ENDRINGER FRA FORRIGE VERSJON: Nytt dokument, erstatter tidligere styrende dokument. Vedtatt av FL 13/4/21

KILDE

Basert på HSØ Regionalt ledelsessystem for informasjonssikkerhet, dokument NO-4 v1.1: *«Organisering av informasjonssikkerhetsarbeidet»*. Oppdatert etter personopplysningslov av 20. juli 2018.

HENSIKT

Sikre at utøvende sikkerhetsansvar, -myndighetsforhold og -oppgaver som del av sykehusets styringssystem for informasjonssikkerhet og personvern er organisert i Sørlandet sykehus (SSHF).

MÅLGRUPPE

Alle medarbeidere ved Sørlandet sykehus HF (SSHF).
Alle **ledere** ved SSHF som behandler helse- og personopplysninger innen eget ansvarsområde.
Alle **systemeiere** ved SSHF har ansvaret for ett eller flere IKT- eller fagsystemer, uavhengig av om systemet inneholder helse- og personopplysninger.

ANSVAR

- **Administrerende direktør** er dataansvarlig for all behandling av helse- og personopplysninger i SSHF. Har ansvar for at alle personopplysninger blir behandlet iht. gjeldende lovverk, se spesielt helseregisterloven og personopplysningsloven.
- **Systemeier** har ansvar for å stille krav til tilgjengelighet, konfidensialitet, integritet og kvalitet for det system vedkommende er systemeier for, slik at det oppfyller lovbestemte og andre krav.
- **Systemforvalter** utfører oppgaver på operasjonelt nivå delegert fra systemeier. Gir råd og rapporterer til systemeier.
- **Leder** på alle nivåer har ansvar for å påse at retningslinjer for informasjonssikkerhet og personvern etterleves innen eget ansvarsområde. Har det overordnede ansvar for etterlevelse av Sikkerhetsinstruksen innen eget ansvarsområde.
- **Personvernombudet** har en rolle i å sikre at den enkeltes personvernrettigheter blir ivaretatt, at all utlevering av personopplysninger registreres, gjøres med nødvendig sikkerhet og at utleveringen skjer kun med gyldig grunnlag.
- **Informasjonssikkerhetsleder** har ansvar for å forvalte, rapportere og rådgi behandlingsansvarlig innen informasjonssikkehetsområdet.
- **Medarbeider** har ansvar for å etterleve dette dokument ved tilgang til helse- og personopplysninger

FREMGANGSMÅTE

Generelt

Organisering av informasjonssikkerhets- og personvernarbeidet avklarer nødvendige ansvars- og myndighetsforhold og omfatter utøvende og kontrollerende ansvar og oppgaver. Informasjonsbehandling som skjer med hjemmel i pasientjournalloven, helseregisterloven, helseforskningsloven, personopplysningsloven med flere, er rent linjestyrte aktiviteter, hvor administrerende direktør har ansvaret for informasjonssikkerheten gjennom sin rolle som behandlingsansvarlig. Informasjonssikkerhetsleder, prosjekteiere, systemeiere/tjenesteeiere og andre i egen organisasjon svarer dermed for administrerende direktør i foretaket i samsvar med sin rolle. Bruk

av databehandler endrer ikke foretakets selvstendige ansvar for informasjonssikkerhet. Krav og forventninger til databehandlere, må kommuniseres klart og følges opp for å sikre at sikkerhetsmålsettingene til foretaket oppnås.

Følgende sikkerhetsfunksjoner med definerte ansvarsområder er som minimum etablert:

- Administrerende direktør
- Systemeier
- Systemforvalter (systemansvarlig[1])
- Tjenesteeier
- Tjenesteansvarlig
- Informasjonssikkerhetsleder
- Personvernombud
- Leder
- Medarbeider
- IKT-leverandør/databehandler

Nivå	Dataansvarlig SSHF	Databehandler Sykehuspartner
Nivå 1 – strategisk	Administrerende direktør SSHF	Administrerende direktør SP
Nivå 2 – taktisk	Systemeier	Tjenesteeier
Nivå 3 – operasjonelt	Systemforvalter	Tjenesteansvarlig

