Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	14. desember 2017

SAK NR 122-2017

ORIENTERINGSSAK - INFORMASJONSSIKKERHET OG PERSONVERN.
NY PERSONVERNLOVGIVNING I EU/EØS (GDPR)

Forslag til vedtak:

Sak om Informasjonssikkerhet og personvern – herunder ny personvernlovgivning i EU/EØS (GDPR) tas til orientering.

Oslo, 7. desember 2017

Cathrine M. Lofthus
administrerende direktør

1. Hva saken gjelder

Saken legges frem for å informere styret om arbeidet med informasjonssikkerhet og personvern i regionen, inkludert arbeidet rundt europeisk personvernlovgivning som blir norsk lov i mai 2018.

2. Hovedpunkter og vurdering av handlingsalternativer

Saken omhandler følgende:

- Databehandlingsansvarlig og databehandler – roller, ansvar og forpliktelser
- Felles regionalt styringssystem for informasjonssikkerhet i Helse Sør-Øst, innhold og realisering
- RSR – Regionalt sikkerhetsfaglig råd - roller og fokusområder
- Ny personvernlovning fra mai 2018, General Data Protection Regulation (GDPR)
- Forberedelser til GDPR i Helse Sør-Øst

Databehandlingsansvarlig og databehandler – roller, ansvar og forpliktelser

Databehandlingsansvarlig

- Pasientjournalloven/Helseregisterloven
  - *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
- Personopplysningsloven
  - *Behandlingsansvarlig*: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes

For journalsystemet DIPS og kurve- og medikasjonsløsning, samt spesialistsystemer som laboratoriesystem og radiologisystem, er det enkelte helseforetak databehandlingsansvarlig. For administrative og økonomiske systemer, som ERP-løsning og Public360, er også Helse Sør-Øst RHF og Sykehuspartner HF databehandlingsansvarlig for sine løsninger på samme måte som helseforetakene.

Databehandler

- Personopplysningsloven
  - *Databehandler:* den som behandler personopplysninger på vegne av den behandlingsansvarlige

Sykehuspartner HF er regionens felles databehandler og er selv databehandler for alle løsninger som driftes av Sykehuspartner HF. Sykehuspartner HF kan videre ha underdatabehandlere. Dette er alle aktører som enten gis tilgang inn i løsningen som Sykehuspartner HF drifter når det er behov for slik tilgang, eller der underleverandør drifter en løsning som Sykehuspartner HF er hovedansvarlig for, eksempelvis personalportalen som driftes hos Bluegarden og ERP-løsningen som driftes hos Evry.

Databehandlingsansvarliges oppgaver

Databehandlingsansvarlig skal fastlegge hvordan arbeidet med informasjonssikkerhet i virksomheten skal organiseres og gjennomføres, slik at det kommer klart frem hvem som er ansvarlig på alle nivåer og hva de er ansvarlig for. Databehandlingsansvarlig er også ansvarlig for at bestemmelsene i personopplysningsforskriften kapittel 2 og 3 følges. Dette omfatter blant annet at databehandlingsansvarlig, basert på risikovurderinger, skal ta stilling til om restrisiko er akseptabel ved innføring av nye databehandlinger eller ved endringer av eksisterende databehandlinger.

Felles regionalt styringssystem for informasjonssikkerhet i Helse Sør-Øst

Det er etablert felles regionalt styringssystem for informasjonssikkerhet i Helse Sør-Øst. Dette omfatter følgende:

- Forvaltningsprinsipper og sammenheng mellom sikkerhetsregulerende lovverk
- Overordnet styring
- Gjennomførende dokumenter – alle bruker
- Gjennomførende dokumenter – systemkrav og føringer
- Kontrollerende dokumenter

Styringssystemet for informasjonssikkerhet er i oppdragsdokumentet forutsatt å implementeres i hvert av helseforetakene, inkludert Sykehuspartner HF, i 2017. De ideelle private sykehusene er også inkludert i dette arbeidet, og arbeider med implementering av det felles regionale styringssystemet for informasjonssikkerhet i Helse Sør-Øst i sine styringssystem.

