SYKEHUSET ØSTFOLD

**STYREMØTE 22. mars 2021**



| | | | |
|---|---|---|---|
| Styresak nr.: | 21-21 | Sakstype: | Orienteringssak |
| Saksnr. arkiv: | 21/01997 | | |

## Ledelsens gjennomgang av informasjonssikkerhet

Sykehuset Østfold HF (SØ) gjennomfører ledelsens gjennomgang av informasjonssikkerhet to ganger i året og dette gir samlet en god oversikt over SØs situasjon på dette området. Det vurderes at SØ har et høyt nivå på tilfredsstillelse av krav innen informasjonssikkerhet og at føringer fra Helse Sør-Øst HF (HSØ) følges.

SØs vurdering av eget informasjonssikkerhetsnivå støttes av Riksrevisjonens rapport om *helseforetakenes forebygging av angrep mot sine IKT-systemer*. Intern oppfølging av denne forvaltningsrevisjonen omtales i denne saken.

Forslag til vedtak:

Styret tar saken til orientering.

Sarpsborg, den 15.03.2021

Hege Gjessing
administrerende direktør

## 1. Administrerende direktørs anbefalinger / konklusjoner

Ledelsens gjennomgang av informasjonssikkerhet gjennomføres to ganger i året og gir samlet en god oversikt over SØs situasjon innen informasjonssikkerhet. Det vurderes at SØ har et høyt nivå på tilfredsstillelse av krav innen informasjonssikkerhet og denne vurderingen støttes av Riksrevisjonens rapport.

Riksrevisjonens rapport fremhever informasjonssikkerhetskulturarbeidet som godt ved SØ. Rapporten trekker også fram ledelsens gjennomgang av informasjonssikkerhet ved SØ som et positivt funn. I etterkant av revisjonen er antallet formelle gjennomganger økt og det gjennomføres også hyppigere gjennomganger av aktuelle problemstillinger.

## 2. Faktabeskrivelse

***Innhold i Ledelsens gjennomgang av informasjonssikkerhet***

- ✓ Internkontroll/styring
- ✓ Regional protokoll
- ✓ Kartlegging av informasjonssikkerhetskultur
- ✓ Forenklet sikkerhetsinstruks for informasjonssikkerhet
- ✓ Smartkort til alle medarbeidere

I tillegg omtales Riksrevisjonens forvaltningsrevisjon av helseforetakenes IKT-systemer i denne saken.

***Hovedbudskap i ledelsens gjennomgang:***

- SØ bør ha større fokus på protokoll over behandlingsaktiviteter av personopplysninger for å oppnå best mulig oversikt.
- En oppdatert protokoll gir et godt utgangspunkt for å ha god oversikt, men den avdekker ikke alle potensielle tekniske sårbarheter i systemer eller feil behandling av personopplysninger.
- SØ har erfart at selv om konsekvensene for de registrerte er relativt liten ved en eventuell feil kan de økonomiske konsekvensene være svært store.
- SØ bør øke bevisstheten rundt systemeieres ansvar for informasjonssikkerhet og personvern.

***Internkontroll/styring***

Internkontroll innebærer å ha oversikt over all behandling av personopplysninger, herunder tilgangskontroll, sårbarheter og oversikt over utlevering.

SØ har etablert et register (*protokoll over behandlingsaktiviteter i personvernforordningen*) over alle personopplysninger som behandles. Dette er en av flere forpliktelser som ble innført da personvernregelverket trådte i kraft i juli 2018. Personopplysninger behandles i SØ blant annet i fagsystemer (DIPS, MV etc.), i medisinsk utstyr, skytjenester, manuelle registre (Excel) og på papir. Begrepet *informasjonssystemer* benyttes som en fellesbetegnelse for disse. Med *personopplysning* menes alle opplysninger som kan identifisere en person, herunder også avidentifiserte personopplysninger som f.eks. NPR-id og rekvisisjonsnummer.