Tabell 1: Relasjoner mellom de ulike rollene innen informasjonssikkerhetsarbeidet ift IKT- og fagsystemer

Administrerende direktør

- er behandlingsansvarlig for all behandling av personopplysninger herunder ansvarlig for å bestemme formålet med databehandlingene og ha dokumentert oversikt over disse
- har det overordnede ansvar for informasjonssikkerheten og personvernet, og skal sikre at tjenester er tilgjengelig for å gjennomføre tiltak
- har ansvar for at styringssystemet for informasjonssikkerhet og personvern blir implementert, vedlikeholdt og fulgt opp
- er ansvarlig for organiseringen av sikkerhetsarbeidet
- har ansvar for at det fastsettes akseptabelt risikonivå som minimum tilfredsstiller kravene i styringssystemet for informasjonssikkerhet og personvern
- har ansvaret for at det finnes et definert regime for tilgang til helse- og personopplysninger
- skal sørge for at det inngås skriftlige avtaler med IKT-leverandør/databehandler med krav til sikkerhetsnivå, tjenestenivå og forvaltning

Systemeier

- har ansvar for å stille krav til tilgjengelighet, konfidensialitet, integritet og kvalitet for det IKT- eller fagsystem vedkommende er systemeier for, slik at det oppfyller lovbestemte og andre krav
- har ansvar for å sikre at informasjon som behandles i systemer er relevant og nødvendig for det definerte formålet
- er ansvarlig for at all behandling av personopplysninger utføres iht krav til innebygd personvern og personvern som standardinnstilling

[1] *Begrepet «systemansvarlig» utgår og erstattes av begrepet «systemforvalter». Årsaken er en definisjon fra Digitaliseringsdirektoratet med bakgrunn i at ansvarsbegrepet hører til systemeier-rollen og ikke til den operative rollen dette er. Samme begrepsforståelse er innført ved SØHF, STHF og SiVHF, men ikke i Sykehuspartner (selv om det i noen grad benyttes i dagligtalen).*

- skal vurdere og, i forståelse med informasjonssikkerhetsleder, godkjenne tilganger til systemet i samsvar med de regionale prinsipper for tilgang, samt eventuelt uttrekk av informasjon i forbindelse med forskning, undervisning og kvalitetssikring, internt og eksternt
- er ansvarlig for nødvendige hjemmelsgrunnlag for behandling av personopplysningene
- definerer tilgangsroller for sitt system innenfor rammene gitt av daglig leder og gjør disse kjent
- skal påse at det inngås skriftlige avtaler (databehandleravtale) med IKT-leverandør/databehandler med krav til sikkerhetsnivå, tjenestenivå og forvaltning. Databehandler er ansvarlig for at slik avtale inngås med underleverandører (underleverandørdatabehandleravtale)
- skal sørge for at det blir gitt nødvendig opplæring for å kunne benytte informasjonssystemet på riktig måte
- skal overvåke risiko forbundet med informasjonsbehandling og forestå risikovurdering ved behov
- skal sørge for at DPIA (personvernkonsekvensvurdering) gjennomføres i samsvar med personopplysnings-loven ved ny eller endret behandling av personopplysninger
- skal inngå i endringsstyringsprosessen hos IKT-leverandør/databehandler og beslutte gjennomføring av endringer for sitt system
- skal bistå foretaket i kontinuitetsplanlegging for arbeidsprosesser der systemet inngår
- skal sørge for at systemet dokumenteres i SSHF sin «protokoll over behandlingsaktiviteter» (jfr GDPR) og at dette føres inn i og vedlikeholdes i SSHF sin løsning til dette formålet[2]
- skal utpeke en systemforvalter som operativt ansvarlig for å ivareta de oppgaver systemeier er ansvarlig for
- er kontaktperson for regional systemeier

Systemforvalter (systemansvarlig)

