AKERSHUS UNIVERSITETSSYKEHUS

Styresak

Dato dok.:	08.02.2021	Administrerende direktør	
Møtedato:	17.02.2021		
Vår ref.:	20/01666-21	Postadresse:	1478 LØRENSKOG
		Telefon:	+47 67 96 00 00
Vedlegg:	Revisjonsrapport		

Sak 04/21 Revisjon fra konsernrevisjonen Helse Sør-Øst om behandling av personopplysninger

Konsernrevisjonens revisjon av protokoll for behandling av personopplysninger ble påbegynt i mars 2020, men ble midlertidig innstilt grunnet koronasituasjonen. Revisjonen ble gjenopptatt i september, og ble sluttført i desember 2020.

Revisjonen tar for seg to spørsmål:

1) *Har helseforetaket på en helhetlig og hensiktsmessig måte organisert ansvar og oppgaver for forvaltning av en protokoll over behandling av personopplysninger?*
2) *Har helseforetaket utarbeidet en samlet oversikt over egen behandling av personopplysninger hvor blant annet behandlingsansvar, behandlingsaktiviteter og systemer framgår?*

Etter Konsernrevisjonens vurdering har Akershus universitetssykehus etablert en protokoll som ivaretar personopplysningslovens grunnleggende krav til oversikt over behandlingsaktiviteter. Det er gitt to anbefalinger for å bidra til at protokollen som helhet skal gi et enda bedre grunnlag for styring og kontroll med behandlingen av personopplysninger, og for å redusere risiko for mangelfull informasjon.

Forbedringsarbeidet knyttet til anbefalingene har startet, men det gjenstår gjennomføring på noen planlagte aktiviteter.

Administrerende direktørs innstilling til vedtak:

Styret tar saken til orientering.

Øystein Mæland
Administrerende direktør

Dokumentet er elektronisk godkjent

Bakgrunn
Etter personvernforordningens artikkel 30 har Akershus universitetssykehus som dataansvarlig institusjon, plikt til å føre en protokoll over egne databehandlinger. Dette ansvaret fremgår også av oppdrag og bestilling fra Helse Sør-Øst for 2019, der det presiseres at helseforetakene har et selvstendig ansvar for at det føres protokoll over behandlingsaktivitetene knyttet til personopplysninger.

Akershus universitetssykehus har i forbindelse med GDPR-prosjektet som ble gjennomført i forkant av ny personopplysningslov, etablert en protokoll for behandling av personopplysninger. Kartleggingen og registreringen som ble gjennomført i 2019 har ikke vært gjenstand for løpende oppdateringer eller justeringer. Protokollen er utarbeidet i Excel, med utgangspunkt i Datatilsynets anbefalte mal. Protokollen gir en oversikt over behandlinger av personopplysninger på det tidspunktet da dette arbeidet ble gjennomført.

Sykehuspartner har i sitt oppdrags- og bestillingsdokument for 2019 fått ansvar for å utvikle en protokoll som alle helseforetakene i regionen skal ta i bruk. Høsten 2020 startet Sykehuspartner jobben med å føre inn de første helseforetakenes databehandlinger i den regionale protokollen.

Målet for revisjonen var å vurdere om Akershus universitetssykehus har utarbeidet en samlet oversikt over vår behandling av personopplysninger, og om helseforetaket har etablert prosesser for å holde oversikten oppdatert.

Revisjonen viste følgende:
1. Det er etablert en protokoll som ivaretar grunnleggende krav. Protokollen består av tre deler som dekker hvert sitt område. Det er konsernrevisjonens vurdering at helseforetakets protokoll sett i sammenheng med helseforetakets samlede rutiner for behandling av personopplysninger, dokumenterer kartlagte behandlingsaktiviteter og ivaretar grunnleggende krav til informasjon i samsvar med Datatilsynets anbefalte mal og veiledning.
2. Tydeligere formål vil gi et bedre grunnlag for styring og kontroll med behandlingen av personopplysninger
3. Det er en forutsetning at Akershus universitetssykehus ferdigstiller rutinen som skal beskrive ansvar, oppgaver og tidsfrister, slik at protokollen fortløpende kan oppdateres med aktuell informasjon om behandlingsaktivitetene.
4. Store deler av ansvaret for behandling av personopplysninger er plassert lokalt i linjeorganisasjonen. Ansvaret for en foretaksovergripende protokoll er sentralt. Koordinering av det lokale og det sentrale ansvaret har ikke helt funnet sin form. Det gjenstår for Akershus universitetssykehus å konkretisere en forvaltningsmodell med operasjonaliserte rutiner som samordner roller og ansvar med hensyn til forvaltning av protokollen.

