Sykehuset Innlandet HF
Styremøte 30.01.18

SAK NR 005 – 2018
INFORMASJON OM INFORMASJONSSIKKERHET OG PERSONVERN I SYKEHUSET INNLANDET

Forslag til

VEDTAK:

1. Styret tar informasjonen om informasjonssikkerhet og personvern i Sykehuset Innlandet til orientering.

2. Styret ber om informasjon på styremøte i juni om eventuelle tiltak for å styrke informasjonssikkerheten og personvernet i helseforetaket når EUs personvernforordning «General Data Protection Regulation» gjøres gjeldende fra 25.5.2018.

Brumunddal, 23. januar 2018

Alice Beathe Andersgaard
administrerende direktør

SAKSFREMSTILLING

SAK NR. 005 – 2018

Bakgrunn

Denne styresaken redegjør for hvordan informasjonssikkerhet og personvern håndteres, organiseres og styres i Sykehuset Innlandet. Saken belyser sentrale begreper, områder og utfordringer innenfor områdene informasjonssikkerhet og personvern.

Begrepet Informasjonssikkerhet er inndelt i tre områder:

- Konfidensialitet - personvern
- Integritet – at opplysninger har tilstrekkelig kvalitet og ikke kan endres uten at det er synlig for mottaker og avsender
- Tilgjengelighet - at informasjonen er tilgjengelig

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og være forklart på en måte som gjør at alle berørte har samme forståelse av hva opplysningene skal brukes til. For at formålet skal være legitimt må det i tillegg ha et rettslig grunnlag som er i samsvar med etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet.

Sykehuset Innlandet er databehandlingsansvarlig for registre opprettet i Sykehuset Innlandet hvor personopplysninger behandles:

- Behandlingsrettede helseregister
- Forsknings- og kvalitetsregister
- Administrative register
- Medisinsk tekniske register

Saksframstilling

Databehandler og databehandleravtaler definisjoner
Personopplysningsloven § 2.

- *behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,*
- *databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige,*

Helseregisterloven § 2.

- *databehandlingsansvarlig: den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, og den som i eller i medhold av lov er pålagt et databehandlingsansvar,*

En databehandler kjennetegnes ved at de kun skal behandle personopplysninger på vegne av (etter instruks) fra den databehandlingsansvarlig. Databehandleren behandler aldri personopplysninger til egne formål og skal derfor ikke bruke opplysningene til annet enn utførelsen av oppgaven for den databehandlingsansvarlige.

Ansvar og roller for informasjonssikkerhet og personvern i Sykehuset Innlandet

Administrerende direktør
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, som pasientjournalloven, helseregisterloven og personopplysningsloven med forskrift.
Administrerende direktør kan delegere oppgaver knyttet til databehandleransvaret til andre ansatte.

Informasjonssikkerhetsleder
Sykehuset Innlandet har per i dag en stilling som informasjonsikkerhetsleder organisert i Stab Helse, avdeling for E-helse & teknologi. Stillingens oppgaver er i hovedsak innen IKT-sikkerhetsrådgivning til virksomheten og risikovurderinger og -analyser av nye og endrede IKT-systemer.
En mer detaljert beskrivelse av ansvarsområder tilknyttet denne rollen er beskrevet i Sykehuset Innlandet kvalitetsportal. *Informasjonssikkerhet – organisering av informasjonssikkerhetsarbeidet (SI / 14.01-03) Vedlegg 1*

Personvernombud
Sykehuset Innlandet HF har eget personvernombud i dag, i tillegg benytter Sykehuset Innlandet seg av Norsk Senter for forskningsdata(NSD) som personvernombud i forskningsprosjekter.

Ved innføringen av EU sin personvernforordning fra 25.5.2018 blir rollen som personvernombud utvidet. Som en EU-forordning vil dette gå rett inn i EU/EØS-landenes lovgivning. Forordningen er også kjent som GDPR - General Data Protection Regulation. Sykehuset Innlandet blir gjennom denne forordningen pålagt å ha et personvernombud med en uavhengig rolle. Dette fordi vi er definert som en databehandler som registrerer, lagrer, og bruker personsensitive data i stor skala.

Personvernombudets oppgaver er spesifisert i forordningens artikkel 39. Hovedområder er:

- Kontrollere overholdelsen av personvernregelverket
- Gi råd om vurdering av personvernkonsekvenser
- Samarbeide med Datatilsynet og fungere som kontaktpunkt

Datatilsynet anbefaler at vi har et personvernombud med dybdekunnskap om personvernlovgivning og praksis på området, noe som betyr juridisk bakgrunn og kompetanse. Forordningen presiserer at personvernombudet skal ha en uavhengig rolle. Dette innebærer at stillingen organiseres slik at ombudet ikke kan motta instrukser om hvordan oppgavene skal utføres eller hvordan utfallet av en sak skal være.