- utføre oppgaver delegert fra systemeier
- rådgi og rapportere til systemeier
- opprette og vedlikeholde autorisasjonsregister for personregisteret vedkommende er ansvarlig for
- opprette og vedlikeholde rutiner for brukerforvaltning, herunder tilgangsstyring og inn/-utmelding av brukere basert på tjenstlig behov
- vedlikeholde systemets oppføring i SSHF sin løsning for «protokoll over behandlingsaktiviteter» (jfr GDPR) (modul i Kvalitetsportalen, jfr fotnote 2)
- gjennomføre revisjoner av personer med tilgang til systemet hvert andre år
- sørge for at tiltak etter revisjon og risikovurderinger gjennomføres
- være kontaktpunkt ved innføring, endring, oppgraderinger, feilsituasjoner og testing
- fungere som stedlig kontaktperson for tjenesteansvarlig/tjenesteforvalter hos databehandler, dvs Sykehuspartner
- planlegge, tilrettelegge og gjennomføre intern opplæring i funksjonell og sikker bruk av systemet
- være oppdatert på relevante lovkrav samt teknisk og faglig utvikling som er relevant for systemet
- bestille endringer ved å omsette krav og funksjonelle behov fra fagmiljøet

Tjenesteansvarlig (rolle hos leverandør/Sykehuspartner)

- er det primære kontaktpunktet for systemeiere hos kunden for faglig dialog med databehandler om tjenestekvalitet og funksjonalitet, samt endring på tjenesten. Tjenesteansvarlig er ansvarlig for at tjenesten leveres etter avtalt tjenestekvalitet, og skal følge opp tjenesten gjennom hele livsløpet i tjenesteporteføljen.

Informasjonssikkerhetsleder

- må være faglig uavhengig, og ikke begrenset av plassering i organisasjonen med hensyn til sine oppgaver
- skal påse at SSHF ikke utsettes for uakseptabel risiko ved behandling av helse- og personopplysninger
- har ansvar for faglig rapportering til virksomhetens ledelse innen sitt fagområde

[2] *I SSHF benyttes modulen «Informasjonssystemer» i Kvalitetsportalen til å føre protokoll over systemer*

- har det utøvende ansvar for virksomhetens sikkerhetsarbeid bl.a. gjennom å:
  - forberede ledelsens årlige gjennomgang av bruk av informasjonssystemet og følge opp iverksetting av tiltak som er besluttet etter gjennomganger
  - lage årlige revisjonsplaner og sikre gjennomføring av sikkerhetsrevisjoner i virksomheten, samt rapportere planer og resultater gjennom virksomhetens etablerte kanaler for øvrig revisjonsaktivitet
  - vurdere rapporterte avvik og meddele avvik til virksomhetens ledelse i samsvar med virksomhetens etablerte rutiner for avviksbehandling
  - vurdere rapporterte avvik og meddele avvik i henhold til avtaler som er inngått
  - iverksette og støtte i gjennomføring av risikovurderinger
- drive opplysningsvirksomhet i foretaket om informasjonssikkerhet
- være rådgiver i sikkerhetsspørsmål
- utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområdet
- ansvarlig for å påse utvikling og vedlikehold av beredskaps-/varslingsplaner (katastrofeplan), samt kontinuitetsplaner relatert til IKT
- iverksette og delta i revisjoner, risikovurderinger og egenkontroll
- bistå og tilrettelegge i relevante tilsynssaker
- vurdere og avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå på vegne av adm. dir.
- stille krav til nye/endrede sikkerhetstiltak innenfor IKT-området, både for etablerte tjenester og nye behov som oppstår ved at nye IKT-løsninger innføres
- skal påse at hendelses- og avvikshåndtering, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, heri om nødvendig å gi pålegg
- iverksette korrektive og andre sikkerhetsrelaterte tiltak
- bistå i felles regionale fora for informasjonssikkerhet etter virksomhetens behov
- skal sørge for at SSHF sine oppføringer i regional «protokoll over behandlingsaktiviteter» blir vedlikeholdt basert på innholdet i SSHF sin egen løsning for «protokoll over behandlingsaktiviteter»

Ved uenighet med systemeiere om et IKT- eller fagsystem innehar, eller uenighet med leder om behandling av helse- og personopplysninger innebærer et uakseptabelt risikonivå, vil informasjonssikkerhetsleder kunne vurdere om saken skal løftes til administrerende direktør for beslutning.

