Informasjonssikkerhet - organisering av informasjonssikkerhetsarbeidet			SI/14.01-03	
Utgave: 1.00	Utarbeidet av: Informasjonssikkerhetsleder Håkon Iversøn	Godkjent av Direktør medisin og helsefag Ellen H. Pettersen	Gjelder fra: 20.10.2017	Side 1 av 5

Hensikt og omfang

Dette dokumentet er en del av det felles regionale styringssystemet for informasjonssikkerhet og er lik, i form og innhold, for alle foretakene i Helse Sør-Øst.

Formålet med dette dokument er å beskrive organisering av utøvende sikkerhetsansvar, -myndighetsforhold og oppgaver som del av Sykehuset Innlandet's styringssystem for informasjonssikkerhet.

Ansvar/målgruppe

Alle ansatte i Sykehuset Innlandet

Handling

Sykehuset Innlandet ved administrerende direktør er databehandlingsansvarlig for all behandling av helse- og personopplysninger med tilknytning til Sykehuset Innlandet. Administrerende direktør har ansvar for at alle personopplysninger blir behandlet iht gjeldende lovverk, se spesielt pasientjournalloven, helseregisterloven og personopplysningsloven med forskrift.

Divisjonsdirektør har det overordnede ansvar for etterlevelse av denne prosedyren i egen divisjon.

Avdelingssjef/leder har ansvaret for etterlevelse av denne prosedyren i egen avdeling/seksjon.

Personell som i kraft av sin stilling på Sykehuset Innlandet har tilgang til helse- og personopplysninger inkludert journal, er ansvarlig for etterlevelse av denne prosedyren.

Fremgangsmåte

Organisering av informasjonssikkerhetsarbeidet 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 databehandlingsansvarlig. Informasjonsinformasjonssikkerhetsleder, prosjekteiere, systemeiere/tjenesteeiere og andre i egen organisasjon svarer dermed for administrerende direktør i foretaket i samsvar med sin rolle. Bruk av databehandler påvirker ikke foretakets 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 etablert:

- Administrerende direktør
- Systemeier/Tjenesteeier
- Informasjonssikkerhetsleder
- Personvernombud

- Leder med personalansvar
- Bruker/medarbeider
- IKT-leverandør/databehandler

Administrerende direktør

- er databehandlingsansvarlig 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 skal sikre at tjenester er tilgjengelig for å gjennomføre tiltak
- har ansvar for at styringssystemet for informasjonssikkerhet 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
- 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 system vedkommende er systemeier/tjenesteeier 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
- skal vurdere og, i forståelse med informasjonssikkerhetsleder, godkjenne tilganger til systemet og uttrekk av informasjon i forbindelse med forskning, undervisning og kvalitetssikring, internt og eksternt
- er ansvarlig for formalia i forhold til konsesjon/meldeplikt/godkjenning hos REK
- definerer tilgangsroller for sitt system innenfor rammene gitt av daglig leder og gjøre disse kjent
- skal bidra til at det inngås skriftlige avtaler (databehandleravtale) med IKT-leverandør/databehandler med krav til sikkerhetsnivå, tjenestenivå og forvaltning
- 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 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

Tjenesteansvarlig

- 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.

Informasjonssikkerhetssleder

- må være faglig uavhengig, og ikke begrenset av plassering i organisasjonen med hensyn til sine oppgaver
- har ansvar for faglig rapportering til virksomhetens ledelse innen sitt fagområde
- har det utøvende ansvar for virksomhetens sikkerhetsarbeid blant annet gjennom å:
    - forberede ledelsens årlige gjennomgåelse 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 uønskede hendelser og meddele disse til foretakets ledelse i samsvar med foretakets etablerte rutiner
    - vurdere rapporterte uønskede hendelser og meddele disse 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
- avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå på vegne av administrerende direktør
- 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 håndtering av uønskede hendelser, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, heri om nødvendig å gi pålegg
- iverksette korrektive og andre sikkerhetsrelaterte tiltak
- bistå og tilrettelegge i relevante tilsynssaker
- bistå i felles regionale fora for informasjonssikkerhet etter foretakets og regionens behov

Personvernombud

Med hjemmel i personopplysningsforskriften § 7-12 har foretaket utnevnt personvernombud (PVO). PVO må være uavhengig, dvs ha en selvstendig rolle, som ikke begrenses i organisasjonen med hensyn på sine oppgaver. Datatilsynet har samtykket i utnevnelsen av PVO ved et vedtak, og det er derfor gjort unntak fra meldeplikt etter personopplysningsloven § 31 første ledd.

PVO har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet skal også føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32, se Datatilsynets nettsider for detaljer om oppgaver.

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

Leder med personalansvar

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

- er kjent med og etterlever sitt ansvar, foretakets styringssystem for informasjonssikkerhet og 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. Sikkerhetsinstruks skal som et minimum legges til grunn for denne opplæringen
- innhenter taushetserklæringer for alle ansatte og innleid personell som ikke har dette regulert i lov, og påser 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 foretakets interne retningslinjer
- følger opp det daglige sikkerhetsarbeidet, herunder sikring av områder og utstyr innenfor eget ansvarsområde gjennom foretakets etablerte system for uønskede hendelser, 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

Bruker/medarbeider:
Den enkelte medarbeider er ansvarlig for å:

- følge foretakets sikkerhetsbestemmelser inkludert sikkerhetsinstruks
- ha en forståelse av hva som er forventet av dem (adferd). For brukere som skal ha tilgang til taushetsbelagte opplysninger, skal også grunnlag og hjemmel for oppslag i de taushetsbelagte opplysningene være forstått
- søke informasjon ved usikkerhet eller tvil
- forhindre eller rapportere hendelser som kan innebære avvik
- rapportere uønskede hendelser til nærmeste leder når disse oppstår, eventuelt informasjonssikkerhetsleder i henhold til foretakets rutiner

IKT-leverandør/databehandler
IKT-leverandør/databehandler har ansvar for at foretakenes 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 databehandlingsansvarlige. 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.

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 databehandlingsansvarlig ved informasjonssikkerhetsleder for beslutning om akseptabelt risikonivå

- overvåke risiko forbundet med informasjonsbehandling og forestå risikovurderinger Avvik og resultater skal rapporteres til databehandlingsansvarlige
- gjennomføre jevnlige sikkerhetsgjennomganger og rapportere resultater til foretakene jevnlig og ved behov
- endringer som påvirker eller som kan påvirke informasjonssikkerheten til den enkelte databehandlingsansvarlige, skal i forkant for endring risikovurderes og gis godkjenning for endring av den enkelte databehandlingsansvarlige
- utarbeide katastrofe- og beredskapsplan for IKT-området og dokumentere at disse møter kravene fra databehandlingsansvarlig
- håndtere registrerte uønskede hendelser
- 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
- 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

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

Referanser

SI/14.01-04 Informasjonssikkerhet - Sikkerhetsmål og nivå for akseptabel risiko

Helseregisterloven
Personopplysningsloven
Forskrift om behandling av personopplysninger