Sykehuset Innlandet HF
Styremøte 29.08.18

SAK NR 061 – 2018
INFORMASJON OM TILPASNINGER TIL NY PERSONOPPLYSNINGSLOV MED FORORDNING (GDPR) – STATUS I ARBEIDET I SYKEHUSET INNLANDET

Forslag til

VEDTAK:

Styret tar informasjon om status i arbeidet med ny «Lov om personopplysninger», personvernforordningen(GDPR) i Sykehuset Innlandet til orientering.

Brumunddal, 23. august 2018

Alice Beathe Andersgaard
administrerende direktør

SAKSFREMSTILLING

SAK NR. 061 – 2018

Bakgrunn

Det vises til tidligere orientering, styresak 005-2018, om innføring av ny personvernforordning. Denne styresaken redegjør for arbeidet med å innføre ny «Lov om personopplysninger», personopplysningsloven, med endringene i personvernforordningen (GDPR) i EU/EØS. Ny lov trådde i kraft i Norge 20.07.18.

Den nye personopplysningsloven består av to hovedelementer:

1. EUs personvernforordning (GDPR) gjøres til norsk lov.
2. En rekke bestemmelser som supplerer reglene i forordningen.

Den nye personopplysningsloven endrer og skjerper pliktene til håndtering av person-opplysninger og borgerne får et styrket personvern. Loven gjelder alle som opererer i EU og EØS-området eller som tilbyr varer eller tjenester til personer som befinner seg der, inkludert Storbritannia.

Administrerende direktør har nedsatt en tverrfaglig arbeidsgruppe som skal utrede og vurdere konsekvenser ny personvernlovgivning har for Sykehuset Innlandet. Arbeidsgruppen skal videre sørge for at det implementeres løsninger og endringer slik at ny personopplysningslov etterleves.

Saksframstilling

De nye lovkravene pålegger bedrifter, herunder helseforetak, strengere plikter ved behandling av personopplysninger. Ansatte og pasienter får flere og bedre rettigheter og en rekke bedrifter får plikt til opprette personvernombud. Brudd på loven kan medføre overtredelsesgebyr fra Datatilsynet på inntil 20 millioner euro eller 4 % av brutto omsetning.

Arbeidet i Sykehuset Innlandet er todelt, en felles regional del og en lokal del. Idet følgende beskrives status på dette arbeidet i forhold til:

- Personvernstrategi
- Prosedyrer for etterlevelse av ny lovgivning
- Personvernerklæring
- Tilgangsprosedyrer
- Databrudd
- Overføring av personopplysninger
- Personvernkonsekvensanalyse
- Personvernombud i Sykehuset Innlandet

Personvernstrategi

Ny lovgivning pålegger både den dataansvarlige og databehandler å sørge for:

- Oversikt over type register
- Formål med register
- Lovhjemmel for opprettelse av register
- Klassifisering av data i register

Sykehuset Innlandet har implementert ny modul i kvalitetssystemet for registrering av alle register i Sykehuset Innlandet. Dette er et omfattende arbeid hvor Sykehuset Innlandet, som dataansvarlig, er avhengig av leveranser fra hoved-databehandler, Sykehuspartner HF.

Prosedyrer for etterlevelse av ny lovgivning

I Helse Sør-Øst er det etablert et felles regionalt styringssystem for informasjonssikkerhet for å kunne tillate tilgang på tvers av foretakene. Dette er et regionalt arbeid og reviderte prosedyrer forventes implementert i Sykehuset Innlandet i løpet av september 2018.
I tillegg til felles regionale prosedyrer for informasjonssikkerhet må lokale prosedyrer i Sykehuset Innlandet revideres når de regionale prosedyrer er implementert. Dette arbeidet pågår.

Personvernerklæring

Sykehuset Innlandet har utarbeidet og distribuert ny personvernerklæring til alle medarbeidere. Personvernerklæringen til medarbeiderne inneholder formålet med registreringen, hvilke personopplysninger som registreres om den ansatte og hvor lenge opplysningene lagres.

Ny personvernlovgivning styrker den registrertes rettigheter og stiller derfor krav til den som samler inn personopplysninger om at den registrerte skal informeres om sine rettigheter. Det stilles krav til at informasjon skal være lett tilgjengelig, lett forståelig, være tilpasset barn og inneha nødvendig kontaktinformasjon. Informasjon må gi opplysninger om:

- Rett til innsyn
- Rett til korrigering
- Rett til sletting
- Rett til begrenset behandling
- Rett til dataportabilitet
- Innsigelsesrett

Det er publisert revidert personvernerklæring på Sykehuset Innlandets intranett og internettsider.