På bakgrunn av funnene kommer Konsernrevisjonen med to anbefalinger:
1. Konsernrevisjonen anbefaler at Akershus universitetssykehus prioriterer videreutviklingen av protokollen som helhet, slik at den gir relevant og nyttig informasjon om alle behandlingsaktiviteter. Helseforetaket bør i tillegg ta stilling til om det oppbevares personopplysninger i fagsystemer og på filområder som ikke er dokumentert i protokollen. Helseforetaket bør også ta stilling til om det er et tydelig formål knyttet til alle behandlingsaktiviteter, og om disse har behov for differensiering med hensyn til behandlingsgrunnlag, sikkerhetstiltak, og behov for risiko- og personvernkonsekvensvurderinger i protokollen.
2. Konsernrevisjonen anbefaler at Akershus universitetssykehus operasjonaliserer oppfølgingsansvaret for protokollen. Den planlagte forvaltningsrutinen for protokollen bør beskrive ansvar, oppgaver og tidsfrister som bereder grunnen for at protokollen

fortløpende kan holdes oppdatert med aktuell informasjon om nye og endrede behandlingsaktiviteter. Rutinen bør innføres som en del av kvalitetssystemet når den er ferdigstilt.

Høsten 2020, og før revisjonen var ferdigstilt og rapport forelå, ble følgende tiltak gjennomført:

- Systemeierskapet for artikkel 30-protokoll ble lagt til viseadministrerende direktør ved foretakssekretariatet som systemforvalter.
- I budsjett 2021 ble det opprettet en stilling for å styrke arbeidet med å forbedre oversikten over alle systemer med personopplysninger, og raskt kunne identifisere systemer som blir utsatte ved ulike sikkerhetshendelser.
- Det er tilsatt en person i stillingen med oppstart 1. mars.
- Akershus universitetssykehus er i dialog med Sykehuspartner om eventuell ibruktakelse og utvikling av regional protokoll.

<u>På bakgrunn av revisjonen vil det igangsettes følgende tiltak knyttet til anbefaling 1:</u>

- Vurdering, utvikling og implementering av egnet protokoll for å sikre ivaretakelse av foretakets ansvar for behandling av personopplysninger;
- Gjennomgang av og eventuell differensiering av formålsbeskrivelsene knyttet til alle behandlingsaktiviteter;
- Gjennomgang av filområder med tanke på å avdekke behandling av personopplysninger som skal registreres i protokollen.

<u>På bakgrunn av revisjonen vil det igangsettes følgende tiltak knyttet til anbefaling 2:</u>

- Prosedyre som beskriver roller og ansvar for registrering, oppdatering og kontroll med protokoll over behandlingsaktiviteter;
- Rutine for registrering og regelmessig oppdatering av protokollen;
- Lage veileder for utfylling som revideres etter behov og minst hvert annet år;
- Opplæring av ansvarlige eller de som er gitt oppgaven å registrere behandlinger, med generell veiledning rundt behandling av personopplysninger.

Arbeidet med dette vil starte i mars, når den nyansatte medarbeideren har tiltrådt stillingen.

HELSE SØR-ØST

Konsernrevisjonen
Rapport 7/2020

Protokoll for behandling av personopplysninger

Akershus universitetssykehus HF

22. desember 2020

Introduksjon

Den nye loven om behandling av personopplysninger (personopplysningsloven) trådte i kraft i juli 2018. EUs personvernforordning er dermed norsk lov. Loven gjelder automatisert og ikke-automatisert behandling av personopplysninger.

