Møtedato: 28. oktober 2020

Arkivnr.:	Saksbeh:	Sted/Dato:
2020/531	Janny Helene Aasen	Bodø, 20.10.2020

Styresak 136-2020 Internrevisjonsrapport nr. 11/2020: Behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering

Formål
Internrevisjonen i Helse Nord RHF har gjennomført en revisjon hvor formålet har vært 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 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.
- Helseforetakets prosesser for å holde protokollen og databehandleravtalene oppdaterte.

I denne styresaken legges den oppsummerende rapporten fra revisjonen fram for styret i Helse Nord RHF.

Sammenheng med grunnleggende verdier
Grunnlovens § 102 fastslår at enhver har rett til *respekt* for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Personopplysningsloven stiller krav til virksomheter slik at den enkelte skal oppleve *trygghet* for at personopplysningene behandles som forutsatt. For å sikre pasienter, pårørende og ansatte sine rettigheter, er det viktig at det er *kvalitet* i sykehusforetakenes oversikter over behandling av personopplysninger og tilhørende rutiner. Internrevisjonen vurderer at det er positivt at dette arbeidet videreutvikles i et *samspill* mellom sykehusforetakene.

Beslutningsgrunnlag
Internrevisjonens konklusjon
Tre av sykehusforetakene i Helse Nord har ikke etablert en behandlingsprotokoll som tilfredsstiller personvernforordningens krav, to år etter ikrafttredelsen. Det er usikkert når tilfredsstillende protokoller vil foreligge. To av helseforetakene har heller ikke en oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om

det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudsordninger er etablert, men rollens oppgaver er noe uklart definert i enkelte av foretakene.

Internrevisjonens anbefalinger
Internrevisjonen har, i rapportene til de enkelte helseforetakene, gitt følgende anbefalinger:

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. Inkludere personvernombudet i beskrivelsen av helseforetakets organisering av informasjonssikkerhet.
4. Finnmarkssykehuset: Oppdatere avtalen om kjøp av personvernombudstjenester i henhold til ny personopplysningslov.
5. UNN/Finnmarkssykehuset/Helgelandssykehuset: Etablere en løpende prosess for å holde protokollen oppdatert.

Behandling i styrets revisjonsutvalg
Revisjonsutvalget er holdt løpende orientert om gjennomføringen av revisjonen, sist i møte 23. september 2020 (sak 17/20), hvor utvalget vedtok:

1. *Revisjonsutvalget er tilfreds med orienteringen.*
2. *Revisjonsutvalget anbefaler at det i styresaken legges opp til forslag til vedtak som inkluderer at styret får følgende tilbakemeldinger om oppfølgingen av internrevisjonens anbefalinger:*
   a. *Foretakenes framdriftsplaner (jf. anbefaling 1) legges fram for styret innen utgangen av desember 2020.*
   b. *Bekreftelse på at internrevisjonens øvrige anbefalinger er fulgt opp, og at påpekte svakheter er håndtert, legges fram for styret innen utgangen av juni 2021.*

Adm. direktørs vurdering
Adm. direktør viser til internrevisjonens konklusjon og anbefalinger, og til revisjonsutvalgets behandling av rapporten. Revisjonsrapporten viser at tre av sykehusforetakene har mangler som ikke anses å være i samsvar med personvern-forordningen, men at det er behov for forbedringer hos alle. Det er derfor viktig at hvert sykehusforetak utarbeider handlingsplan for oppfølging av internrevisjonens anbefalinger, jf. krav i *Tilleggsliste til Oppdragsdokument 2020*, pkt. 9.2.

Styret i Helse Nord RHF inviteres til å fatte følgende vedtak:

1. Styret i Helse Nord RHF tar *Internrevisjonsrapport nr. 11/2020, behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering*, til orientering.

2. Styret forutsetter at alle sykehusforetakene følger opp internrevisjonens anbefalinger, og ber adm. direktør sørge for at styret får følgende tilbakemeldinger om oppfølgingen av disse:
   a. Helseforetakenes framdriftsplaner (jf. anbefaling 1) legges fram for styret innen utgangen av desember 2020.
   b. Bekreftelse på at internrevisjonens øvrige anbefalinger er fulgt opp, og at påpekte svakheter er håndtert, legges fram for styret innen utgangen av juni 2021.

