhetskultur og –kompetanse

Riksrevisjonens undersøkelse om IKT-angrep påpeker noen svakheter i informasjonssikkerhets-kulturen i foretaksgruppen.

Måling av informasjonssikkerhetskultur
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2021–2022
Beskrivelse: Informasjonssikkerhetskulturen i foretaksgruppen skal måles og eventuelle tiltak iverksettes med bakgrunn i målingen. Målingene utføres av Sykehuspartner HF. Det er helseforetakene som er ansvarlig for informasjonssikkerhetskulturen i eget helseforetak.
Status: Arbeid med måling av informasjonssikkerhetskultur er startet opp. Det vil sendes spørsmål til et utvalg ansatte i foretaksgruppen. Resultatet av undersøkelsen er planlagt presentert i oktober 2021, som internasjonalt er en måned for økt oppmerksomhet om informasjonssikkerhet.

Helse- og omsorgsdepartementet har i foretaksmøtet 14. januar 2021 bedt om mer samarbeid og erfaringsutveksling mellom helseregionene, Direktoratet for e-helse og Norsk helsenett SF.

Etablere samarbeidsforum
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Spesialisthelsetjenesten
Tidsperiode: 2021
Beskrivelse: Det skal etableres et samarbeidsforum for å dele erfaringer mellom helseregionene, Direktoratet for e-helse og Norsk helsenett SF.
Status: Det er satt opp tre møter for 2021. De to første møtene er gjennomført.

3.4 Informasjonssikkerhet i anskaffelser

Riksrevisjonens undersøkelse om IKT-angrep peker på at det i anskaffelser kan være manglende kompetanse innen informasjonssikkerhet. Medisinsk-teknisk utstyr er i større grad enn tidligere tilkoblet nettverk. Det er utfordringer med utstyr som i seg selv ikke har tilstrekkelig sikkerhet. Det er også utfordringer med utstyr som ikke støtter moderne sikkerhetsmekanismer i nettverket, slik at sikkerheten i hele nettverket må reduseres for at utstyret skal kunne benyttes.

Informasjonssikkerhetskompetanse i anskaffelser
Ansvarlig: De regionale helseforetakene
Relevant for: Spesialisthelsetjenesten

Tidsperiode: 2019–2021
Beskrivelse: For bedre kravstilling og vurdering av informasjonssikkerhet i anskaffelser, skal Sykehusinnkjøp HF benytte kapasitet og kompetanse innen informasjonssikkerhet fra helse-regionenes IKT-leverandører.
Status: De administrerende direktørene i de regionale helseforetakene har besluttet at behovet for informasjonssikkerhet i anskaffelser skal dekkes ved å benytte regionenes informasjons-sikkerhetsmiljøer og at Sykehusinnkjøp HF ikke skal bygge opp et eget miljø innen informasjonssikkerhet. Det pågår et arbeid, ledet av regionenes IKT-direktører, med å detaljere hvordan informasjonssikkerhetsmiljøene skal involveres, og hvordan deltakelsen skal fordeles mellom regionene.

Informasjonssikkerhet i produkter og tjenester som anskaffes krever også forvaltning etter anskaf-felsen 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: 2021–2022
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

Riksrevisjonens undersøkelse om IKT-angrep påpeker at helseforetakene i liten grad reviderer sine IKT-leverandører.

Revisjon av Sykehuspartner HF
Ansvarlig: Konsernrevisjonen
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2022
Beskrivelse: Sykehuspartner HF, som regionens IKT-leverandør, vil revideres av konsernrevisjonen. Innretning og omfang avstemmes i samråd med Regionalt sikkerhetsfaglig råd.
Status: Innledende møter og planlegging av revisjonen er igangsatt.

Riksrevisjonens undersøkelse om IKT-angrep påpekte flere tekniske svakheter i infrastrukturen. Noen områder som ble trukket frem var svakheter med kontroll over nettverket og svakheter i hvordan ansatte logger på ulike systemer.

Tekniske sikkerhetstiltak i infrastrukturen
Ansvarlig: Sykehuspartner HF
Relevant for: Foretaksgruppen
Tidsperiode: 2018–2022
Beskrivelse: Infrastrukturmodernisering er et pågående og kontinuerlig arbeid. En viktig del av moderniseringen handler om å redusere kompleksitet i IKT-porteføljen og få mindre teknisk gjeld. Styrket kontroll med nettverk og styrket autentisering er to sentrale områder.
Status: Modernisering av infrastrukturen har vært prioritert siden 2018, og vil fortsatt ha høy prioritet fremover. Styrket kontroll med nettverk vil ferdigstilles i 2021. For Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer er 43 av 47 identifiserte tekniske tiltak gjennomført per 31. juli 2021.

