UNIVERSITETSSYKEHUSET NORD-NORGE
DAVVI-NORGGA UNIVERSITEHTABUOHCCEVIESSU

STYRESAK

Styresak:	**97/2021**
Møtedato:	**16.12.2021**
Arkivsak:	2021/4-9
Saksbehandler:	Ingrid Lernes Mathiassen

Orienteringssaker til styremøte 16.12.2021

Innstilling til vedtak

Styret ved Universitetssykehuset Nord-Norge HF tar orienteringssakene til orientering.

1. Informasjon fra administrerende direktør til styret – *muntlig*
2. Samvalg - *muntlig*
3. Orientering om framtidig utvikling av UNN Breivika og kommunal legevakt – *muntlig*
4. Nye hovedindikatorer 2022 - *muntlig*
5. Statusrapport oppfølging av handlingsplan for informasjonssikkerhet – *skriftlig (unntatt offentlighet)*
6. Orientering om internrevisjon fra Helse Nord RHF fra 2020 - behandling av personopplysninger i Universitetssykehuset Nord-Norge HF – *skriftlig*

Tromsø, 03.12.2021

Anita Schumacher (s.)
administrerende direktør

UNIVERSITETSSYKEHUSET NORD-NORGE
DAVVI-NORGGA UNIVERSITEHTABUOHCCEVIESSU

ORIENTERINGSSAK TIL STYRET

Møtedato:	16.12.2021
Arkivsak:	2020/4297-11
Saksbehandler:	Einar Bugge

Orientering om internrevisjon fra Helse Nord RHF fra 2020 - Behandling av personopplysninger i Universitetssykehuset Nord-Norge HF

Bakgrunn

Helse Nord RHFs internrevisjon har i perioden april-september 2020 utført en internrevisjon av de underliggende foretakenes behandling av personopplysninger. Formålet med revisjonen var å bekrefte at det enkelte sykehusforetak har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

Revisjonen fant vesentlige avvik, og presenterte viktige anbefalinger for Universitetssykehuset Nord-Norge HF (UNN) i rapporten.

Formål
Orientere styret om Helse Nord RHFs internrevisjonsrapport 07/20 *Behandling av personopplysninger i Universitetssykehuset Nord-Norge HF* og foretakets oppfølging av denne.

Saksutredning

Revisjonen hadde fire fokusområder:

- Hvorvidt helseforetakets oversikt over behandlingsaktiviteter (protokoll) er utarbeidet og inneholder påkrevd informasjon.
- Om det foreligger oppdaterte databehandleravtaler med leverandører som behandler personopplysninger på vegne av foretaket.
- Personvernombudets rolle og oppgaver.
- Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte.

Foretakets øvrige ansvar vedrørende informasjonssikkerhet og behandling av personopplysninger er ikke omfattet av revisjonen.

Revisjonens funn

1. Revisjonens observasjon er at UNN ikke kan legge frem en protokoll som overholder kravene i personvernforordningen. En protokoll er under utarbeidelse gjennom applikasjonen «Sureway», men det er ikke laget en fremdriftsplan for arbeidet. Revisjonen anser det som usikkert når tilfredsstillende protokoll vil foreligge, og anser det som hensiktsmessig å styrke oppfølgingen av arbeidet.
2. Internrevisjonen vurderer at Universitetssykehuset Nord-Norge har en god oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, og om det finnes en tilhørende databehandleravtale som regulerer dette.
3. Etter revisjonens vurdering framstår det som en mangel i henhold til den regionale retningslinjen RL6911 om organisering av informasjonssikkerhetsarbeidet i Helse Nord, at Universitetssykehuset Nord-Norge ikke har opprettet en egen beskrivelse av sin sikkerhetsorganisering, herunder en beskrivelse av personvernombudet.
4. Revisjonen observerer at det i UNN ikke er avklart hvordan protokollen og tilhørende oversikt over databehandleravtaler skal holdes oppdatert, når man har etablert og tatt i bruk den nye protokollen i Sureway. Videre understreker revisjonen viktigheten av å fastsette en løpende prosess for å holde protokollen oppdatert, når den tas i bruk.