Bodø, den 20. oktober 2020

Cecilie Daae
adm. direktør

Vedlegg:
Internrevisjonsrapport 11/2020: Behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering

HELSE NORD

Internrevisjonsrapport 11/2020

Behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering

Internrevisjonen i Helse Nord RHF, 25.09.2020

Innholdsfortegnelse

Vedlegg:
1. Revisjonskriterier

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Universitetssykehuset Nord-Norge, Finnmarkssykehuset, Helgelandssykehuset og Nordlandssykehuset i perioden april - september 2020.

Formål og omfang av revisjonen
Formålet med revisjonen har vært 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.

Metoder
Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer.

Konklusjon
Tre av sykehusforetakene i Helse Nord har ikke etablert en behandlingsprotokoll som tilfredsstiller personvernforordningens krav, to år etter ikrafttredelsen. Det er usikkert når tilfredsstillende protokoller vil foreligge. To av foretakene har heller ikke en oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudsordninger er etablert, men rollens oppgaver er noe uklart definert i enkelte av foretakene.

Anbefalinger
Internrevisjonen har, i rapportene til de enkelte foretakene, gitt hvert foretak følgende tre til fem anbefalinger:

1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.[1]
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll og databehandleravtaler.
3. Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet.
4. FIN: Oppdatere avtalen om kjøp av personvernombudstjenester i henhold til ny personopplysningslov.
5. UNN/FIN/HSYK: Etablere en løpende prosess for å holde protokollen oppdatert.

[1] Anbefalingen har en mer begrenset ordlyd til to av foretakene.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i regionens sykehusforetak i perioden april-september 2020. Internrevisor Hege Knoph Antonsen har vært oppdragsleder og revisjonssjef Janny Helene Aasen har hatt det overordnede ansvaret.

Denne rapporten oppsummerer revisjonene i helseforetakene, rapportert som følger:

- Universitetssykehuset Nord-Norge HF (UNN), IR-rapport 07/2020, 23.09.2020
- Finnmarkssykehuset HF (FIN), IR-rapport 08/2020, 23.09.2020
- Helgelandssykehuset HF (HSYK), IR-rapport 09/2020, 25.09.2020
- Nordlandssykehuset HF (NLSH), IR-rapport 10/2020, 23.09.2020

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 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.

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 foretakenes øvrige plikter knyttet til informasjonssikkerhet og personvernforordningen.

3 Metoder

Følgende metoder er benyttet i revisjonsoppdraget:

Dokumentgjennomgang:
Dokumenter mottatt fra foretakene, eller innhentet fra deres websider, er gjennomgått og vurdert opp mot revisjonskriteriene, samt benyttet i forberedelser til intervjuene. Dokumentoversikter følger de foretaksvise rapportene som vedlegg.

Intervjuer:
Det er gjennomført intervjuer med tre-fire nøkkelpersoner i hvert foretaks 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

Det enkelte foretaket har lagt fram sin protokoll over behandling av personopplysninger. Alle foretakene har en protokoll som er innrettet etter IT-system. I varierende grad mangler det påkrevd informasjon hos alle. Finnmarkssykehusets protokoll er bare en liste over IT-systemene som benyttes i foretaket, mens Nordlands-sykehuset har en detaljert oversikt som i hovedsak innfrir forordningens krav.

Det pågår et arbeid med omlegging fra en systemorientert til en behandlingsorientert protokoll ved hjelp av applikasjonen Sureway[2]. 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 ingen av foretakene har utarbeidet en tidfestet framdriftsplan.

4.1.2 Internrevisjonens vurderinger av protokollen

Internrevisjonen vurderer det som uheldig at tre av foretakene ikke kan legge fram en behandlingsprotokoll i henhold til personvernforordningens krav, to år etter at den nye personopplysningsloven trådte i kraft. Vi anser de behandlingsorienterte protokollene som er under utvikling, som mer formålstjenlige, og legger til grunn at disse skal innfri forordningens krav når de er ferdigstilt. Vi vurderer imidlertid at det er usikkert når tilfredsstillende protokoller vil foreligge, ettersom det ikke er utarbeidet framdriftsplaner. Det synes hensiktsmessig å styrke oppfølgingen av arbeidet med etablering av protokoll i det enkelte foretaket.