Databehandleravtalen mellom Sykehuset Innlandet HF og Sykehuspartner HF
Databehandleravtalen er bilag i årlig tjenesteavtale (SLA) mellom Sykehuset Innlandet HF og Sykehuspartner. Kapittel 8 i databehandleravtalen omtaler databehandlerens bruk av underleverandør. I henhold til denne avtalen har Sykehuset Innlandet HF det fulle ansvar som databehandlingsansvarlig.

Databehandleravtalen beskriver roller, oppgaver og ansvar knyttet til dem. Med bakgrunn i Datatilsynets varsel og erfaring fra den regionale prosessen så langt, etablererer Sykehuset Innlandet bedre systemer for oppfølging av databehandleravtalen. Sykehuset Innlandet må gjøre egne/selvstendige vurderinger av de gjennomførte risiko- og sårbarhetsanalyser (ROS-analyser) på alle endringene, før eventuell godkjenning.

Som tiltak vil Sykehuset Innlandet i samarbeid med det regionale helseforetaket forsøke å få endret eksisterende databehandleravtale til ny standard databehandleravtale med sjekkliste som Direktoratet for e-helse har utarbeidet. Databehandleravtalen mellom Sykehuset Innlandet og Sykehuspartner skal oppdateres og har som målsetting å være signert innen 1.4.2018.

Der hvor Sykehuspartner ikke er databehandler må Sykehuset Innlandet inngå databehandleravtaler med de som behandler data på vegne SI, det kan være leverandører, forskningsprosjekter o.l.

Hva betyr ny personvernlovgivning (GDPR) for databehandlingsansvarlig og databehandler?

Ny personvernforordning skal innføres i hele EU og EØS den 25.mai 2018.

GDPR: Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

Databehandlingsansvarlig, også kalt "behandlingsansvarlig", skal påse at behandlingen av helse- og personopplysninger og informasjonssikkerhet organiseres slik at det er tydelig hvem som har ansvar for de ulike deler av databehandlingen. Ansvaret knyttes i dag til Normen, en norsk bransjenorm som går lengre enn GDPR. Databehandlingsansvarlig er alltid øverste leder i bedriften. Ansvar og organisering skal dokumenteres før behandlingen av helse- og personopplysninger begynner. I Sykehuset Innlandet er det administrerende direktør som er databehandlingsansvarlig.

GDPR: Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
Databehandler behandler personopplysninger på vegne av og i henhold til avtale med Databehandlingsansvarlig. Databehandler for Sykehuset Innlandet er i dag enten Sykehuspartner eller Forskningsdirektør, og i noen tilfeller leverandører til Avdeling medisinsk teknologi. Helt konkret er Databehandlers rolle eksempelvis å sørge for diskplass, nettverk og servere. Dersom databehandler bruker underleverandør, skal databehandlingsansvarlig godkjenne denne.

Forberedelse til ny personvernregulering
Sykehuset Innlandet arbeider med å forberede overgang til ny personvernordning GDPR med følgende punkter:

- Oversikt over hvilke databehandlinger som gjennomføres og hvilket hjemmelsgrunnlag disse har
- Gjennomførte risikovurderinger av løsninger og infrastruktur
- Oversikt over leverandørtilganger, herunder risikovurderinger og databehandleravtaler
- Gjennomgang og oppgradering av rutiner og prosedyrer, herunder tilgang for leverandører
- Prosedyrer og rutiner for gjennomføring av databehandleravtaler og personvernkonsekvensvurderinger. Dette arbeidet er Sykehuspartner sentral i for å sikre felles rutiner og prosedyrer i regionen, samtidig som prosessene skal sikre at den enkelte databehandlingsansvarlig kan ivareta sitt ansvar, herunder og ikke akseptere hva som vurderes som for høy restrisiko.

Styring, organisering og oppgaver

Sykehuset Innlandet har en sikkerhetsledelse på personvern- og informasjons-sikkerhetsområdet, hvor ansvars- og myndighetsforhold er dokumentert og øverste ledelse er involvert. Det vil iverksettes ulike tiltak for å sikre og bedre foretakets ansvar for og kontroll av personopplysninger. Dette gjelder også i forbindelse med at Sykehuspartneres databehandleravtaler og deres databehandleravtaler med underleverandører.