Personvernombud

Personvernforordningens artikkel 37 nr. 1 pålegger virksomheten til å utpeke Personvernombud (PVO), når vilkårene i bokstav a til c er oppfylt. PVO skal utpekes på grunnlag av faglig kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området, i tillegg til evne til å utføre oppgavene [nevnt i artikkel 39 / som beskrevet under jf. artikkel 39]. PVO må være uavhengig, dvs. ha en selvstendig rolle, som ikke begrenses i organisasjonen med hensyn på sine oppgaver.

Personvernombudet skal minst ha følgende oppgaver:

- informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til personopplysningsloven
- kontrollere overholdelsen av personvernforordningen, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner
- på anmodning gi råd om vurderingen av personvernkonsekvenser (DPIA) og kontrollere gjennomføringen av den i henhold til artikkel 35
- samarbeide med tilsynsmyndigheten
- fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål

Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

Utpeking av personvernombud fritar ikke databehandlingsansvarlig for sitt ansvar for at reglene i personopplysningsloven overholdes.

Se for øvrig dokumentet Stillingsbeskrivelse personvernombud Rune Nesdal Jonassen.

Leder

Enhver leder er ansvarlig for informasjonssikkerhet og personvern innen eget område. Ledere skal sørge for at underlagte enheter og ansatte der det er relevant:

- er kjent med og etterlever sitt ansvar, virksomhetens styringssystem for informasjonssikkerhet og personvern, samt sikkerhetsbestemmelser som er relevante
- gjennomfører tilstrekkelig sikkerhetsopplæring av eget og innleid personell, slik at disse har en forståelse av hva som er forventet av dem. IKT Sikkerhetsinstruks skal som et minimum legges til grunn for denne opplæringen
- innhente signert taushetserklæring[3] for alle ansatte og innleid personell som ikke har dette regulert i lov, og påse at disse er kjent med og etterlever styrende dokumenter som regulerer brukeratferd
- tildeler og kontrollerer personellets tilgang til informasjon og tjenester etter fastsatt tilgangsregime, herunder ved avgang av personell. Som grunnleggende prinsipp skal den enkelte kun tildeles de rettigheter og tilganger som nødvendig i forhold til vedkommendes arbeidsoppgaver og tjenstlige behov.
- ved behov for registre og øvrige databehandlinger innenfor eget ansvarsområde, påse at nødvendige interne og eventuelt eksterne godkjenninger er innhentet i henhold til virksomhetens interne retningslinjer
- at alle helse- og personopplysninger som behandles og lagres utenfor de etablerte fag-systemene blir registrert og dokumentert i SSHF sin løsning[4] for føring av «protokoll over behandlingsaktiviteter» (jfr GDPR)
- følger opp det daglige sikkerhetsarbeidet, herunder sikring av områder og utstyr innenfor eget ansvarsområde gjennom virksomhetens etablerte system for avviksbehandling, nødvendige kontroller og iverksette relevante tiltak
- er ansvarlig for resultater, fremdrift og rapportering av sikkerhetsarbeidet innen eget ansvarsområde
- er ansvarlig for at kontinuitetsplaner ved bortfall av informasjonssystemer finnes

Dersom leder innen sitt ansvarsområde, beslutter ny eller endret behandling av personopplysninger, gjelder også følgende:

- skal sørge for at personvernkonsekvensvurdering (DPIA) gjennomføres i samsvar med personopplysningsloven ved ny eller endret behandling av personopplysninger, i samarbeid med personvernombudet
- er ansvarlig for at all behandling av personopplysninger utføres iht krav til innebygd personvern og personvern som standardinnstilling
- følge virksomhetens øvrige føringer ved slike endringer

Medarbeider

Den enkelte medarbeider er ansvarlig for å:

- følge virksomhetens sikkerhetsbestemmelser inkludert Sikkerhetsinstruks
- ha en forståelse av hva som er forventet av dem (adferd). For medarbeidere som skal ha tilgang til taushetsbelagte opplysninger, skal også grunnlag og hjemmel for oppslag i de taushetsbelagte opplysningene være forstått

[3] *Pr des 2020 erstattes tidligere taushetserklæring og databrukerkontrakt av ny felles IKT Sikkerhetsinstruks. IKT Sikkerhetsinstruksen er et obligatorisk dokument i SSHF sin kompetanseportal og anses som elektronisk signert når bekreftet lest der.*