Det fremgår av personopplysningsloven at den behandlingsansvarlige skal føre en protokoll over behandlingsaktivitetene som utføres under deres ansvar, og dermed er dette både et krav og en plikt for foretaket. Denne protokollen skal inneholde vesentlig informasjon om behandlingen og er å anse som støttedokumentasjon for omkringliggende prosesser som risikovurderinger og avvikshåndtering, og ved behov for å informere de registrerte om behandlingsaktiviteter og behandlingsgrunnlag.

Konsernrevisjonen kartla i 2018 status for arbeidet med å tilpasse prosessene for behandling av personopplysninger i helseforetakene i Helse Sør-Øst. Kartleggingen viste at helseforetakene var i ferd med å kartlegge behandlingsaktiviteter og oppgradere internkontrollsystemer og rutiner i tråd med kravene som fremkommer av loven. Helseforetakene var kommet ulikt i tilpasningsarbeidet, og prosesser og organisasjon hadde ikke funnet sin varige form på området.

Oppdrags- og bestillingsdokumentene til helseforetakene for 2019 viser til at helseforetakene har et selvstendig ansvar for at det føres protokoll over behandlingsaktivitetene knyttet til personopplysninger.

Målet for denne revisjonen er å vurdere om helseforetaket har utarbeidet en samlet oversikt over sin behandling av personopplysninger og om helseforetaket har etablert prosesser for å holde oversikten oppdatert. I dette inngår at organisering og ansvarsdeling er tydelig definert, og at helseforetaket har en behandlingsoversikt som er i samsvar med kravene i personopplysningsloven.

Revisjonen har to problemstillinger:

1. Har helseforetaket på en helhetlig og hensiktsmessig måte organisert ansvar og oppgaver for forvaltning av en behandlingsoversikt?
2. Har helseforetaket utarbeidet en samlet oversikt over egen behandling av personopplysninger hvor blant annet behandlingsansvar, behandlingsaktiviteter og systemer framgår?

Revisjonen ble påbegynt mars 2020, men ble midlertidig innstilt i på grunn av at Akershus universitetssykehus HF gikk i beredskap som følge av Covid-19. Revisjonen ble gjenopptatt i september og pågikk fram til desember 2020.

INNHOLD

1. Konklusjoner og anbefalinger

1.1 Protokoll som ivaretar grunnleggende krav – men med behov for styrket forvaltning

Akershus universitetssykehus HF (Ahus) har utarbeidet en protokoll som ivaretar personopplysningslovens grunnleggende krav til oversikt over behandlingsaktiviteter. De underliggende strukturene for forvaltning er etablert gjennom definerte roller med ansvars- og oppgavefordeling som er styrt gjennom et rammeverk bestående av styrende, gjennomførende og kontrollerende dokumentasjon. Foretaket har siden den nye personvernloven trådte i kraft i 2018 oppgradert sine styrings- og internkontrollprosesser for å ivareta krav til personvern og informasjonssikkerhet. Dette gjelder blant annet ledelsens gjennomgang og årlig gjennomgang av internkontroll, som inkluderer vurderinger på personvern- og informasjonssikkerhetsområdet, risikovurderinger, personvernkonsekvensvurderinger og avvikshåndtering.

Ahus har utformet et system for å ivareta helseforetakets ansvar med henblikk på behandling av personopplysninger. Behandling av personopplysninger er en integrert del av det foretaksovergripende styringssystemet for virksomhetsstyring og internkontroll. Personvernet er dokumentert i styrende, gjennomførende og kontrollerende dokumentasjon. Dokumentasjonen ivaretar ansvarsplassering, roller, oppgaver, avvikshåndtering og rapportering. Det samlede systemet skal gi en rimelig sikkerhet for at behandlingen av personopplysninger er i samsvar med lovverket og at de registrertes rettigheter blir ivaretatt av foretaket. Protokollen er et ledd i dette og skal gi informasjon om behandlingsaktivitetene.

Den samlede vurderingen er at protokollen legger til rette for å ivareta kravene til informasjon om blant annet formål, behandlingsgrunnlag og behandlingsaktiviteter i henhold til personopplysningslovens artikkel 30.