Revisjonens anbefalinger for UNN

a) Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav.
b) Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll.
c) Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet
d) Etablere en løpende prosess for å holde protokollen oppdatert.

Vurdering

Revisjonens funn var alvorlige, og anbefalingene svært viktige å følge opp. Arbeidet med å utarbeide protokoll hadde pågått i lang tid også før revisjonen, men fremdriften har ikke vært tilfredsstillende. Det ble kort tid etter at revisjonsrapporten ble mottatt i UNN utarbeidet handlingsplan for å følge opp anbefalingene fra internrevisjonen.

Rapporten fra internrevisjonen faller i tid sammen med rapport fra Riksrevisjonen som også påpeker en rekke forhold som er nødvendig å forbedre for å sikre tilfredsstillende IKT-sikkerhet og personvern, og etterlevelse av gjeldende regelverk, i UNN. I sum er arbeidet på disse områdene over de siste årene blitt betydelig mer ressurskrevende, og selv om ressursbruken på området er styrket har ressurstilgangen ikke holdt tritt med behovet. Det har også vært mangler ved systematikken i arbeidet. Organiseringen av arbeidet med ikt-sikkerhet og personvern i UNN er endret med oppdelingen av det tidligere Kvalitets- og utviklingssenteret, og feltet er styrket.

UNN har over 600 systemer som innebærer behandling av personopplysninger. Det er et meget omfattende og detaljert arbeid å samle og systematisere nødvendig informasjon om alle systemene. Mange av disse systemene håndteres i klinikkene og senterne i UNN, og arbeidet krever et nært samarbeid mellom de rette ressurser i klinikkene og ressurser i stabsenhetene.

Hver klinikk/hvert senter utpekte en kontaktperson som personvernombudet og ikt-sikkerhetsansvarlig har forholdt seg til i arbeidet. Handlingsplanen la opp til at protokollen skulle være ferdigstilt før sommeren 2021, i tråd med krav i oppdragsdokumentet for UNN. Status i oppfølging av handlingsplanen har vært fulgt opp regelmessig av e-helse, samhandlings- og innovasjonssjefen (ESI-sjefen) og fag- og forskningssjefen. Fremdriften har vært tilfredsstillende, og hovedelementene i protokoll ble etablert i tråd med handlingsplanen. Alle de større systemene for behandling av personopplysninger er inkludert i protokollen.

Imidlertid har det vist seg krevende å få samlet inn tilstrekkelig detaljerte og nøyaktige opplysninger om alle de over 600 systemene som håndterer personopplysninger i UNN, særlig for de mange mindre systemene som benyttes lokalt i enkeltenheter/enkeltavdelinger, og der eierskapet til systemet også ligger lokalt. Protokollen er derfor fortsatt ikke fullstendig. Det er nødvendig å ha dedikerte ressurser til dette detaljerte og omfattende arbeidet i større grad enn vi har klart å avsette til nå. ESI-sjefen arbeider nå konkret for å få denne ressursen på plass, og arbeidet med protokollen vil bli høyt prioritert så snart ressursen er på plass. Vi er dog pr nå ikke i stand til å angi en sikker dato for når protokollen vil være helt ferdigstilt.

Prosessen med å utarbeide protokollen har tydeliggjort at det er en utfordring med at det er manglende tydelighet i hvilke enheter som eier de ulike systemer i UNN. Dette bidrar til å vanskeliggjøre arbeidet med å innhente opplysninger om, og få oversikt over behandlinger av personopplysninger i virksomheten. Denne utfordringen vil bli fulgt opp i det videre arbeidet med å informasjonssikkerhet i UNN, i samarbeid med Helse Nord IKT HF.

