Styresak 107/2020
Vedlegg 1

HELSE NORD

Internrevisjonsrapport 09/2020

Behandling av personopplysninger i Helgelandssykehuset HF

Internrevisjonen i Helse Nord RHF, 25.09.2020

Innholdsfortegnelse

Vedlegg:
1. Revisjonskriterier
2. Dokumentoversikt

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Helgelandssykehuset i perioden april - september 2020.

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

Metoder
Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer.

Konklusjon
Helgelandssykehuset har etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, men innholdet i protokollen tilfredsstiller ikke alle kravene i personvernforordningen. Foretaket har ikke en oversikt over om det er inngått databehandleravtaler med alle aktører som behandler personopplysninger på dets vegne. Det er usikkert når en tilfredsstillende protokoll, inkludert oversikt over databehandlere, kan legges fram. Personvernombudsordning er etablert, men rollens oppgaver er noe uklart definert.

Anbefalinger
Internrevisjonen anbefaler Helgelandssykehuset å:
1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll og databehandleravtaler.
3. Oppdatere beskrivelsen av foretakets organisering av informasjonssikkerhet, herunder personvernombudets rolle.
4. Etablere en løpende prosess for å holde protokollen oppdatert.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i Helgelandssykehuset 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 Helgelandssykehuset
- Intervjuer med sentrale nøkkelpersoner 03.06-05.06.2020.
- Oppsummeringsmøte med Helgelandssykehuset 19.08.2020.
- Rapportutkast sendt 27.08.2020, tilbakemelding mottatt 17.09.2020.

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 Helgelandssykehuset 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 Helgelandssykehuset, 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 tre 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 benytter applikasjonen Sureway[1], for å holde oversikt over behandlingsaktivitetene og har lagt fram en protokolloversikt som viser hvilke datasystemer og kvalitetsregistre som er registrert her, samt hvilken sektor/avdeling som forvalter de enkelte systemene/registrene. Vi fikk opplyst at grunnlaget for denne oversikten er en kartlegging som ble utført i 2018, og at man anser oversikten over systemer/registre som rimelig komplett, men med enkelte kjente mangler. Det er lagt opp til at protokollen skal inneholde opplysningene som personvernforordningen krever om den enkelte behandling, inkludert navn på behandlingsansvarlig og personvernombud, og for 44 % av systemene/registrene finnes det detaljerte opplysninger om behandlingen.

Vi har fått opplyst at det foreligger en egen oversikt over behandling av personopplysninger som del av forskningsaktiviteten, men vi har ikke innhentet denne.

Det pågår et arbeid med omlegging fra en systemorientert til en behandlingsorientert protokoll. 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), og det foreligger ikke en tidfestet framdriftsplan.

4.1.2 Internrevisjonens vurderinger av protokollen

Internrevisjonen konstaterer at foretaket har etablert en systemorientert protokoll over sin behandling av personopplysninger, men at denne mangler en del av opplysningene som personvernforordningen krever. Vi anser den behandlingsorienterte protokollen som er under utvikling, som mer formålstjenlig, og legger til grunn at denne skal innfri forordningens krav når den er ferdigstilt. Vi vurderer imidlertid at det er usikkert når

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

foretaket vil kunne legge fram en tilfredsstillende protokoll, ettersom det ikke er utarbeidet en framdriftsplan. Det synes hensiktsmessig å styrke styringen med oppfølgingen av arbeidet med etablering av ny 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

Vi har fått opplyst at foretaket ikke har en oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket og tilhørende databehandleravtaler, og at man ikke stoler på at spesifikke søk i arkivsystemet, Elements, gir korrekt informasjon om hvorvidt avtale finnes. Videre ble vi gjort kjent med at det er behov for å fornye en del av avtalene, slik at de tilfredsstiller kravene i personvernforordningen, men at man vil prioritere å skaffe oversikt over status først. Den regionale malen benyttes når nye avtaler inngås, så fremst man klarer å få gjennomslag for dette i forhandlinger med databehandleren. Personvernombudet opplyste at hun involveres i prosessen når det skal inngås nye regionale avtaler, men sjelden når det dreier seg om lokale avtaler.

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 Helgelandssykehuset og Helse Nord IKT, utstedt 24.01.2020. Helgelandssykehusets informasjonssikkerhets-rådgiver er oppgitt som kontaktperson i avtalen.

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

4.2.2 Internrevisjonens vurderinger av databehandleravtaler

Internrevisjonen vurderer det som uheldig at foretaket ikke kan legge fram en oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, med tilhørende informasjon om hvorvidt det finnes en gyldig databehandleravtale som regulerer dette. Det ser ut til at protokollen som er under utvikling vil legge til rette for en god oversikt over dette, 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

Personvernombudet er organisert i Senter for Fag, forskning og utdanning, men det vurderes om stillingen skal flyttes til organisasjonsdirektør fra høsten 2020. Det er avsatt en halv stilling til denne rollen, som kombineres med en halv stilling knyttet til generell juridisk rådgivning. På foretakets nettsider er det oppgitt navn og epostadresse til personvernombudet, og telefonnummer til sentralbordet. Det er ikke utarbeidet stillingsbeskrivelse for personvernombudet.