For at protokollen som helhet skal gi et enda bedre grunnlag for styring og kontroll med behandlingen av personopplysninger, og for å redusere risiko for mangelfull informasjon, er det et behov for å styrke den systematiske forvaltningen noe. Den samlede vurderingen begrunnes med følgende:

- det er etablert en protokoll som ivaretar grunnleggende krav
- tydeligere formål vil gi et bedre grunnlag for styring og kontroll med behandlingen av personopplysninger
- rutine for regelmessig oppdatering av protokollen må ferdigstilles
- ansvaret for forvaltning av protokollen bør operasjonaliseres.

Det er etablert en protokoll som ivaretar grunnleggende krav

Ahus har en protokoll som skal gi oversikt over behandlingen av personopplysninger i helseforetaket. Protokollen ble utarbeidet i forbindelse med GDPR-prosjektet. Prosjektet ble gjennomført for å implementere de nye kravene som personvernforordningen stiller til helseforetaket.

Protokollen består av tre deler som dekker hvert sitt område. Del 1 omfatter helsehjelp og består av behandlingsaktiviteter knyttet til pasientbehandling. Del 2 er en generell del og omfatter i hovedsak administrative formål. Del 3 omfatter behandlingsaktiviteter knyttet til forsknings- og innovasjonsprosjekter. Del 1 og 2 er sammenfattet i et regneark, og del 3 er integrert i et helhetlig fagsystem for forskningsstøtte ved Ahus (eSkjema).

De tre delene har i ulik grad vært gjenstand for systematisk forvaltning. Delen som omfatter forskning og innovasjon, er lengst framskreden ved at helseforetaket har utviklet en løsning som dokumenterer formålet med

behandling av personopplysninger knyttet til forskningsprosjekter og kvalitetsstudier i hele behandlingsaktivitetens livsløp. Etter konsernrevisjonens vurdering har det vært en riktig prioritering å utvikle denne løsningen, siden dette reduserer risikoen for at personopplysninger behandles i prosjekter uten et avklart rettslig grunnlag. Mangfoldige prosjekter i kombinasjon med et desentralt forvaltningsansvar for disse, gjør at iboende risiko i utgangspunktet er relativt høy på dette området. De øvrige delene av protokollen har i mindre grad vært gjenstand for systematisk forvaltning med løpende vedlikehold av behandlingsaktivitetene. Dette kan delvis tilskrives lav endringstakt på noen områder. For eksempel har HR-området bestått av relativt stabile prosesser, fagsystemer, organisatorisk struktur og regelverk siden protokollen ble etablert. Stabile miljøer gir relativt få endringer som må oppdateres i protokollen.

Det er konsernrevisjonens vurdering at Ahus' protokoll sett i sammenheng med helseforetakets samlede rutiner for behandling av personopplysninger, dokumenterer kartlagte behandlingsaktiviteter og ivaretar grunnleggende krav til informasjon i samsvar med Datatilsynets anbefalte mal og veiledning. Vurderingen bygger på at Ahus har utformet et internkontrollsystem for å ivareta helseforetakets ansvar med henblikk på behandling av personopplysninger. Videre inneholder helseforetakets protokoll, som en del av dette systemet, informasjon om formålet med behandlingen, kategorier av registrerte, overføring av personopplysninger til en tredjestat samt tekniske og organisatoriske sikkerhetstiltak.

Tydeligere formål vil gi et bedre grunnlag for styring og kontroll med behandlingen av personopplysninger

Protokollen ble i sin tid utarbeidet av et prosjekt og overlevert til linjen for videre forvaltning. I foretakets protokoll har virksomheten definert overordnende formål per behandling. Dette suppleres videre med angivelse av informasjon om hva behandlingen gjelder og overordnet behandlingsaktivitet. Mer gjennomarbeidet struktur og mer detaljert informasjon om behandlingsaktivitetene kan gi bedre innsikt i risiko og hvordan den registrertes rettigheter blir ivaretatt gjennom tilpassede sikkerhetstiltak, nødvendige risiko- og personvernkonsekvensvurderinger og avviksoppfølging. For at protokollen skal gi ytterligere merverdi og fungere som dokumentasjon i en utvidet sammenheng, bør den innrettes slik at ytterligere relevant støtteinformasjon blir en del av protokollen, for eksempel risiko- og sikkerhetsnivå, avvik og informasjon om risiko- og personvernkonsekvensvurderinger.