De tre øvrige anbefalingene fra internrevisjonen er fulgt opp; oppfølging av arbeidet med protokollen er styrket med regelmessig lederoppfølging, personvernombudets rolle er inkludert i beskrivelsen av foretakets organisering av informasjonssikkerhet og det er utarbeidet prosedyre med beskrivelse av løpende prosess for å holde protokollen oppdatert.

Konklusjon

Internrevisjonen fra Helse Nord RHF fra 2020 avdekket vesentlige forbedringsbehov i forhold til UNNs behandling av personopplysninger, primært i form av mangel på oppdatert og fullstendig protokoll. Handlingsplan for å følge opp internrevisjonens anbefalinger til UNN er utarbeidet og fulgt opp. Viktige elementer i protokollen er på plass, men det mangler fortsatt en del detaljerte opplysninger på særlig mindre systemer som brukes lokalt i enkeltenheter i UNN. Arbeidet med å fullføre protokollen styrkes og prioriteres de kommende måneder. Revisjonens øvrige anbefalinger er fulgt opp. Styret vil bli orientert om fremdrift i arbeidet med protokollen i statusrapporter for det omfattende arbeidet med å styrke informasjonssikkerheten i UNN utover i 2022.

Tromsø, 03.12.2021

Anita Schumacher (s.)
Administrerende direktør

Vedlegg

- Internrevisjonsrapport 07/2020 Behandling av personopplysninger i UNN

HELSE NORD

Internrevisjonsrapport 07/2020

Behandling av personopplysninger i Universitetssykehuset Nord-Norge HF

Internrevisjonen i Helse Nord RHF, 23.09.2020

Innholdsfortegnelse

Vedlegg:
1. Revisjonskriterier
2. Dokumentoversikt

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Universitetssykehuset Nord-Norge i perioden april - september 2020.

Formål og omfang av revisjonen
Formålet med revisjonen har vært å bekrefte at Universitetssykehuset Nord-Norge har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

Metoder
Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer.

Konklusjon
Universitetssykehuset Nord-Norge har ikke etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, slik de plikter i henhold til personvernforordningen. Det er usikkert når en tilfredsstillende protokoll kan legges fram. Foretaket har oversikt over inngåtte avtaler med aktører som behandler personopplysninger på dets vegne. Internrevisjonen vurderer at en rendyrking av personvernombudets rolle fra høsten 2020, i større grad vil sikre ombudets uavhengighet og redusere risikoen for interessekonflikter.

Anbefalinger
Internrevisjonen anbefaler Universitetssykehuset Nord-Norge å:
1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav.
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll.
3. Beskrive organiseringen av foretakets informasjonssikkerhetsarbeid, herunder personvernombudets rolle, i eget dokument.
4. Etablere en løpende prosess for å holde protokollen oppdatert.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i Universitetssykehuset Nord-Norge (UNN) i perioden april- september 2020. Internrevisor Hege Knoph Antonsen har vært oppdragsleder og revisjonssjef Janny Helene Aasen har hatt det overordnede ansvaret. Tilsvarende revisjon er gjennomført i alle regionens sykehusforetak.

Revisjonen har bestått av:
- Melding om internrevisjon sendt 24.04.2020
- Dokumentgjennomgang av interne dokumenter for UNN
- Intervjuer med sentrale nøkkelpersoner 08.06.-15.06.2020.
- Oppsummeringsmøte med UNN 27.08.2020.
- Rapportutkast sendt 27.08.2020, tilbakemelding mottatt 18.09.2020.

1.1 Bakgrunn

Den nye loven om behandling av personopplysninger (personopplysningsloven) trådte i kraft i juli 2018 og inkluderer EUs personvernforordning. Loven gjelder automatisert og ikke-automatisert behandling av personopplysninger. Det framgår av forordningen at den behandlingsansvarlige skal føre en protokoll over behandlingsaktivitetene som utføres under deres ansvar. Denne protokollen skal inneholde vesentlig informasjon om behandlingen. Behandlingsansvarlige som benytter seg av andre leverandører til å utføre behandlingsaktiviteter har plikt til å ha en databehandleravtale som regulerer dette. Forordningen stiller også krav om utpeking av personvernombud, og til personvernombudets stilling og oppgaver.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, Normen, er en bransjenorm detaljerer og supplerer gjeldende regelverk, og alle som er tilknyttet Norsk Helsenett er forpliktet til å følge den.