Helse- og omsorgsdepartementet har i foretaksmøter bedt de regionale helseforetakene om å innføre Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Grunnprinsippene dekker flere av de tekniske funnene i Riksrevisjonens undersøkelse om IKT-angrep. Det systematisk arbeidet med informasjonssikkerhet i Helse Sør-Øst er basert på ISO 27001, en internasjonal standard for ledelsessystemer for informasjonssikkerhet. Dette er i henhold til krav og anbefalinger i eForvaltningsforskriften. ISO 27001 har et tillegg med mulige tiltak. Helse Sør-Øst benytter disse og flere andre kilder for valg av tiltak. Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet har god dekning av sikkerhetsområdet og benyttes som en sentral kilde til tiltak.

Grunnprinsipper for IKT-sikkerhet
Ansvarlig: Helseforetak
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2021
Beskrivelse: Helseforetakene skal arbeide med systematisk innføring av Nasjonal sikkerhets-myndighets grunnprinsipper for IKT-sikkerhet.
Status: Helseforetakene har i oppdrags- og bestillingsdokument for 2021 fått i oppdrag å videreføre arbeidet med Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Arbeid med innføring av grunnprinsippene pågår.

Riksrevisjonen har gjennomført en undersøkelse av styring og kontroll av tilgang i elektroniske pasientjournaler i fire helseforetak[4]. Undersøkelsen ble offentliggjort i 2014. Funn i Riksrevisjonens

[4] https://riksrevisjonen.no/rapporter-mappe/no-2014-2015/undersokelse-av-helseopplysninger-i-elektroniske-pasientjournaler-i-fire-helseforetak/

undersøkelse er i all hovedsak håndtert i Helse Sør-Øst. Det gjenstår to forbedringspunkter hvor det ene handler om 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: Spesialisthelsetjenesten
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.
Status: Leverandør av løsning er valgt og plan for innføring i Helse Sør-Øst er utarbeidet.

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: 2020–2022
Beskrivelse: Systemstøtte for å oppdage helse- og personopplysninger i dokumentene som skal publiseres i offentlig postjournal.
Status: Det er gjennomført flere arbeidsmøter med ekstern leverandør, Sykehuspartner HF, Oslo universitetssykehus HF, Vestre Viken HF og Helse Sør-Øst RHF.

3.6 Kontinuerlig forbedring

Trusselbildet er i endring. Digitale løsninger videreutvikles. Nye sårbarheter oppdages jevnlig. Arbeidet med informasjonssikkerhet er derfor et kontinuerlig arbeid.

Videreutvikling av ledelsessystemet for informasjonssikkerhet
Ansvarlig: Helseforetakene
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2022
Beskrivelse: Flere av tiltakene i denne handlingsplanen krever endringer som må reflekteres i ledelsessystemet for informasjonssikkerhet.
Status: Sommeren 2020 ble arbeidet med videreutvikling av ledelsessystemet for informasjonssikkerhet styrket.

Kjennskap til avvik er et viktig underlag i beslutninger som skal hindre at samme feil oppstår mange ganger. Riksrevisjonen har påpekt at det rapporteres få avvik innen informasjonssikkerhet. Avviksystemet er én kilde til kjennskap om avvik. Andre kilder kan være spørreundersøkelser, dybdeintervjuer med mer.

Avvik innen informasjonssikkerhet
Ansvarlig: Helse Sør-Øst RHF
Relevant for: Foretaksgruppen
Tidsperiode: 2020–2021
Beskrivelse: Avvik innen informasjonssikkerhet må identifiseres og følges opp som grunnlag for systematisk forbedring.
Status: Helse Sør-Øst RHF har bedt om at helseforetakene rapporterer overordnet om avvik innen informasjonssikkerhet i den ordinære rapporteringen. Rapporteringen er startet. Et helseforetak har rapportert om et alvorlig brudd på personvernet for en pasient. Det er også rapportert om flere sikkerhetsbrudd som har gitt moderate[5] konsekvenser for pasientbehandlingen.

[5] Iht. Norsk kodeverk for uønskede pasienthendelser (NOKUP)