Revisjon av dokumentene

I løpet av en 2-års periode skal alle dokumentene ha vært vurdert i forhold til behov for revisjon. Dette omfatter behov for ytterligere detaljering av føringer og oppdateringer i forhold til lov- og forskriftsendringer.

Med grunnlag i at norsk personvernlovgivning blir oppdatert med EUs GDPR i mai 2018, er arbeidet med å oppdatere dokumentene i forhold til denne endringen under planlegging. Som en del av dette arbeidet er det tatt kontakt med sekretariatet til Norm for informasjonssikkerhet for helse som er etablert i Direktoratet for e-helse. Direktoratet vil blant annet delta på kommende regionale fagsamling i Regionalt sikkerhetsfaglig råd (RSR).

Organisering av informasjonssikkerhetsarbeidet

Sikkerhetsfunksjoner med definerte ansvarsområder i felles regionale styringssystem for informasjonssikkerhet:

- Administrerende direktør
- Systemeier/tjenesteansvarlig
- Informasjonssikkerhetsleder
- Personvernombud
- Leder med personalansvar
- Bruker/medarbeider
- IKT-leverandør/databehandler

RSR – Regionalt sikkerhetsfaglig råd - roller og fokusområder

Det har i flere år eksistert et felles faglig råd innen informasjonssikkerhet i regionen. Fra 2015 har medlemmene vært formelt oppnevnt av administrerende direktør i det enkelte helseforetak.

Nærmere om Regionalt sikkerhetsfaglig råd (RSR):

- Det påligger den enkelte oppnevnte deltaker å sikre forankring og deling av informasjon, samt at det fattes nødvendige beslutninger i eget helseforetak.
- Ved uenighet i RSR i saker som krever enighet for å sikre regionalt sikkerhetsnivå eller felles løsninger, skal saken eskaleres til egen administrerende direktør.
- Regionalt sikkerhetsfaglig råd er faglig ressurs for regionen samlet, for de enkelte helseforetakene og for Helse Sør-Øst RHF
- Regionalt sikkerhetsfaglig råd ivaretar bredde på kompetanse innen personvern og informasjonssikkerhet og benyttes for å sikre gode anbefalinger og beslutninger i regionen innen disse fagområdene
- Sentrale koordineringsoppgaver og områder hvor RSR gir råd til foretaksgruppen:
  - Felles regionalt styringssystem for informasjonssikkerhet
  - Sikkerhetsmål og -strategi for regionale tjenester og for foretaksspesifikke tjenester som kan påvirke felles sikkerhetsnivå
  - Akseptabelt risikonivå
  - Sikkerhetsføringer og -krav
  - Tilgangsstyring
  - Revisjon, avvikshåndtering og opplæring innen personvern og informasjonssikkerhet
  - Sikre felles vurderinger innen informasjonssikkerhet og personvern

RSR spiller en sentral rolle knyttet til å etablere og koordinere felles føringer for informasjons-sikkerhet i regionens IKT-løsninger. RSR har også etablert et eget arbeidsutvalg for i fellesskap å gjøre faglig gjennomganger av risikovurderinger av løsninger. Sykehuspartner HF gjennomfører og presenterer risikovurderingene for arbeidsutvalget. De ulike risikoelementer blir diskutert faglig med bruk av hele regionens sikkerhetskompetanse, men det er hvert enkelt helseforetak som må konkludere på om restrisiko er akseptabel eller om det er nødvendig med tilleggstiltak.

Ny personvernlovning fra mai 2018 - GDPR

GDPR gjelder direkte for alle EUs medlemsstater fra 25. mai 2018. Forordningen skal innlemmes i EØS-avtalen, og gjennomføres i norsk rett gjennom en ny personopplysningslov som henviser til GDPR. Justis- og beredskapsdepartementet tar sikte på at den nye personopplysningsloven skal tre i kraft i Norge 25. mai 2018. Forordningens regler vil i hovedsak måtte anvendes slik de står. Dette innebærer at personvernlovgivningen i EU og EØS-land blir mer lik enn hva den er i dag. Norge er et av de land som allerede har sterk personvernlovgivning, og mye av det som nå kommer i europeisk lovgivning er allerede i samsvar med nåværende regelverk. Likevel er det noen tydeliggjøringer og klarere krav som vil gjøres gjeldende ved den nye loven.