Den regionale retningslinjen RL6911, Organisering av informasjonssikkerhetsarbeidet i Helse Nord, stiller krav om et eget dokument som beskriver foretakets sikkerhets-organisering, herunder personvernombudets rolle. Helgelandssykehuset har utarbeidet et slikt dokument, RL2033, men dette har ikke vært oppdatert siden 2010 og personvernombudet er ikke nevnt.

Internrevisjonen har sammenstilt mottatt informasjon om personvernombudets oppgaver, og vi konstaterer at forordningens oppgavekrav i hovedsak blir ivaretatt.. Vi fikk imidlertid opplyst at det ikke er en klar oppgavefordeling mellom personvernombud og informasjonssikkerhetsrådgiver i arbeidet med protokoll, men at de samarbeider om dette arbeidet. Videre fikk vi opplyst at man anser rådgivnings-oppgaven som den viktigste, og at personvernombudet blir konsultert i enkeltsaker.

4.3.2 Internrevisjonens vurderinger av personvernombudets rolle og oppgaver

Internrevisjonen vurderer at det er etablert en personvernombudsordning i Helgelands-sykehuset i henhold til kravene i personvernforordningen. Vi anser det imidlertid som svakheter at det ikke finnes en stillingsbeskrivelse eller lignende som synliggjør hva rollen innebærer, og at det heller ikke finnes en oppdatert beskrivelse av sikkerhetsorganiseringen i Helgelandssykehuset der også personvernombudet omtales.

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, behandlings-orienterte oversikten. Det vises også til informasjon i kap. 4.3.1 om uklarheter i oppgavefordeling mellom personvernombud og informasjonssikkerhetsrådgiver.

Temaet informasjonssikkerhet og personvern inngikk i ledelsens gjennomgang for 2018, styrebehandlet i sak 75-2018. Styret har også behandlet egne styresaker om status innen informasjonssikkerhet, herunder arbeidet med personvern og protokoll, i mai 2019 (sak 48-2019) og mai 2020 (sak 43-2020). I mai 2020 framkom det at det pågår et regionalt arbeid med felles oppbygging av protokoll og at det gjenstår arbeid med innholdet i protokollen. Styresaken inneholdt ingen informasjon om planlagt tidspunkt for ferdigstillelse av protokollen.

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 informasjon om når protokollen forventes ferdigstilt. Videre understreker vi viktigheten av å fastsette en løpende prosess for å holde protokollen oppdatert, når ny protokoll tas i bruk. Det er derfor uheldig at ansvarsfordelingen ikke oppleves avklart.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Helgelandssykehuset har etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, men innholdet i protokollen tilfredsstiller ikke alle kravene i personvernforordningen. Foretaket har ikke en oversikt over om det er inngått databehandleravtaler med alle aktører som behandler personopplysninger på dets vegne. Det er usikkert når en tilfredsstillende protokoll, inkludert oversikt over databehandlere, kan legges fram. Personvernombudsordning er etablert, men rollens oppgaver er noe uklart definert.

5.2 Anbefalinger

Internrevisjonen anbefaler Helgelandssykehuset å:

1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll og databehandleravtaler.
3. Oppdatere beskrivelsen av foretakets organisering av informasjonssikkerhet, herunder personvernombudets rolle.
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.

- Personvernerklæring om hvordan personopplysninger samles inn og brukes på Helgelandssykehuset HF, https://helgelandssykehuset.no/om-oss/om-nettstedet/personvernerklering#sykehusets-personvernombud, hentet 27.04.2020
- Oversendelsesbrev til Internrevisjonen i Helse Nord RHF, 15.05.2020
- Protokolloversikt for Helgelandssykehuset per 13.05.2020, og tilhørende eksempel
- RL2033, Sikkerhetsledelse Helgelandssykehuset HF - applikasjonsoversikt, versjon 1 (2010)
- Sikkerhetsrevisjon 2017, 13.06.2017
- Styresak 75/2018, Vedlegg 2, Ledelsens gjennomgang 2018
- Styresak 48/2019, Informasjonssikkerhet. Status risiko- og sårbarhetsanalyse
- Styresak 43/2020, Informasjonssikkerhet Helgelandssykehuset - status, unntatt offentlighet
- Avtale om behandling av personopplysninger, Databehandleravtale, mellom Helgelandssykehuset HF og Helse Nord IKT HF, utstedt 24.01.2020