Innenfor informasjonssikkerhet og personvern arbeides det med:

- Rådgivning og saksbehandling innen områdene sikkerhetsstrategi, sikkerhetsteknologi, tilsynssaker, informasjonssikkerhet, taushetsplikt, personvern, tilgang til pasientopplysninger, ivaretakelse av personvern ved forskning og kvalitetsregistre
- Planlegge, forberede, iverksette, gjennomføre eller bistå ved planlagte og systematiske tiltak (internkontroll) innen informasjonssikkerhet:
- Sikkerhetsrevisjoner
- Sikkerhetstester
- Risikovurderinger ved innføring av nye eller endring av eksisterende løsninger
- Avvikshåndtering og sikkerhetsbrudd
- Ledelsens gjennomgang av informasjonssikkerhet
- Utarbeide og vedlikeholde styrende dokumentasjon for informasjonssikkerhet etter retningslinjer fra Helse Sør-Øst RHF og Helsedirektoratet
- Følge opp behandling av helse- og personopplysninger til tilsynsmyndigheter

Elektronisk journal ved Sykehuset Innlandet.
Den elektroniske pasientjournalen består av alle IKT systemer som lagrer informasjon knyttet til å yte eller administrere helsehjelp til den enkelte. Hovedsystemet i den elektroniske pasientjournalen er DIPS, men det er også en rekke andre systemer som laboratoriesystemer, radiologisystemet (RIS/PACS), Partus, Auditbase, Noklus, Muuse mv. Disse systemene er fagsystemer hvor det er avgrensede personellgrupper som har tilgang.
Av de ulike journalsystemer er det DIPS som har den mest komplekse løsningen for tilgangsstyring.

Sykehuset Innlandet har benyttet DIPS fra 2007. Dagens DIPS løsning sikrer at pasientinformasjon følger hele pasientforløpet innenfor foretaket. I Helse Sør-Øst har hvert foretak sitt eget system med egen journal. Det pågår et regionalt prosjekt som har som mål å etablere en løsning hvor helsepersonell som har behov, gis mulighet til å lese journalinformasjon produsert ved andre foretak i regionen.

I DIPS ligger hele pasientens journal. I tillegg benyttes systemet som pasientadministrativt system som bl.a. håndterer ventelister, timebøker, innkallinger, offentlig rapportering, diagnoser, takster m.m. DIPS har et omfattende system for tilgangskontroll og logging knyttet til både journal og pasientadministrative data.

Logging
Alle ansatte logger inn i DIPS med sin egen unike identitet. All aktivitet blir deretter logget knyttet til den enkelte ansatte. Oppslag i journaldokumenter blir detaljert logget for hvert enkelt dokument. I tillegg blir oppslag i ulike lister og oversikter logget. Oversikt over oppslag i det enkelte journaldokumenter er tilgjengelig og synlig for andre ansatte. Det er også egne rapporter over dokumentoppslag foretatt av den enkelte ansatte som utleveres pasienter ved forespørsel.

Oppfølging av logg
Det utføres to typer innsynskontroll i EPJ: målrettet innsynskontroll og systematisk logganalyse. Med målrettet innsynskontroll menes kontroll basert på konkrete henvendelser fra pasient, pårørende, Helsetilsynet, ansatte eller lignende der det er mistanke om at uautorisert innsyn i journal har funnet sted.
Med systematisk logganalyse menes kontroller som utføres ved nærmere definerte tidsintervall og med bruk av metoder som både er vilkårlige og delvis målrettede.
Det arbeides i tillegg regionalt med å etablere system for mønstergjenkjenning-/statistisk loggkontroll. Dette vil gi betydelig større grad av treffsikkerhet enn manuell kontroll. Dette skulle vært på plass tidlig i 2017, men er forsinket. Helse Sør-Øst har etablering av løsning under planlegging.

Administrerende direktørs vurdering

Arbeidet med Informasjonssikkerhet og personvern er krevende og omfattende.

Administrerende direktør mener at foretaket har etablert gode systemer for å ivareta informasjonssikkerhet og personvern, men framtidige krav utfordrer helseforetaket innenfor dette området. Ny personvernforordning som skal innføres i hele EU og EØS den 25.mai 2018 fordrer mer ressurser og en langt mer aktiv personvernombudfunksjon.

Administrerende direktør vil at igangsette en prosess for å utrede om personvern-ombudsfunksjonen bør styrkes for å oppfylle framtidig lovkrav. Styret vil bli informert om det videre arbeidet med tiltak for å styrke pasientsikkerheten og personvernet i styremøte i juni 2018.

Vedlegg: Informasjonssikkerhet – organisering av informasjonssikkerhetsarbeidet (SI / 14.01-03)