[4] *I SSHF benyttes modulen «Informasjonssystemer» i Kvalitetsportalen til å føre protokoll over systemer*

- søke informasjon ved usikkerhet eller tvil
- forhindre og/eller rapportere hendelser som kan innebære eller er et avvik eller uønsket hendelse
- rapportere avvik og uønskede hendelser til nærmeste leder når disse oppstår, eventuelt informasjonssikkerhetsleder og/eller personvernombud i henhold til virksomhetens avviksrutiner[5]

IKT-leverandør/databehandler

IKT-leverandør/databehandler har ansvar for at virksomhetens informasjonssystem er tilgjengelig og fungerer som besluttet. Dette innebærer at IKT-leverandør har plikt til å etablere og vedlikeholde en infrastruktur som understøtter informasjonsbehandlingen som avtalt. IKT-leverandør skal gjøre fortløpende vurderinger av tekniske tiltak som må iverksettes for å sikre at infrastrukturen alltid har et tilstrekkelig nivå av sikkerhet. Endringer som kan påvirke sikkerhetsnivået skal risikovurderes og godkjennes av den enkelte dataansvarlige. Disse forpliktelser og oppgaver må etableres i databehandleravtale med IKT-leverandør/databehandler i forkant for overlevering av personopplysninger som skal forvaltes på vegne av foretaket.
Ved avvik rundt personopplysningssikkerhet eller generell informasjonssikkerhet og personvern skal databehandler varsle dataansvarlig umiddelbart og uten ugrunnet opphold.

Forpliktelser og oppgaver som databehandler er forpliktet til å oppfylle, og som må sikres i databehandleravtale:

- gjennomføre risikovurderinger og sikkerhetsrevisjoner knyttet til infrastruktur og basiskomponenter, og melde resultatene av vurderingene til dataansvarlig ved informasjonssikkerhetsleder for beslutning om akseptabelt risikonivå
- overvåke risiko forbundet med informasjonsbehandling og forestå risikovurderinger. Avvik og resultater skal rapporteres til dataansvarlige
- gjennomføre jevnlige sikkerhetsgjennomganger og rapportere resultater til foretakene jevnlig og ved behov
- endringer som påvirker eller som kan påvirke den enkelte dataansvarlige, skal i forkant for endring risikovurderes og gis godkjenning for endring av den enkelte dataansvarlige
- utarbeide katastrofe- og beredskapsplan for IKT-området og dokumentere at disse møter kravene fra dataansvarlig
- håndtere registrerte avvik og bistå ved oppfølging av avvik
- å etablere tiltak for å registrere sikkerhetsavvik, hindre forsøk på uautorisert bruk og tilhørende avvikshåndtering
- følge opp partnere, leverandører og andre databehandlere som har betydning for informasjonssikkerheten og personvernet
- sørge for at bruk av personopplysninger begrenses til det som er avtalt
- sørge for, utvikle og etterleve driftsdokumentasjon
- sørge for, utvikle og etterleve dokumentasjon for konfigurasjons- og endringskontroll
- etablere tiltak for å hindre uautorisert bruk og adgang til informasjonssystemene
- etablere tiltak for å motstå angrep fra skadelig kode
- etablere tiltak for å registrere, rapportere og håndtere sikkerhetsavvik
- inngå underdatabehandleravtale med eksterne leverandører

IKT-leverandør kan ikke benytte personopplysninger til andre formål enn det som er avtalt med dataansvarlig. IKT-leverandør skal holde oversikt over når et nytt system blir implementert eller et system fases ut.

Avvik eller dissens

Avvik på denne instruksen meldes i SSHF sitt system for uønskede hendelser (i Kvalitetsportalen). Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

[5] *Avvik og uønskede hendelser skal registreres i SSHF sin Kvalitetsportal, modul for uønskede hendelser*

Kryssreferanser

I.1.4-58 Stillingsbeskrivelse personvernombud Rune Nesdal Jonassen

Eksterne referanser

168 Regionalt ledelsessystem for informasjonssikkerhet