Forslag til konsernrevisjon informasjonssikkerhet

HSØ har som ett av sine mål at ny teknologi skal bedre og effektivisere pasientbehandling og understøtte nye typer helsetjenester. Men for å nå dette målet må det sikres modenhet og kompetanse innen informasjonssikkerhet og personvern. Det må derfor kunne bekreftes etterlevelse av lovverk og kartlegge om styrende dokumentasjon finnes/følges innen viktige temaer innen informasjonssikkerhet og personvern;

Tre undertemaer/spørsmål:

1. Hvilke retningslinjer/rutiner har man for systematisk opplæring av ledere/ansatte i informasjonssikkerhet og personvern (eventuelt samordning på tvers i HSØ). Hvordan jobbes det for systematisk oppbygging av sikkerhetskultur.
    a. Et økt risikobilde innen cybersikkerhet og trusselbilde kombinert med økende teknologiutvikling vil stille større krav til ledere når det gjelder informasjonssikkerhet og sikkerhetskultur.
    b. Kartleggingen av sikkerhetskultur gjort av SP i oktober 2021 viste at det fortsatt er en vei å gå når det gjelder sikkerhetskultur innen blant annet systematisk opplæring og ledelsesforankring.
    c. I april 2021 besluttet styret i Helse Sør-Øst RHF at risikostyringen innen informasjonssikkerhetsområdet skal følge ordinær risikostyring, og at det skal fastsettes kriterier for å sikre at aksept av risiko tas på riktig ledernivå med et tilstrekkelig beslutningsgrunnlag. Det derfor viktig at risikoeier har tilstrekkelig kompetanse innen informasjonssikkerhet/personvern og at beslutningsstøtteverktøy er gode nok slik at det kan fattes gode beslutninger.

2. Hvilke rutiner/retningslinjer sørger for tilstrekkelig kompetanse hos systemeier og systemansvarlig (HF) og samarbeid med tjenesteansvarlig (SP), herunder aksept og forståelse av risiko
    a. Økning av antall systemer og kontinuerlig endring gjør at kommunikasjonen mellom systemeier og systemansvarlig bør være tettere enn hva den er i deg. Hvilke krav stilles det?

3. Rutiner for opplæring og etterlevelse av HSØ sikkerhetsinstruks
    a. Sikkerhetsinstruksen et dokument som gjelder for alle helseforetak og som underbygger/forankrer mange av de grunnleggende prinsippene innen god informasjonssikkerhet og personvern.
    b. Hvordan sikres det at innholdet i dokumentet er ivaretatt og implementert?

4. Gjennomføres/utføres risikoreduserende tiltak i helseforetakene som anbefalt i ROSer?
    a. Etter at en ROS anbefales av informasjonssikkerhetsleder eller regionalt sikkerhetsfaglig råd (RSV), skal tjenesteansvarlig (SP) og/eller systemansvarlig/systemeier (HF) sikre for at anbefalte tiltak iverksettes. Hvordan sikres det at tiltak gjennomføres/etterleves?

Informasjonssikkerhetsleder Tina Nyhus
SunHF August 2022