Tilgangsprosedyrer

Et krav i ny lovgivning er innebygd personvern («by design and default») i løsninger som behandler personopplysninger. Dette innebærer blant annet å revidere og etablere nye retningslinjer for tilgang til personopplysninger, inkludert krav til retting, sletting, innsyn og sperring. For de store og mest sentrale systemene (elektronisk pasientjournal, laboratoriesystemer, radiologisystemer og fødesystem) er retningslinjer implementert.
Det gjenstår revidering av andre (mindre) systemer.
Dette arbeidet påbegynnes i september 2018, og beregnes ferdig innen juni 2019.

Databrudd

Ny personvernlovgivning stiller strengere krav til rapportering til tilsynsmyndighet (Datatilsynet). Sykehuset Innlandets prosedyrer ved databrudd må revideres, herunder dokumentasjonskrav og hendelseshåndtering, slik at ny lovgivning etterleves. Nye prosedyrer og rapporteringsskjema vil bli ferdigstilt innen 01.10.18.

Overføring av personopplysninger

Sykehuset Innlandet, som dataansvarlig, skal påse at det er inngått databehandleravtaler med de som behandler personopplysninger på vegne av Sykehuset Innlandet. Dette innebærer at Sykehuset Innlandet skal ha tilgang til og godkjenne underleverandøravtaler dersom databehandler har avtale med andre leverandører.

Nye maler for databehandleravtaler er utarbeidet og tilpasset ny lovgivning. Allerede inngåtte avtaler med leverandører vil erstattes av avtaler basert på den nye malen. Arbeid med signering av ny avtaler vil starte så snart som mulig etter at ny mal er kvalitetssikret og beregnes ferdig i løpet av første halvår 2019.

Mal for databehandleravtaler med land utenfor EU/EØS er utarbeidet. Det gjenstår revidering/implementering av prosedyrer, og det forventes at dette vil være ferdig implementert innen 01.11.2018.

Personvernkonsekvensanalyse (DPIA)–Data Protection Impact Assessment

Personvernkonsekvensvurdering (DPIA) skal gjøres ved behov og Sykehuset Innlandet er selv ansvarlig for å gjøre en slik behovsvurdering. Rutiner for gjennomføring og forankring av behovsvurdering, samt eventuell gjennomføring av personvernkonsekvensvurdering må etableres.
Veiledere og retningslinjer fra Datatilsynet er publisert. Arbeidet med slike vurderinger er ikke startet i Sykehuset Innlandet.

Med ny personopplysningslov vil det bli et større behov for risikovurderinger, da også som en dynamisk metodikk og prosess som sikrer identifisering og gjennomføring av tiltak for å nå en akseptabel risiko. Dette også som grunnlag for beslutninger.
Risikovurderinger legges til grunn for personvernkonsekvensvurderingene. Det er ikke hensiktsmessig å gjøre en personvernkonsekvensvurdering for hvert IKT-system, men heller for aktuelle arbeidsprosesser. Hensikten med å vurdere personvernkonsekvens for arbeidsprosesser er å fange opp forbedringspunkter i informasjonsflyt, saksgang og manuelle rutiner.

Personvernombud

I henhold til ny lovgivning er alle virksomheter av en viss størrelse og offentlige myndigheter pålagt å oppnevne et personvernombud.
I forbindelse med innføring av nytt lovverk er det kommet anbefaling fra Datatilsynet om at rollen som personvernombud og informasjonssikkerhetsleder bør skilles. I dag innehas disse rollene av samme person i Sykehuset Innlandet.

Ved innføring av nytt lovverk må det utarbeides en rollebeskrivelse som tydeliggjør ansvar, struktur, omfang og ressurser for personvernombud i Sykehuset Innlandet.

Administrerende direktørs vurdering

Arbeidet med informasjonssikkerhet og personvern er krevende og omfattende. Endringene i personvernlovgivningen vil føre til økt fokus på informasjonssikkerhet og personvern med tilhørende behov for innføring av tiltak på mange områder. Sykehuset Innlandet prioriterer dette arbeidet og jobber sammen med andre helseforetak og det regionale helseforetaket for kontinuerlig å ha gode løsninger og rutiner.

Sykehuset Innlandet er godt i gang med å implementere de nye kravene. Arbeidet er lagt slik opp at hele organisasjonen bidrar til at rutiner og prosedyrer blir tilpasset. Ledere på alle nivåer må ta ansvar for prosessene med bistand fra stabsfunksjonene, personvernombud og leder for informasjonssikkerheten.