Oppdragsdokumentene fra Helse Nord RHF til helseforetakene i perioden 2017-2020, viser til at helseforetakene gjennom systematiske tiltak skal sørge for at nasjonale krav til personvern og informasjonssikkerhet blir ivaretatt. Det har vært stilt spesifikke krav om etablering av personvernombud i 2017, og om oversikt over databehandlere og innholdet i «ledelsens gjennomgang» i 2018.

1.2 Revisjonsgrunnlag

Følgende regelverk og nasjonale føringer er særlig aktuelle i denne revisjonen:
- LOV-2018-06-15-38, Lov om behandling av personopplysninger (personopplysningsloven), inkludert EUs personvernforordning 2016/679
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), v. 6.0

Regionale føringer:
- Oppdragsdokumentene fra Helse Nord RHF til HF-ene i årene 2017-2020
- DS6121, Felles styringssystem informasjonssikkerhet

2 Formål og omfang

2.1 Formål med revisjonen

Formålet med revisjonen har vært å bekrefte at Universitetssykehuset Nord-Norge har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

2.2 Omfang, fokusområder og avgrensninger

Revisjonen har omfattet og vært konsentrert om følgende fire fokusområder:
- Hvorvidt helseforetakets oversikt over behandlingsaktiviteter (protokoll) er utarbeidet og inneholder påkrevd informasjon.
- Om det foreligger oppdaterte databehandleravtaler med leverandører som behandler personopplysninger på vegne av foretaket.
- Personvernombudets rolle og oppgaver.
- Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte.

Innenfor hvert av fokusområdene er det definert revisjonskriterier basert på revisjonsgrunnlaget, jf. kap. 1.2. Disse er presentert samlet i *Vedlegg 1 – Revisjonskriterier*, samt innledningsvis i delkapitlene til kapittel 4. Revisjonskriteriene er de krav og forventninger som revisjonens observasjoner sammenlignes med.

Denne revisjonen har ikke omfattet foretakets øvrige plikter knyttet til informasjonssikkerhet og personvernforordningen.

3 Metoder

Følgende metoder er benyttet i revisjonsoppdraget:

Dokumentgjennomgang:
Dokumenter mottatt fra Universitetssykehuset Nord-Norge, eller innhentet fra foretakets websider, er gjennomgått og vurdert opp mot revisjonskriteriene, samt benyttet i forberedelser til intervjuene. Se *Vedlegg 2 – Dokumentoversikt.*

Intervjuer:
Det er gjennomført intervjuer med fire nøkkelpersoner i foretakets stabsfunksjoner.

4 Observasjoner og vurderinger

4.1 Helseforetakets protokoll over behandlingsaktiviteter

I henhold til personvernforordningens artikkel 30, skal helseforetaket føre en protokoll over behandlingsaktiviteter som utføres under dets ansvar. Protokollen skal inneholde navnet på og kontaktopplysningene til den behandlingsansvarlige, til den felles behandlingsansvarlige dersom det er relevant, og til personvernombudet. Videre skal blant annet følgende informasjon om behandlingsaktivitetene være registrert: kategorier av registrerte, kategorier av personopplysninger, formål og planlagt tidsfrist for sletting. Datatilsynet anbefaler at protokollen suppleres med tilleggsinformasjon som kilde, behandlingsgrunnlag og navn på databehandlere.