Rutine for regelmessig oppdatering av protokollen må ferdigstilles

Over tid vil det vil være endringer i behandlingsaktiviteter som må dokumenteres som en del av en samlet oversikt over behandlingsaktivitetene (protokoll). Det er en forutsetning at Ahus ferdigstiller rutinen som skal beskrive ansvar, oppgaver og tidsfrister slik at protokollen fortløpende kan oppdateres med aktuell informasjon om behandlingsaktivitetene.

Ansvaret for forvaltning av protokollen bør operasjonaliseres

Store deler av ansvaret for behandling av personopplysninger er plassert lokalt i linjeorganisasjonen. Ansvaret for en foretaksovergripende protokoll er sentralt. Koordinering av det lokale og det sentrale ansvaret har ikke helt funnet sin form. Dette har medført at deler av protokollen i mindre grad har vært gjenstand for en systematisk oppfølging og forvaltning med oppdatering av relevant informasjon, og det kan være en risiko for at enkelte behandlingsaktiviteter ikke er dokumentert i tilstrekkelig omfang. Det gjenstår for Ahus å konkretisere en forvaltningsmodell med operasjonaliserte rutiner som samordner roller og ansvar med hensyn til forvaltning av protokollen.

1.2 Anbefalinger

Konsernrevisjonen har to anbefalinger. Den første anbefalingen handler om videreutvikling av selve protokollen og den andre handler om en forsterket forvaltning av protokollen med hensyn til operasjonalisering av ansvar samt at vedlikeholdsrutinen ferdigstilles.

Videreutvikle protokollen

Protokollen ble i sin tid utarbeidet av et prosjekt og overlevert til linjen for videre forvaltning. Siden overleveringen har den videre forvaltningen av de ulike delene vært gjenstand for ulik prioritering i helseforetaket. Konsernrevisjonen anbefaler at helseforetaket prioriterer videreutviklingen av protokollen som helhet slik at den gir relevant og nyttig informasjon om alle behandlingsaktiviteter. Dette kan gi bedre innsikt i risiko og hvordan den registrertes rettigheter blir ivaretatt. I denne sammenhengen bør helseforetaket i tillegg ta stilling til om det oppbevares personopplysninger i fagsystemer og på filområder som ikke er dokumentert i protokollen.

Helseforetaket bør også ta stilling til om det et tydelig formål knyttet til alle behandlingsaktiviteter og om disse har behov for differensiering med hensyn til behandlingsgrunnlag, sikkerhetstiltak, og behov for risiko- og personvernkonsekvensvurderinger i protokollen.

Styrke forvaltningen av protokollen

Konsernrevisjonen anbefaler at Ahus operasjonaliserer oppfølgingsansvaret for protokollen. Forsterket ressursinnsats og tydeliggjøring av ansvar vil legge til rette for bedre samordning av det sentrale ansvaret for den foretaksovergripende protokollen med det det lokale ansvaret for behandling av personopplysninger. Dette vil videre tilrettelegge for at nivået og systematikken i forvaltningen av protokollen blir konsistent på tvers av hele helseforetaket.

Det er planlagt for å utarbeide en forvaltningsrutine i Ahus for protokollen. Rutinen skal ligge til grunn for en systematisk forvaltning og bør beskrive ansvar, oppgaver og tidsfrister som bereder grunnen for at protokollen fortløpende kan holdes oppdatert med aktuell informasjon om nye og endrede behandlingsaktiviteter. Rutinen bør innføres som en del av kvalitetssystemet når den er ferdigstilt.