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

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

Universitetssykehuset Nord-Norge og Nordlandssykehuset har oversikt over leverandører som behandler personopplysninger på deres vegne, med statusinformasjon om tilhørende databehandleravtaler og saksnummer i arkivsystemet, Elements. Fra Finnmarkssykehuset og Helgelandssykehuset fikk vi opplyst at man ikke har en slik oversikt. Vi har videre fått opplyst at avtaler fra 2018 og eldre bør fornyes slik at de tilfredsstiller kravene i personvernforordningen, men at foretakene ikke har etablert systematiske prosesser for slike fornyelser. 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 oppdaterte, signerte databehandleravtaler mellom det enkelte sykehusforetaket og Helse Nord IKT HF, alle utstedt 24.01.2020.

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 at Universitetssykehuset Nord-Norge og Nordlandssykehuset har en god oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, og om det finnes en tilhørende databehandleravtale som regulerer dette.
Vi vurderer det som uheldig at de andre to sykehusforetakene ikke har en slik oversikt. Det ser ut til at protokollen som er under utvikling vil legge til rette for en god integrering av informasjon om databehandlere, jf. vurderingen i kap. 4.1.2.

4.3 Personvernombudets rolle og oppgaver

Personvernforordningen stiller i artikkel 37-39, en rekke krav relatert til personvernombudsrollen, blant annet at foretaket plikter å offentliggjøre aktuell kontaktinformasjon, 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

I Universitetssykehuset Nord-Norge har funksjonene personvernombud og sikkerhetssjef/informasjonssikkerhetsansvarlig blitt ivaretatt av samme person i en kombinert stilling, men fra 1. oktober 2020 vil funksjonene splittes og personvernombudsrollen blir egen stilling. Finnmarkssykehuset kjøper personvernombudstjenesten fra Universitetssykehuset Nord-Norge og har inngått egen avtale som regulerer dette. Oppdraget utgjør ca. 30 % stilling. Helgelandssykehuset og Nordlandssykehuset har tilsatt personvernombud i stillingsstørrelse på henholdsvis 50 % og 100 %. På foretakenes nettsider er det oppgitt navn, epostadresse og telefonnummer direkte til personvernombudet.

Noen av foretakene har utarbeidet en egen beskrivelse av personvernombudets rolle og oppgaver, eksempelvis i form av en stillingsbeskrivelse eller som del av avdelingens organisasjonsplan. Tjenesteavtalen mellom Universitetssykehuset Nord-Norge og Finnmarkssykehuset er utarbeidet i henhold til gammel personvernlovgivning, og avtaleteksten bidrar til at oppgavedelingen mellom personvernombud og informasjonssikkerhetsrådgiver oppleves noe uavklart når det gjelder utarbeidelse og vedlikehold av protokollen. Heller ikke i Helgelandssykehuset er det en klar oppgavefordeling mellom disse to funksjonene.

Internrevisjonen har sammenstilt mottatt informasjon om personvernombudets oppgaver i det enkelte foretaket og konstaterer at forordningens oppgavekrav i hovedsak blir ivaretatt. Det er imidlertid noe ulikt hvordan oppgaven med å kontrollere overholdelse av regelverk og interne personvernretningslinjer blir ivaretatt, ut over i enkeltsaker der personvernombudet blir konsultert. I Nordlandssykehuset er det innarbeidet i foretakets revisjonsplan at personvernombudet skal gjennomføre interne revisjoner innenfor temaet.

Personvernombudet i Nordlandssykehuset er i tillegg tillagt oppgaven med «å føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene» og har hovedansvaret for at denne er oppdatert.

Den regionale retningslinjen RL6911, Organisering av informasjonssikkerhetsarbeidet i Helse Nord, stiller krav om et eget dokument som beskriver foretakets sikkerhetsorganisering, inkludert personvernombudets rolle. Tre av foretakene har utarbeidet et

slikt dokument, uten at personvernombudet er nevnt i dette. Universitetssykehuset Nord-Norge har ikke opprettet eget dokument om sin sikkerhetsorganisering.

