Ansvar for informasjonssikkerhet - En reise for ledere

Øyvind Grinde, Normkonferansen, 22. november 2023

HELSE SØR-ØST

HELSE SØR-ØST

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

HELSE SØR-ØST

Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	26. oktober 2023

Sak 123-2023

Status for arbeidet med informasjonssikkerhet

Forslag til vedtak:

1. Styret tar status for arbeidet med informasjonssikkerhet til orientering.
2. Styret ber om å holdes orientert om arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst.

Hamar, 19. oktober 2023

Terje Rootwelt
administrerende direktør

HELSE SØR-ØST

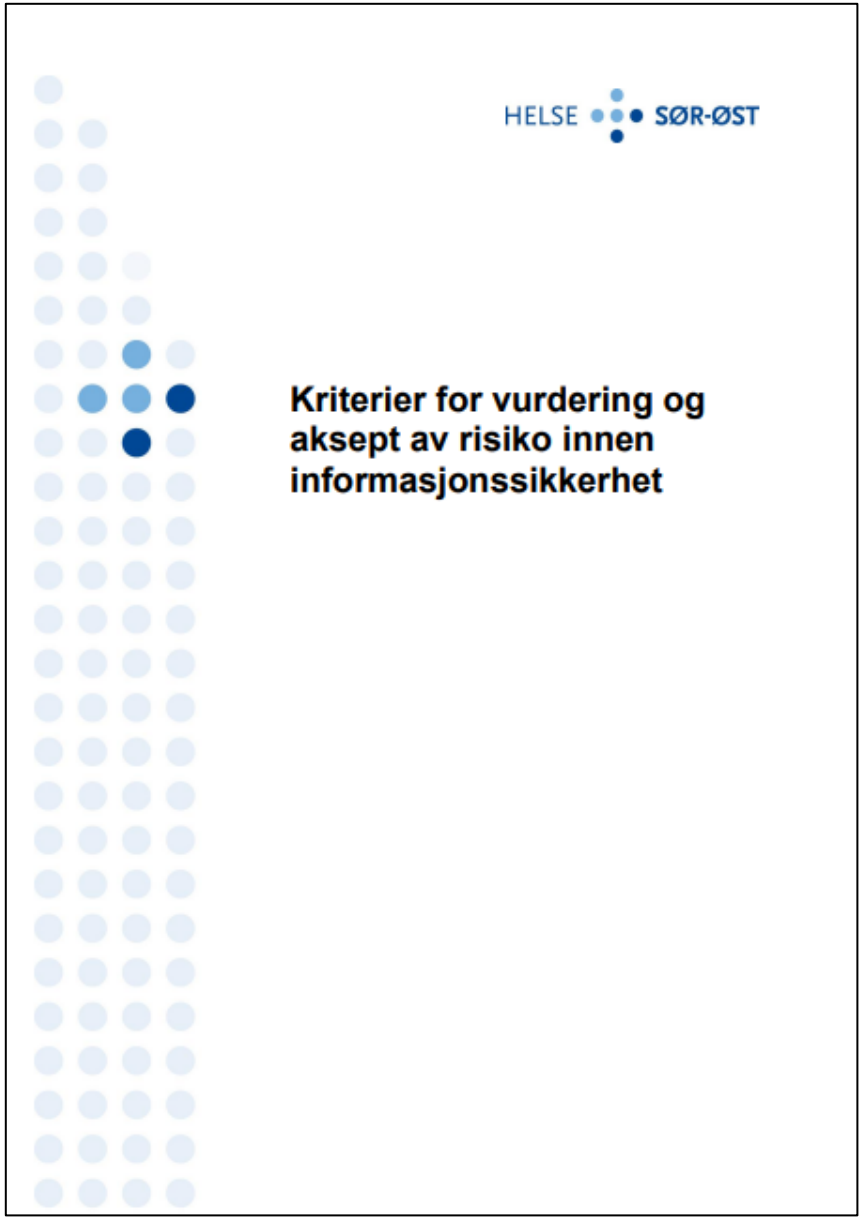
Regional handlingsplan for arbeidet med informasjonssikkerhet

SYKEHUSPARTNER CERT

Hvor var vi?