I protokollen er det også inkludert systemer hvor det ikke lagres personopplysninger for å få en helhetsoversikt, ikke minst innen bruk av leverandører. Det føres separat protokoll for forskningsprosjekter.

De tre viktigste rollene i informasjonssikkerhet er:

- Systemeier – har overordnet ansvar for at systemet tilfredsstiller krav til behandling av personopplysninger.
- Systemforvalter – har de daglige oppgavene knyttet til informasjonssikkerhet, opprette/slette brukere og oppdatere protokollen.
- Tjenesteansvarlig – har ansvaret for at systemet fungerer som avtalt. Denne rollen er plassert i Sykehuspartner (SP), eventuelt i MTA (medisinskteknisk avdeling) for medisinsk utstyr.

Rollene er utdypende beskrevet i prosedyren *Informasjonssikkerhet – organisering*.
Systemeier og systemforvalter skal arbeide i den klinikken/avdelingen som bruker systemet, for virksomhetsovergripende systemer ligger disse rollene i *klinisk IKT* eller *IKT-avdelingen*.

Som en del av den løpende internkontrollen har det vært gjennomført en oppdatering og delvis internrevisjon av den overordnede protokollen som SØ ble pålagt å ha etter at GDPR trådte i kraft juli 2018. Protokollen gir en overordnet oversikt over all behandling av personopplysninger i SØ, men protokollen er fortsatt ikke fullstendig og iht. alle kravene som stilles. Oppdateringen som er i gang viser at det er mye gjenstående arbeid.

*Status på gjennomført oppdatering av protokoll*
Det ble før jul 2020 gjennomført en oppdatering og supplering av innholdet i protokollen, herunder:

- systemeier- og systemforvalter
- formål
- kategorier av opplysninger
- databehandler og leverandør
- tilgangsmekanismer og roller

*Sentrale resultater og tiltak*

- Protokollen er ikke oppdatert.
  Det er registrert flere systemer enn vi faktisk har, blant annet fordi det har pågått sanering av systemer parallelt med registreringen i protokollen.
  Tiltak: Det er igangsatt arbeid for å ajourføre innholdet med andre registre, eksempelvis regional protokoll og saneringsprosjektet i SP.
- Enkelte informasjonssystemer er ikke oppdatert.
  Informasjon om det enkelte informasjonssystem må detaljeres for 1/3 av porteføljen.
  Det er behov for en grundigere revisjon av hvert enkelt informasjonssystem for å avdekke sårbarheter.
  Tiltak: Det er nedsatt en intern arbeidsgruppe for utforming av mal og gjennomføring av revisjon.
- Personvernkonsekvensvurdering (DPIA)
  Det er krav om å gjennomføre en personvernkonsekvensvurdering for alle informasjonssystemer med personopplysninger.
  Tiltak: Det er innført rutine for å gjøre dette på nye systemer, men det bør også gjøres på eldre systemer. Behov kartlegges gjennom ovennevnte revisjon.

***Regional protokoll***
SP har i samsvar med oppdrag- og bestillingsdokument 2019 tilgjengeliggjort *Medinsight* som er planlagt brukt som regional protokoll.
Hensikten med en regional protokoll er å ha én felles protokoll for all behandling av personopplysninger. Fordelen er en bedre innsikt på tvers av helseforetak, men viktigere er bedre tilgang til informasjon fra SP.

Den lokale protokollen ivaretar mer enn bare minimumskravene til en protokoll, og er et viktig verktøy i SØs arbeid med internkontroll. Det legges opp til at begge protokollene benyttes med en gjensidig oppdatering av informasjon.

***Kartlegging av informasjonssikkerhetskultur blant ledere***
SP har fått i oppdrag å utarbeide en spørreundersøkelse for å måle informasjons-sikkerhetskulturen på helseforetakene. SØ har gjort dette tidligere og vil bidra i den regionale prosjektgruppen. Prosjektgruppen er ikke formelt i gang, men det forventes at undersøkelsen gjennomføres inneværende år og vil bli gjentatt årlig.