4.3.2 Internrevisjonens vurderinger av personvernombudets rolle og oppgaver

Internrevisjonen vurderer at foretakene har etablert personvernombudsordninger i henhold til kravene i personvernforordningen, men at noen av foretakene bør oppdatere sin beskrivelse av funksjonen. Vår vurdering forutsetter at det operative ansvaret med å føre og oppdatere protokollen som personvernombudet er tillagt i Nordlandssykehuset, ikke medfører interessekonflikter. Vi anser det som avgjørende at det er behandlingsansvarlige som beslutter formålet med behandlingsaktivitetene og melder fra om oppføringer og endringer i protokollen til personvernombudet.

Vi anser det som en svakhet at personvernombudsrollen i Universitetssykehuset Nord-Norge hittil har blitt kombinert med rolle som sikkerhetssjef/informasjonssikkerhetsansvarlig, da dette kan ha redusert personvernombudets uavhengighet. Pågående splitting av roller vurderes hensiktsmessig og vil styrke personvernarbeidet.

Det framstår 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, samt at de øvrige foretakene ikke omtaler personvernombudet i sine beskrivelser.

4.4 Foretakets prosesser for å holde protokollen og databehandleravtalene 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

I tre av foretakene er det ikke avklart hvordan protokollen og tilhørende oversikt over databehandleravtaler skal holdes oppdatert, når man har etablert og tatt i bruk den nye protokollen i Sureway. Det vises også til informasjon i kap. 4.3.1 om uklarheter i oppgavefordeling mellom personvernombud og informasjonssikkerhetsrådgiver i noen av foretakene.

Nordlandssykehuset har prosedyrefestet at dersom bruken av personopplysningene opphører eller endres, må den enkelte behandlingsansvarlige («melderen») sende endringsinformasjon til personvernombudet. Personvernombudet i Nordlandssykehuset er tillagt hovedansvaret for at protokollen er oppdatert, slik det tidligere er opplyst i kap. 4.3.1.

Temaet informasjonssikkerhet og personvern inngikk i «Ledelsens gjennomgang for 2018», som har blitt styrebehandlet i alle foretakene. Styrene har også behandlet status innen informasjonssikkerhet, herunder arbeidet med personvern og protokoll, i mai 2020. Her fikk styrene informasjon om at det pågår et arbeid om oppbygging av det enkelte foretaks protokoll, og at dette gjøres i nært samarbeid mellom sykehusforetakene i Helse Nord. Styresakene inneholdt ingen informasjon om planlagt tidspunkt for ferdigstillelse av protokollen.

4.4.2 Internrevisjonens vurderinger av prosesser for oppdateringer

Internrevisjonen anser separat statusorientering til styrene om temaet informasjonssikkerhet og personvern som sidestilt med «Ledelsens gjennomgang», og legger derfor til grunn at det har vært årlige gjennomganger innenfor temaet. Vi vurderer det imidlertid som en svakhet at styrene 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 den tas i bruk.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Tre av sykehusforetakene i Helse Nord har ikke etablert en behandlingsprotokoll som tilfredsstiller personvernforordningens krav, to år etter ikrafttredelsen. Det er usikkert når tilfredsstillende protokoller vil foreligge. To av foretakene har heller ikke en oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudsordninger er etablert, men rollens oppgaver er noe uklart definert i enkelte av foretakene.

5.2 Anbefalinger

Internrevisjonen har, i rapportene til de enkelte foretak, gitt følgende anbefalinger (tall = anbefalingens nummer i den enkelte HF-rapport):

Anbefaling	*UNN*	*FIN*	*HSYK*	*NLSH*
Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.		1	1	
Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav	1			1*
Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll.	2	2	2	2*
Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet	3	3	3	3
Oppdatere avtalen om kjøp av personvernombudstjenester i henhold til ny personopplysningslov.		4		
Etablere en løpende prosess for å holde protokollen oppdatert.	4	5	4	

*Anbefalingen har en mer begrenset ordlyd.

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.