4.1.1 Observasjoner

Foretaket har lagt fram en protokoll med oversikt over IT-systemer med enkelte tilleggsopplysninger, som benyttes ved behandling av personopplysninger i UNN. Protokollen inneholder ikke opplysningene som personvernforordningen krever om den enkelte behandling, og heller ikke navn på behandlingsansvarlig og personvernombud.

I tillegg til framlagt protokoll har vi fått opplyst at det finnes en egen oversikt over det medisinsktekniske utstyret og dets behandling av personopplysninger, samt et separat register for meldinger om bruk av pasientinformasjon til forskning og kvalitetssikring. Internrevisjonen har ikke innhentet disse oversiktene.

Det pågår et arbeid med etablering av en behandlingsorientert protokoll ved hjelp av applikasjonen Sureway[1]. Her legges det opp til å inkludere alle påkrevde opplysninger, samt supplerende informasjon basert på Datatilsynets anbefalinger. Sykehusforetakene samarbeider om dette arbeidet, med bistand fra leverandøren av Sureway. Internrevisjonen er ikke kjent med at det foreligger formelle dokumenter som beskriver organiseringen av dette arbeidet (eksempelvis mandat). Det foreligger ikke en tidfestet framdriftsplan, og de vi intervjuet så ulikt på tidsperspektivet. Kvalitets- og utviklingssjefen som i dag er administrativt ansvarlig for sikkerhetssjef/personvernombud, ga uttrykk for at det er realistisk å få en protokoll ferdigstilt våren 2021, og at arbeidet er kritisk og må prioriteres.

Kvalitets- og utviklingssenteret er under omorganisering, med påfølgende endringer i roller og ansvarsdeling relatert til informasjonssikkerhet og personvern. Vi har fått opplyst at det etter omorganiseringen vil være ansvarlig for informasjonssikkerhet som skal sørge for å holde protokollen oppdatert. Organiseringen omtales nærmere i kap. 4.3.1.

[1] Sureway: personvernløsning (applikasjon) fra ekstern leverandør

4.1.2 Internrevisjonens vurderinger av protokollen

Internrevisjonen vurderer det som uheldig at foretaket ikke kan legge fram en behandlingsprotokoll i henhold til personvernforordningens krav, to år etter den nye personvernloven trådte i kraft. Vi anser den behandlingsorienterte protokollen som er under utvikling, som formålstjenlig, og legger til grunn at denne skal innfri forordningens krav når den er ferdigstilt. Vi vurderer imidlertid at det er usikkert når foretaket vil kunne legge fram en tilfredsstillende protokoll, ettersom det ikke er utarbeidet en framdriftsplan og det pågår omorganisering og utskifting av nøkkelpersoner. Det synes hensiktsmessig å styrke oppfølgingen av arbeidet med etablering av protokoll.

4.2 Databehandleravtaler

Dersom en databehandler skal utføre behandling av personopplysninger på vegne av foretaket, skal behandlingen være underlagt en skriftlig avtale. Personvernforordningens artikkel 28 stiller krav til inngåelse og innhold i slike avtaler.

4.2.1 Observasjoner

Personvernombudet kvalitetssikrer og fører oversikt over leverandører som behandler personopplysninger på foretakets vegne, med saksnummer til tilhørende databehandleravtale i arkivsystemet, Elements. Internrevisjonen har mottatt denne oversikten, som omfatter 119 avtaler hvor UNN er behandlingsansvarlig, og den angir status for den enkelte avtale. Det er imidlertid ingen kobling mellom avtaleoversikten og behandlingsprotokollen. Vi konstaterer at over halvparten av avtalene i oversikten har en merknad om at de bør erstattes av ny avtale slik at de tilfredsstiller kravene i personvernforordningen. Det er ikke etablert en systematisk prosess for slike fornyelser, men dette gjøres ved anledning eller behov. Vi fikk også opplyst at det mangler enkelte avtaler. Den regionale malen, eventuelt med enkelte modifikasjoner, benyttes når nye avtaler inngås.