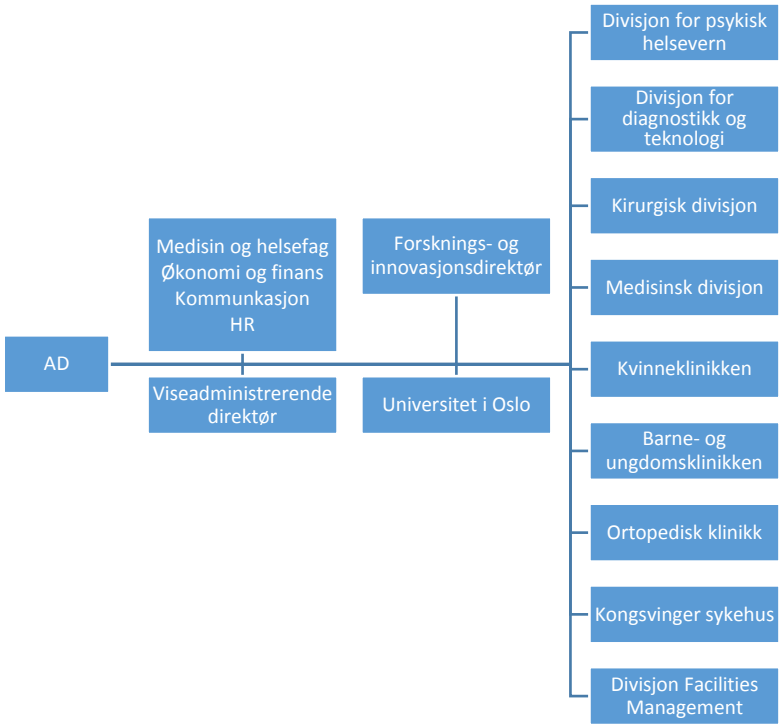
2. Kontekst

2.1 Akershus universitetssykehus HF

Organisering og virksomhetsområder

Akershus universitetssykehus HF er et lokal- og områdesykehus for cirka 560 000 innbyggere. Hovedoppgavene er pasientbehandling, forskning, undervisning og pasientopplæring.

Akershus universitetssykehus HF er organisert med ni divisjoner og klinikker i tillegg til stabsfunksjoner, se figuren under.



Figur 1: Akershus universitetssykehus HF – organisasjonskart

Styringssystem for virksomhetsstyring og internkontroll

Retningslinjen for virksomhetsstyring og internkontroll beskriver virksomhetsstyring og internkontroll ved Akershus universitetssykehus HF og styringssystemet "Orden i eget Ahus". Orden i eget Ahus er et styringssystem som inkluderer alle gjeldende prosedyrer for virksomhetsstyring og internkontroll, se vedlegg 3. Retningslinjen er det overordnende styrende dokumentet som øvrige prosedyrer og rutiner i virksomheten skal bygge på.

Styrende dokumenter og prosedyrer er kommunisert i foretaket og gjort tilgjengelig gjennom dokument- og avvikshåndteringssystemet EQS.

Retningslinje for personvern

Ahus har utarbeidet en overordnet retningslinje for personvern som gjelder alle virksomhetsområder. Retningslinjen er et styrende dokument som skal sikre foretakets etterlevelse av personvernregelverket.

Retningslinjen beskriver overordnende føringer og prinsipper, roller og ansvar og viser til øvrige prosedyrer som gjelder på personvernområdet innenfor ulike områder.

Ledelsessystem for informasjonssikkerhet

Til grunn for styring av informasjonssikkerhet ved Ahus ligger det regionale felles ledelsessystemet for informasjonssikkerhet i Helse Sør-Øst og Norm for informasjonssikkerhet i helse- og omsorgstjenesten. Gjennom dette skal virksomhetens arbeid med informasjonssikkerhet styres slik at helse- og personopplysninger blir behandlet i samsvar med gjeldende krav. Informasjonssikkerhet er en del av Akershus universitetssykehus HFs styringssystem og omfatter all behandling av helse- og personopplysninger i helseforetaket.

Strategi for personvern og informasjonssikkerhet

Ahus har utarbeidet en strategi for personvern og informasjonssikkerhet for perioden 2019 - 2022. Strategien er et styrende dokument og skal bidra til planmessig og strukturert arbeid på overordnet nivå for å nå målene innen personvern og informasjonssikkerhet. Med strategien som utgangspunkt utarbeides årlige handlingsplaner for personvern og informasjonssikkerhet.

