SUNNAAS SYKEHUS

Saksfremlegg

Saksgang	Møtedato
Orientering status GDPR	18.12.2019
Orienteringssak til styret 20.03.2018	20.03.2018
Orientering status GDPR	21.09.2018
Orientering GDPR	23.01.2018
Oppdatering av styringssystem for informasjonssikkerhet	16.10.2018
Separasjon av rollene informasjonssikkerhetsleder og personvernombud	15.04.2019

Sak 0080-2019

Status arbeid med GDPR (General Data Protection Regulation) og videre fokusområder

Forslag til vedtak

Styret tar saken til orientering

Nesodden, 18.12.2019.

Einar Magnus Strand
Administrerende direktør

1. Hva saken gjelder

Saken er en oppfølgingssak, og har vært i foretaksledelsen og styret ved flere anledninger tidligere. Omfanget og kompleksiteten har vært vanskelig å forutsi, og har gjennom perioden økt. Risikovurderinger på MTU-området (medisinsk teknisk utstyr) har vært prioritert. Konsulentselskapet Sopra Steria har fullført sitt arbeid med kartlegging og protokoll. Større fokus fremover på etterlevelse og forvaltning, som samsvarer med krav og føringer fra offentlige myndigheter. Avvik fra konsernrevisjonen er lukket.

2. Hovedpunkter og vurdering av handlingsalternativer

General Data Protection Regulation (GDPR) ble innført sommer 2018, og har ført til endringer i Sunnaas sykehus HF knyttet til informasjonssikkerhet og personvern. Saken har vært til behandling i foretaksledelsen og styret ved flere anledninger. Implementering av GDPR-relaterte prosesser, rutiner og oppgaver var temasak i oktober 2018. Arbeidet hadde frist til 01.05.2019, og var forankret i en implementeringsplan utarbeidet høsten 2018. Planen ble revidert underveis der oppgaver ble tatt bort og tilført etter behov.

Det ble tildelt ressurser tilsvarende 0,5 årsverk (innleid konsulent) som så langt har blitt benyttet i arbeid med implementering av oppgaver, spesielt knyttet til medisinsk teknisk utstyr (MTU) og risikovurderinger. I tillegg ble det bevilget ekstra midler for å engasjere Sopra Steria til å jobbe med GDPR-relaterte oppgaver som i hovedsak innebærer arbeid med protokoll over behandlingsaktiviteter og artikkel 30 i personvernforordningen.

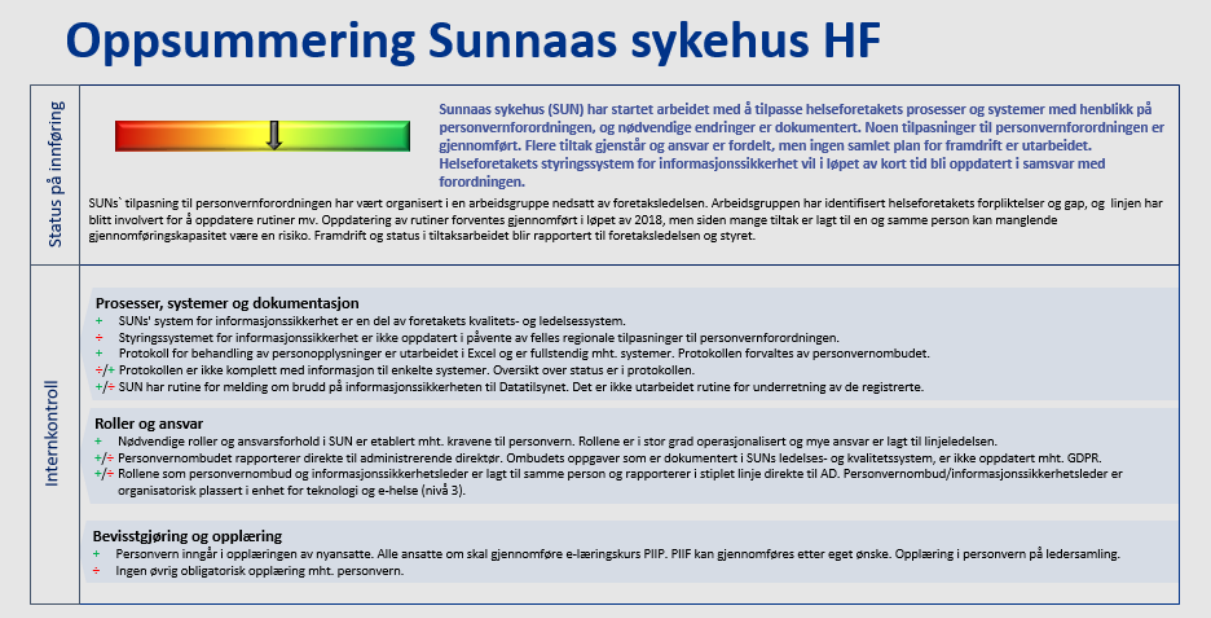
Sopra Steria kom ikke helt i mål med arbeidet innenfor de økonomiske rammene av oppdraget. Det ble imidlertid etablert en mal for protokollene, og de mest vesentlige behandlingene er dekket. Det ble i sluttrapporten anbefalt at Sunnaas sykehus sluttfører arbeidet. En viktig del som må fullføres er dokumentasjon av behandlingsgrunnlag. Rapporten avdekket at kompleksiteten med arbeidet var større enn antatt, prosesser som bør forbedres er konkretisert. Det krever fortsatt både tid og ressurser for å fullføre dette. Økt bevissthet rundt disse prosessene vil styrke arbeidet med personvern i klinikken og foretaket.