Helse IKT HF er en viktig databehandler av helse- og personopplysninger, i og med at de drifter de fleste av regionens IKT-systemer. Siden 2018 har det pågått et arbeid med oppdatering av databehandleravtalene mellom Helse Nord IKT og helseforetakene, etter klare krav i oppdragsdokumentene for 2018 og 2019. Internrevisjonen konstaterer at det foreligger oppdatert, signert databehandleravtale mellom Universitetssykehuset Nord-Norge HF og Helse Nord IKT HF, utstedt 24.01.2020. UNNs sikkerhetssjef er oppgitt som kontaktperson i avtalen.

Det legges opp til at ny protokoll i Sureway skal inneholde opplysninger om databehandlere og lenke til aktuelle databehandleravtaler.

4.2.2 Internrevisjonens vurderinger av databehandleravtaler

Internrevisjonen vurderer at UNN har en god oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, og om det finnes en tilhørende

databehandleravtale som regulerer dette. Det ser ut til at protokollen som er under utvikling vil legge til rette for en god kobling av disse to oversiktene, når den er ferdigstilt. Vi viser videre til vurderingen i kap. 4.1.2.

4.3 Personvernombudets rolle og oppgaver

Personvernforordningen stiller i artikkel 37-39, en rekke krav relatert til personvern-ombudsrollen, blant annet at foretaket plikter å offentliggjøre aktuell kontakt-informasjon og at personvernombudet skal rapportere direkte til det høyeste ledelsesnivået i foretaket. Personvernombudet skal minst ha følgende oppgaver:

- informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har,
- kontrollere overholdelsen av personvernforordningen, annet regelverk og interne retningslinjer om personvern,
- på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den,
- samarbeide med tilsynsmyndigheten,
- fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, og ved behov rådføre seg med tilsynsmyndigheten.

Foretaket plikter å sikre at eventuelle andre oppgaver som personvernombudet utfører, ikke medfører interessekonflikt.

4.3.1 Observasjoner

UNN har etablert et team bestående av ansatte innenfor fagområdene personvern og informasjonssikkerhet, i tillegg til jurister, som omtales som «Personvern og informasjonssikkerhet i UNN» (PIU), men det finnes ikke et eget dokument som beskriver foretakets sikkerhetsorganisering, slik det er stilt krav om i Helse Nords regionale styringssystem for informasjonssikkerhet, RL6911.

Funksjonene personvernombud og sikkerhetssjef/informasjonssikkerhetsansvarlig ivaretas av samme person i en kombinert stilling. Personvernombudsrollen for Finnmarkssykehuset inngår også i denne stillingen (utleid i 30 % stilling). I stillingsinstruksen framkommer det at personvernombudet er administrativt og operativt underlagt kvalitets- og utviklingssjef, men rapporterer direkte til sikkerhetsledelsen v/administrerende direktør. Videre står det i stillingsinstruksen at personvernombudsrollen er avgrenset til forskning. Vi har imidlertid fått opplyst at funksjonen er definert i henhold til kravene i personvernforordningen, og at funksjonsbeskrivelsen burde vært oppdatert. Det ble gitt uttrykk for at personvern-ombudet har en uavhengig rolle og ikke opplever interessekonflikter som følge av den kombinerte stillingen. Vi konstaterer imidlertid at det er samme person som i rollen som informasjonssikkerhetsansvarlig skal sørge for at protokollen ajourføres, og som i rollen som personvernombud skal se til/kontrollere at den finnes og er oppdatert. Vi viser også til rolle- og oppgavebeskrivelser i kap. 4.2.1.

Internrevisjonen har sammenstilt mottatt informasjon om personvernombudets oppgaver, og konstaterer at forordningens oppgavekrav blir ivaretatt. På foretakets nettsider er det oppgitt navn og epostadresse til personvernombudet, og telefonnummer til sentralbordet.