Ledelses-systemet på nett 2019	• Virksomhetens administrerende direktør har besluttet å delegere myndighet for informasjons-sikkerhet til virksomhetens informasjonssikkerhetsleder • Informasjonssikkerhetsleder [skal] vurdere og avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå på vegne av administrerende direktør
Mørketalls-undersøkelsen 2020	• NSM har over flere år observert en klar sammenheng mellom sikkerhetsengasjerte ledere og sikkerhetstilstanden i virksomheten. Der ledelsen er fraværende i sikkerhetsspørsmål, blir avstanden til sikkerhetsarbeidet fort stor, og det blir vanskeligere å få besluttet, gjennomført og evaluert relevante tiltak. • NSM erfarer at de mest alvorlige avvikene ved tilsyn gjerne forekommer i virksomheter hvor sikkerhet behandles som et fagområde som er litt på siden av virksomhetens fokus og av en adskilt gruppe mennesker.
Riksrevisjonen 2020	• Ledelsen i både de regionale helseforetakene og underliggende foretakene har mangelfull informasjon om reell sikkerhetstilstand og sikkerhetsrisiko.
Helsetilsynet rapport 7/2021	• Understreke viktigheten av at tjenestene gjennomfører ROS-vurderinger knyttet til bruk av IKT i tjenesteytingen, som balanserer kravene til forsvarlig helsehjelp, brukervennlighet, pasientsikkerhet, personvern og informasjonssikkerhet.

Hvor skal vi?
- Ledere med et helhetlig ansvar



- Beslutninger om hvorvidt en risiko er akseptabel, skal tas av risikoeier.
- Aksept av høyere risiko krever beslutning på høyere ledelsesnivå.
- Der foreløpige analyser tyder på høy risiko skal både risikovurderingene og vurdering av mulig risikohåndtering gjøres grundigere enn ved lav risiko.
- Dersom helseforetaket er kjent med hvordan risikoen er vurdert i andre foretak, skal vurderingen hensyntas i akseptvurderingen.

Helhetlig ansvar inkludert informasjonssikkerhet og personvern

Mål og strategi for informasjons-sikkerhet	• Ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret • Ved målkonflikter skal det legges stor vekt på å ivareta helseberedskap og pasientsikkerhet • Helseforetakene skal ha god oversikt over de høyeste risikoene
Organisering av personvern- og informasjons-sikkerhets-arbeidet	• Sørge for at arbeidet med personvern og informasjonssikkerhet er risikobasert og at det er en integrert del av virksomhetens risikostyring. Helseforetaket skal ha tilstrekkelig oversikt over risikoer ved informasjonsbehandlingen, samt personvern- og sikkerhetstilstanden. • Leder er risikoeier for måloppnåelsen innen sitt ansvarsområde i samsvar med fastsatte rammer […] Leder skal sørge for at det daglige informasjonssikkerhetsarbeidet følges opp innen sitt ansvarsområde.

Hvor er vi?

- HOD har etablert en hensiktsmessig kravstilling og oppfølging innen informasjonssikkerhet.
- Helse Sør-Øst RHF rapporterer risiko og sikkerhetstilstand regelmessig til styret og eier.
- Helseforetakene rapporterer risiko og sikkerhetstilstand til Helse Sør-Øst RHF.
- Informasjonssikkerhet behandles i mange ledermøtesaker, direktørmøtesaker og styresaker.
- Ledere på ulike nivåer har varierende bevissthet om ansvar for informasjons-sikkerhet og personvern

Tips

- Bruk ledelsens gjennomgang til å legge frem risiko og sikkerhetstilstanden.
- Foreslå bestillinger fra ledelsen i konklusjonen.