Mål og strategi for informasjonssikkerhet i Helse Sør-Øst – overordnet styrende dokument

Versjonsnummer	Dato	Behandling/endring	Godkjent av
1.0	11.03.21	Fremlegg for styret	Adm.dir. Cathrine M. Lofthus
1.1	22.04.21	Styrebehandling	

1 Omfang

Informasjonsbehandling er en vesentlig del av det å yte gode helsetjenester. Informasjonssikkerhet handler om å sikre informasjonsbehandlingen og inngår i større eller mindre grad i alle systemer og alle ansattes arbeid. Informasjonssikkerhet handler om å kunne levere helsetjenester selv om flom, brann eller digital angrep påvirker IKT-systemene, det handler om å hindre avansert datainnbrudd, om en kultur der ansatte behandler opplysninger fortrolig, om at digitale støttesystemer gjengir opplysninger uforandret, og ikke minst handler informasjonssikkerhet om at opplysninger om pasienter skal være tilgjengelig for helsepersonell når de trenger dem.

Dette dokumentet gjelder for all informasjonsbehandling i Helse Sør-Øst, både manuell og maskinell, analog og digital, lagret og kommunisert. Dokumentet gir rammer og retning for arbeid med informasjonssikkerhet i Helse Sør-Øst. I underliggende dokumenter vil rammene bli konkretisert, blant annet med hensyn til ansvar, organisering og prosesser for informasjonssikkerhetsarbeidet.

2 Formålet med informasjonsbehandlingen

Foretaksgruppens visjon er gode og likeverdige helsetjenester til alle som trenger det, når de trenger det. Informasjonsbehandlingen skal understøtte helseforetakenes oppgaver og tjenester innen pasientbehandling, forskning, undervisning og pasient- og pårørendeopplæring, slik at helseforetakenes mål nås.

Informasjonsbehandlingen skal legge til rette for gode og sammenhengende pasientforløp, også på tvers av helseforetak og omsorgsnivåer. Informasjonsbehandlingen omfatter også kommunikasjon med pasienter, brukere og pårørende, blant annet for at pasienter skal kunne medvirke i egen behandling.

3 Mål for informasjonssikkerhet

Det overordnede målet for informasjonssikkerheten er at:

- Informasjon er tilgjengelig ved behov (tilgjengelighet)
- Informasjon ikke endres utilsiktet eller av uvedkommende (integritet)
- Informasjon ikke blir kjent for uvedkommende (konfidensialitet)

For å oppnå dette må informasjonssystemene være både motstandsdyktige mot trusler og innrettet slik at funksjonaliteten raskt kan gjenopprettes etter svikt.

Behandlingen av informasjon må være i samsvar med lover, regler og avtaler, slik at informasjonsbehandlingen på en formåls- og kostnadseffektiv måte bidrar til realisering av helseforetakenes samlede mål. Sentralt regelverk er blant annet helselovgivningen, sikkerhetsloven og personopplysningsloven. Helseberedskap er regnet som en av de grunnleggende nasjonale funksjoner.

Ved målkonflikter skal det legges stor vekt på å ivareta helseberedskap og pasientsikkerhet.

4 Strategi for informasjonssikkerhet

Alle helseforetak i regionen skal ha et relevant og oppdatert ledelsessystem for informasjonssikkerhet basert på anerkjente standarder. Helseforetakene skal benytte Helse Sør-Øst RHFs styringsdokumenter supplert med foretaksinterne dokumenter, slik at det overordnet er en samlet og lik håndtering av informasjonssikkerhet i regionen. Helseforetakene skal tilstrebe harmonisering med likelydende dokumenter, men skal også kunne utarbeide egne dokumenter basert på lokale organisatoriske forhold, eksisterende infrastruktur og tekniske muligheter og begrensninger.

Ledelsessystemet for informasjonssikkerhet skal være en del av internkontrollen for helhetlig risikostyring i helseforetakene. I dette ligger krav om:

- At ledelsen kommuniserer krav til informasjonssikkerhet i styrende dokumenter, og at krav og føringer kommuniseres tydelig til ansatte og ledere på ulike nivåer
- At lederlinjen er ansvarlig for systematisk bruk av risikovurderinger
- Klart definert ansvar og krav om tilstrekkelig kompetanse innen informasjonssikkerhet, både i linjen og i fagmiljøene som skal gi råd til linjen
- Tilstrekkelige tiltak for å beskytte informasjon og informasjonssystemer, samt for å håndtere uønskede hendelser
- At tiltak evalueres med hensyn på at det er forholdsmessighet mellom tiltakets risikoreduserende effekt, nytte, kostnader og ulemper
- Kontinuerlig forbedringsarbeid og systematisk oppfølging av avvik
- Evaluering, revisjoner og jevnlig gjennomgang av om ledelsessystemet fungerer som tilsiktet

Informasjonssikkerhetsarbeidet skal være risikobasert.

- Helseforetakene skal ha god oversikt over de høyeste risikoene
- Ressursinnsatsen skal tilpasses risiko, der høy risiko vurderes grundigere enn lav risiko
- Risikoreduserende tiltak skal velges basert på risikovurderinger, vesentlighet, kost-nytte-vurderinger og ledelsens føringer for risikohåndtering, samt et effektivt sikkerhetsarbeid

Ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret.

- Risikostyring innen informasjonssikkerhet følger den ordinære risikostyringen i helseforetakene
- Helseforetakene skal utforme akseptkriterier slik at avgjørelser om aksept av risiko kan tas på riktig ledernivå med et tilstrekkelig beslutningsgrunnlag
- Det skal i akseptkriteriene blant annet tas hensyn til risikoens størrelse og hvordan risikoen vurderes i andre helseforetak
- Måloppnåelse innen informasjonssikkerhet og effekt av tiltak skal måles og rapporteres, slik at hvert helseforetak og Helse Sør-Øst RHF kan vurdere måloppnåelse på ulike nivå
- Helse Sør-Øst RHF kan gi føringer for ivaretakelsen av informasjonssikkerhet i regionen. Helseforetakene skal forelegge avvik fra regionale føringer innen informasjonssikkerhet for eget styre
- Dersom to helseforetak ikke kommer til enighet om hvorvidt en risiko kan aksepteres, skal saken drøftes med Helse Sør-Øst RHF

Helseforetakene skal samarbeide for å effektivisere og styrke informasjonssikkerhetsarbeidet på tvers og for å ivareta likeverdige tjenestetilbud. Dette skal skje gjennom samarbeidsforum, informasjonsutveksling og ved å utnytte felles løsninger.

- Analyser og tiltak for informasjonssikkerhet skal koordineres mellom helseforetakene i Helse Sør-Øst og gjennom bruk av felles databehandler, slik at synergier kan utnyttes og tiltak ikke kommer i konflikt med hverandre
- Resultat av analyser skal kommuniseres til berørte helseforetak i regionen

Opplæring og arbeid med informasjonssikkerhetskultur vil være et viktig område for å etterleve krav i mål og strategi for informasjonssikkerhet. Dette vil konkretiseres i underliggende dokumenter.