Status ad arbeidet med MTU viser at foretaket er mer a jour med gjennomføring av risikoanalyser. Det jobbes også med å lære opp medarbeidere som skal ha ansvaret for MTU – herunder internkontroll, risikovurderinger, vedlikehold med mer. Enhet for teknologi og e-helse er i kontakt med Sykehuspartner for å få tilgang til opplæringsmateriell, samt mulighet for hospitering i 2020.

Sunnaas sykehus HF er ikke helt mål med alle oppgavene som skissert i implementeringsplanen, men dette vil komme på plass i løpet av kort tid. Fokuset nå er mer rettet mot etterlevelse og forvaltning, fremfor implementering. Det er fortsatt behov for å arbeide videre med å etablere en metodikk for å avdekke gap mellom gjeldende praksis og regelverket. Dette er også i tråd med risikobasert styring, hvilket er nødvendig for å ha tilstrekkelig kontroll med personvern og informasjonssikkerhet.

Et annet prioritert område fremover er å se på overordnende prosesser og arbeid knyttet til personvern og informasjonssikkerhet. Dette krever at fagfeltet får mer tid og fokus knyttet til

virksomhetsovergripende prosesser. Det har vært mye oppmerksomhet rundt nytt regelverk og informasjonssikkerhet siden innføringen av GDPR sommeren 2018, noe som viser seg gjennom rådgivende revisjon fra konsernrevisjonen høsten 2018, forvaltningskontroll fra Riksrevisjonen avlevert april 2019, og Datatilsynets uttalelser om tilsyn med fokus på personvernombud og organisering. Avvikene som ble synliggjort av konsernrevisjonen høsten 2018 er nå tilstrekkelig lukket, og gode prosesser og rutiner på plass. Det vurderes derfor at foretaket står sterkt rustet ved en konsernrevisjon i 2020.



Oppsummering Sunnaas sykehus HF

Status på innføring

Sunnaas sykehus (SUN) har startet arbeidet med å tilpasse helseforetakets prosesser og systemer med henblikk på personvernforordningen, og nødvendige endringer er dokumentert. Noen tilpasninger til personvernforordningen er gjennomført. Flere tiltak gjenstår og ansvar er fordelt, men ingen samlet plan for framdrift er utarbeidet. Helseforetakets styringssystem for informasjonssikkerhet vil i løpet av kort tid bli oppdatert i samsvar med forordningen.

SUNs' tilpasning til personvernforordningen har vært organisert i en arbeidsgruppe nedsatt av foretaksledelsen. Arbeidsgruppen har identifisert helseforetakets forpliktelser og gap, og linjen har blitt involvert for å oppdatere rutiner mv. Oppdatering av rutiner forventes gjennomført i løpet av 2018, men siden mange tiltak er lagt til en og samme person kan manglende gjennomføringskapasitet være en risiko. Framdrift og status i tiltaksarbeidet blir rapportert til foretaksledelsen og styret.

Internkontroll

Prosesser, systemer og dokumentasjon

+ SUNs' system for informasjonssikkerhet er en del av foretakets kvalitets- og ledelsessystem.
÷ Styringssystemet for informasjonssikkerhet er ikke oppdatert i påvente av felles regionale tilpasninger til personvernforordningen.
+ Protokoll for behandling av personopplysninger er utarbeidet i Excel og er fullstendig mht. systemer. Protokollen forvaltes av personvernombudet.
÷/+ Protokollen er ikke komplett med informasjon til enkelte systemer. Oversikt over status er i protokollen.
+/÷ SUN har rutine for melding om brudd på informasjonssikkerheten til Datatilsynet. Det er ikke utarbeidet rutine for underretning av de registrerte.

Roller og ansvar

+ Nødvendige roller og ansvarsforhold i SUN er etablert mht. kravene til personvern. Rollene er i stor grad operasjonalisert og mye ansvar er lagt til linjeledelsen.
+/÷ Personvernombudet rapporterer direkte til administrerende direktør. Ombudets oppgaver som er dokumentert i SUNs ledelses- og kvalitetssystem, er ikke oppdatert mht. GDPR.
+/÷ Rollene som personvernombud og informasjonssikkerhetsleder er lagt til samme person og rapporterer i stiplet linje direkte til AD. Personvernombud/informasjonssikkerhetsleder er organisatorisk plassert i enhet for teknologi og e-helse (nivå 3).

Bevisstgjøring og opplæring

+ Personvern inngår i opplæringen av nyansatte. Alle ansatte om skal gjennomføre e-læringskurs PIIP. PIIF kan gjennomføres etter eget ønske. Opplæring i personvern på ledersamling.
÷ Ingen øvrig obligatorisk opplæring mht. personvern.

Videre prosess i GDPR-arbeidet innebærer overgang mot etterlevelse og forvaltning av personvernforordningen, og innebærer som nevnt ovenfor økt krav til dokumentasjon, kontroll og styring.

3. Administrerende direktørs anbefaling

1. Implementeringsarbeidet fortsetter, og det opprettholdes fokus på GDPR og videre etterlevelse av regelverket, slik at man kan jobbe med gap og mangler som blir oppdaget. Kontinuerlig fokus vil styrke personvernarbeidet.

2. Jobbe strukturert med oppfølgingspunktene fra Sopra Steria. En oppdatering av dette arbeidet vil presenteres for foretaksledelsen før sommeren 2020.

3. Videre arbeid med MTU – området, herunder anskaffelser og dokumentasjon, prioriteres for å komme på et tilstrekkelig sikkerhetsnivå