Kvalitets- og utviklingssenteret skal deles i tre sidestilte sentre. I denne anledningen, og i forbindelse med at dagens personvernombud/sikkerhetssjef slutter 1. oktober 2020, vil personvernombudsrollen bli omgjort til en egen stilling, organisert i forsknings- og utdanningssenteret (ett av de nye senterne). Nytt personvernombud er ansatt og vil jobbe overlappende med dagens personvernombud en periode.

4.3.2 Internrevisjonens vurderinger av personvernombudets rolle og oppgaver

Internrevisjonen vurderer at det er etablert en personvernombudsordning i UNN i henhold til kravene i personvernforordningen, men at beskrivelsen av stillingen bør oppdateres. Vi anser det likevel som en svakhet at personvernombudsrollen kombineres med rolle som sikkerhetssjef/informasjonssikkerhetsansvarlig, da dette kan redusere personvernombudets uavhengighet. Pågående splitting av roller vurderes hensiktsmessig og vil styrke personvernarbeidet. Så snart organiseringen er avklart, bør dette beskrives i et eget dokument, slik det er stilt krav om i Helse Nords regionale styringssystem for informasjonssikkerhet, RL6911.

4.4 Foretakets prosesser for å holde protokollen og databehandler-avtalene oppdaterte

En løpende prosess er nødvendig for å holde protokollen og oversikt over databehandleravtaler oppdaterte. Minst én gang årlig skal foretakets ledelse gjennomgå og vurdere om styringssystemet innen informasjonssikkerhet og personvern fungerer som forutsatt, slik foretaket har fått føringer om i oppdragsdokumentene. «Ledelsens gjennomgang» skal også styrebehandles.

4.4.1 Observasjoner

Det er ikke avklart hvordan protokollen og tilhørende oversikt over databehandler-avtaler skal holdes oppdatert, når man har etablert og tatt i bruk den nye protokollen i Sureway. Vi har fått opplyst at dette har vært mye diskutert internt, og at oppdateringer ses på som utfordrende, særlig hvilken rolle klinikkene skal ha i dette arbeidet. Det vises også til informasjon i kap. 4.3.1 rundt framtidig oppgavefordeling.

Temaet informasjonssikkerhet og personvern inngikk i ledelsens gjennomgang for 2018, behandlet i styremøte september 2019 (sak 64-2019). Styret har behandlet egne styresaker om status i arbeidet med informasjonssikkerhet, herunder implementering av personvernforordningen i mai 2019 (sak 45-2019) og i mai 2020 (sak 45-2020).

I mai 2019 ble det formidlet til styret at man hadde et mål om å ha registrert behandlinger og fornyet gamle databehandleravtaler innen utgangen av 2019. I september 2019 ble det orientert om at prosessen pågikk, og i mai 2020 fikk styret informasjon om at arbeidet ikke var kommet så langt som planlagt. Utfordringer knyttet til organiseringen av fagområdene i PIU har også vært omtalt i de nevnte sakene, men i mai 2020 fikk styret informasjon om den pågående omorganiseringsprosessen og styrkingen av arbeidet med personvern og informasjonssikkerhet. Styret ba om ny statusinformasjon innen utgangen av mai 2021.

4.4.2 Internrevisjonens vurderinger av prosesser for oppdateringer

Internrevisjonen anser de separate statusorienteringene til styret som sidestilte med ledelsens gjennomgang i denne sammenhengen, og legger derfor til grunn at det har vært årlige gjennomganger innenfor temaet. Vi vurderer det imidlertid som en svakhet at styret ikke har fått oppdatert informasjon om når protokollen forventes ferdigstilt. Videre understreker vi viktigheten av å fastsette en løpende prosess for å holde protokollen oppdatert, når protokollen tas i bruk.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Universitetssykehuset Nord-Norge har ikke etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, slik de plikter i henhold til personvernforordningen. Det er usikkert når en tilfredsstillende protokoll kan legges fram. Foretaket har oversikt over inngåtte avtaler med aktører som behandler personopplysninger på dets vegne. Internrevisjonen vurderer at en rendyrking av personvernombudets rolle fra høsten 2020, i større grad vil sikre ombudets uavhengighet og redusere risikoen for interessekonflikter.