***Forenklet sikkerhetsinstruks for informasjonssikkerhet***
Det er utarbeidet en forenklet versjon av sikkerhetsinstruksen. Hensikten med denne er å få frem hovedbudskapet på en tydeligere måte tilpasset medarbeiderne og kunne fokusere på problemstillinger som fremkommer i kartleggingene av informasjonssikkerhetskulturen. Det pågår et arbeid med revidering av regionalt ledelsessystem for informasjonssikkerhet. Den forenklede utgaven av sikkerhetsinstruks spilles inn som forslag i dette arbeidet. Den forenklede versjonen sendes ut til alle medarbeidere en gang i året for elektronisk signering.

***Smartkort til alle medarbeidere***
Det innføres strengere regionale tiltak for pålogging. Det er innført to-faktor autentisering (TFA) for tilgang fra eksterne nettverk, dvs. hjemmekontor og mobile enheter. Det er også påkrevet TFA for all behandling av personopplysninger over internett, slik som Altinn, helsenorge.no osv.
TFA oppnås i dag i stor grad ved bruk av BankID.

Det er igangsatt utarbeidelse av en nasjonal tillitsmodell som skal regulere samarbeid om personopplysninger mellom offentlig etater i Norge. Denne modellen vil basere kommunikasjon på kravene i eIDAS-forordningen, som krever sertifikatbasert pålogging (TFA).

Prosjekt Styrket autentisering vil legge fram en rapport som beskriver de mulige løsningene for stasjonære og mobile klienter. Det er forventet at prosjektet vil anbefale at all pålogging skal gjøres med TFA.

Det er besluttet at de som daglig benytter TFA kan få utdelt Smartkort som alternativ til BankID.

**Riksrevisjonens forvaltningsrevisjon av helseforetakenes IKT-systemer**
Riksrevisjonen har gjennomført en forvaltningsrevisjon med temaet helseforetakenes forebygging av angrep mot IKT-systemer. Det ble foretatt en dybdeundersøkelse ved SØ, Sykehuset i Vestfold og SP våren 2019. Dybdeundersøkelsen omfattet intervjuer med administrerende direktør, en systemeier, en systemforvalter og noen sluttbrukere. I tillegg ble relevante prosedyrer, retningslinjer og referater gjennomgått samt at det ble gjennomført en omfattende sikkerhetstest.

Det var ingen alvorlige funn ved SØ, men det ble funnet noen svakheter som det ble innført tiltak mot etter revisjonen.

SØ, SP og HSØ ble innkalt til møte i Kontroll- og konstitusjonsutvalget i Stortinget 22. februar for å presentere SØs arbeid relatert til Riksrevisjonen rapport. Administrerende direktørs innledning er gjengitt i vedlegg 1.

### 3. Administrerende direktørs vurdering

Administrerende direktør vurderer at SØ har et høyt nivå på tilfredsstillelse av krav innen informasjonssikkerhet og denne vurderingen støttes av Riksrevisjonens rapport. Ledelsens gjennomgang av informasjonssikkerhet gjennomføres to ganger i året og gir samlet en god oversikt over SØs situasjon innen informasjonssikkerhet.

I Riksrevisjonens rapport anbefales det en mer detaljert gjennomgang av informasjonssikkerheten, og at informasjonssikkerhet i større grad inkluderes i virksomhetens øvrige forvaltningsmodell. HSØ iverksetter nye strategiske tiltak innen informasjonssikkerhet i 2021. Dette inkluderer tiltak for å måle informasjonssikkerhetskulturen og tydeliggjøre roller og ansvar innenfor informasjonssikkerhetsarbeidet. SØ har allerede helt eller delvis innført flere av disse tiltakene.

Foreslåtte tiltak i *Ledelsens gjennomgang av informasjonssikkerhet* i SØ er i tråd med anbefalinger i Riksrevisjonens rapport og kommende føringer fra HSØ.