De største endringer i forhold til nåværende lovgivning er:

- Rettigheter til inkluderte tydeliggjøres og økes
- IKT-løsninger skal ha innebygget personvern
- Sterkere krav til avviksvarsling til Datatilsynet og kort tidsfrist for varsling
- Fornærmede ved avvik skal varsles
- Må ha personvernombud og rollen styrkes
- Databehandler får et selvstendig ansvar
- Krav til personvernkonsekvensvurdering i tillegg til risikovurdering
- Ansvaret til virksomheten for å sikre etterlevelse av personvernlovgivningen blir skjerpet
- Konsekvenser ved brudd på GDPR er betraktelig større enn i inneværende lovverk, opp til 4 % av omsetningen i bøter, begrenset oppad til 20 millioner Euro

Hovedbudskap fra Datatilsynets nettsider for å forberede GDPR

Datatilsynet har lagt ut veiledninger for hva som må gjøres. En av disse gir en enkel overordnet anbefaling om hvilket arbeid som må gjennomføres:

- Ha oversikt over hvilke personopplysninger som behandles
- Oppfylle dagens lovkrav
- Sette seg inn i det nye regelverket
- Lag rutiner for å følge de nye reglene

Det vises forøvrig til vedlegg fra Datatilsynet.

Kort om forberedelser til GDPR i Helse Sør-Øst

Følgende arbeid og forberedelser til GDPR er under gjennomføring i Helse Sør-Øst:

- Oppdragsdokumentet for 2017 forutsetter at det gjøres forberedende arbeid for å møte kravene ny personvernlovgivning vil innebære.
- Målrettet oppdatering av felles regionalt styringssystem for informasjonssikkerhet i Helse Sør-Øst. I dette arbeidet er både Datatilsynets fagpersonell og Direktoratet for e-helse, som arbeider med tilsvarende oppdatering av Norm for informasjonssikkerhet for helse, invitert inn for å informere om sitt arbeid i RSR.
- Sykehuspartner HF har fått følgende oppdrag, som etter ferdigstilling vil inngå i felles regionalt styringssystem for informasjonssikkerhet:
    - Forbedre metoden for risikovurdering, herunder ta med krav som ligger i GDPR
    - Utarbeide forslag til håndtering av personvernkonsekvensvurdering som tillegg til gjennomført risikovurdering
    - Utarbeide oppdatert mal for databehandleravtale som omfatter kravene i GDPR
    - Alle helseforetakene skal oversende oversikt over alle registre med personopplysninger, slik at Sykehuspartner HF kan forberede og gjennomføre nødvendige sikkerhetstiltak.

- Informasjonsmøter om hvilke endringer og krav GDPR innebærer:
    - Ledergruppen i Helse Sør-Øst RHF
    - Avdelinger i Helse Sør-Øst RHF
    - Regionalt direktørmøte
    - Regionalt teknologiledermøte
    - RSR
    - To halvdags seminarer for regionens jurister og informasjonssikkerhetsledere
    - Det er under planlegging et halvdags seminar for forskning

3. Administrerende direktørs anbefaling

Administrerende direktør konstaterer at det er igangsatt flere aktiviteter med sikte på å forberede foretaksgruppen på å møte krav om informasjonssikkerhet og personvern generelt, men også i forhold til å møte nye krav som kommer i mai 2018 som følge av nye krav fra EU/EØS (GDPR).

Administrerende direktør understreker at det er stilt krav til helseforetakene knyttet til informasjonssikkerhet og personvern i oppdragsdokumentet for 2017. Det legges opp til særskilt oppfølging av helseforetakene for å forsikre at kravene knyttet til informasjonssikkerhet og personvern per november er oppfylt.

Administrerende direktør anbefaler at styret tar saken til orientering.

Trykte vedlegg:

- Nye personvernregler fra 2018. Hva betyr det for din virksomhet? Veileder fra Datatilsynet

Utrykte vedlegg:

- Ingen