5.2 Anbefalinger

Internrevisjonen anbefaler Universitetssykehuset Nord-Norge å:

1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav.
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll.
3. Beskrive organiseringen av foretakets informasjonssikkerhetsarbeid, herunder personvernombudets rolle, i eget dokument.
4. Etablere en løpende prosess for å holde protokollen oppdatert.

Vedlegg 1 – Revisjonskriterier

Følgende fokusområder og kriterier er lagt til grunn for internrevisjonens arbeid og vurderinger:

1. Helseforetakets protokoll over behandlingsaktiviteter
    a. Det foreligger en samlet oversikt (protokoll) over foretakets behandlingsaktiviteter.
    b. Oversikten (protokollen) inneholder navnet på og kontaktopplysningene til:
    -den behandlingsansvarlige
    -den felles behandlingsansvarlige (dersom det er relevant)
    -personvernombudet.
    c. Registrert informasjon om behandlingsaktivitetene omfatter blant annet: kategorier av registrerte (a), kategorier av personopplysninger (a), formål (a), kilde (b), behandlingsgrunnlag (b), navn på databehandlere (b) og planlagt tidsfrist for sletting (a)
    a: krav i personvernforordningen / b: anbefaling fra Datatilsynet

2. Databehandleravtaler
    a. Det foreligger databehandleravtale med databehandlere som er identifisert i foretakets protokoll over behandlingsaktiviteter.
    b. Avtalen er oppdatert i samsvar med kravene i personvernforordningen.

3. Personvernombudets rolle og oppgaver
    a. Kontaktopplysninger til personvernombudet er offentliggjort på foretakets webside.
    b. Personvernombudet rapporterer direkte til foretaksdirektør.
    c. Personvernombudets oppgaver inkluderer de som er påkrevd gjennom forordningen.
    d. Personvernombudet har ikke andre oppgaver som kan medføre interessekonflikt.

4. Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte
    a. Foretaket har etablert en løpende prosess for å holde behandlingsoversikten oppdatert.
    b. «Ledelsens gjennomgang» innen informasjonssikkerhet og personvern gjennomføres minst en gang i året.

Vedlegg 2 – Dokumentoversikt

Oversikt over dokumenter som er gjennomgått i forbindelse med revisjonen.

- Erklæring om behandling av personopplysninger ved Universitetssykehuset Nord-Norge (UNN), https://unn.no/om-oss/om-nettstedet/personvern#sykehusets-personvernombud, hentet 24.04.2020
- Oversendelsesbrev til Internrevisjonen i Helse Nord RHF, 18.05.2020
- Protokoll over systemer som inneholder personopplysninger (excel-liste), per 18.05.2020
- Oversikt over databehandlere og databehandleravtaler, mottatt 25.08.2020
- Stillingsinstruks for sikkerhetssjef/personvernombud, versjon 6
- Styresak 45-2019, Oppfølging risikovurdering av informasjonssikkerhet, unntatt offentlighet
- Styresak 64-2019, Ledelsens gjennomgang 2018
- Status i arbeidet, grunnlagsnotat til regionalt direktørmøte 11.03.2020
- Presentasjon «Workshop – Informasjonssikkerhet, Hva er de viktigste sikkerhetsutfordringer for ledere i UNN», ledermøtesak 67.20, 28.04.2020
- Styresak 45-2020, Status i oppfølging av risikovurderinger av informasjonssikkerhet, unntatt offentlighet
- Referat fra møter i regionalt nettverk for personvernombud 15.04.2020 og 20.05.2020
- Avtale om behandling av personopplysninger, Databehandleravtale, mellom Universitetssykehuset Nord-Norge HF og Helse Nord IKT HF, utstedt 24.01.2020