Tilnærming til nye lovregler – GDPR-prosjektet

I forbindelse med innføringen av den nye personopplysningsloven i 2018 etablerte Ahus et prosjekt – GDPR-prosjektet – for å kartlegge tilstanden for behandling av personopplysninger og hva som var manglende for at behandlingen av personopplysninger ved helseforetaket skulle være i samsvar med det nye lovverket. Rutiner og systemer har blitt omarbeidet på bakgrunn av prosjektets anbefalinger. Prosjektet ble avsluttet i desember 2018 og gjenstående aktiviteter overført til linjen. Etter prosjektets avslutning har den videre innsatsen vært særlig rettet mot forskning og innovasjon og mot medisinteknisk utstyr.

Personvernerklæring i foretaket

Ahus har gjort personvernerklæringen sin tilgjengelig på helseforetakets internettsider. Der opplyser foretaket om hvem som er dataansvarlig, hvilke personopplysninger som lagres, innsynsrett og behandlingsgrunnlag. Det er videre informasjon om utlevering av personopplysninger og hvem som er personvernombud på helseforetaket.

2.2 Personopplysninger i et helseforetak

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Typiske personopplysninger er navn, adresse, telefonnummer, e-postadresse og fødselsnummer. Biologiske mønstre av for eksempel fingeravtrykk og iris er også personopplysninger. Videre kan bilder og lydopptak under visse omstendigheter være personopplysninger.

Særlige kategorier av personopplysninger – helseopplysninger

I personvernforordningen er det definert særskilte kategorier av personopplysninger. Helseopplysninger er en av disse kategoriene.

Rettigheter og plikter

Helsetjenester er generelt gjenstand for omfattende lovregulering. Lovverket setter mål og rammer for helseforetakenes innsamling og behandling av personopplysninger. Personopplysningsloven fastsetter at personvernforordningen gjelder som norsk lov. Personvernforordningen fastlegger rettigheter og plikter med hensyn til personvern og informasjonssikkerhet, og skal legges til grunn ved all behandling av helseopplysninger.

Personvernforordningen krever at all behandling av personopplysninger har rettslig grunnlag i forordningen og eventuelt i norsk lov. Dersom det etter norske regler er lov til å behandle opplysningene, kan det legges til grunn at dette gir tilstrekkelig grunnlag også etter forordningen. Det er relevante regler i pasientjournalloven, helseregisterloven, helseforskningsloven mv. og i flere forskrifter.

Behandlingsgrunnlag i forbindelse med helsehjelp

Det følger av *pasientjournalloven* § 19 at helseforetaket skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell, når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp.

Av *spesialisthelsetjenesteloven* § 3-2 følger det at helseforetak skal sørge for at journal- og informasjonssystemene ved institusjonen er forsvarlige.

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten fastlegger at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter. Virksomheten skal ha et styringssystem der aktiviteter

planlegges, gjennomføres, evalueres og korrigeres. Det skal omfatte oversikt over og beskrive virksomhetens mål, oppgaver, aktiviteter og organisering. Fordeling av ansvar, oppgaver og myndighet skal klart framgå og videre skal det systematiske arbeidet for kvalitetsforbedring og pasient- og brukersikkerhet i virksomheten være beskrevet.

Det er videre rettsregler for personopplysninger til bruk i læringsarbeid og kvalitetssikring regulert i *helsepersonelloven*, *pasientjournalloven* og *pasientjournalforskriften*. Deling av forskningsdata og publisering av forskningsresultater reguleres i *helseforskningsloven* og *helsepersonelloven*.

Dataansvarlig (behandlingsansvarlig)

Enhver behandling av helseopplysninger må kunne knyttes til en behandlingsansvarlig, jamfør personvernforordningen artikkel 4 nr. 7. Behandlingsansvarlig betegnes dataansvarlig i helselovgivningen. Ingen kan behandle helseopplysninger uten at det er klart hvem som er dataansvarlig. Det er helseforetaket som er dataansvarlig, og det er den dataansvarlige som har ansvaret for personvernet ved behandling av helseopplysninger. Den dataansvarlige har også ansvaret for at de registrerte får oppfylt sine personvernrettigheter.

(Avsnitt *2.2 Personopplysninger på et helseforetak* bygger på rundskriv I-3/2019 *Informasjonshåndtering i spesialisthelsetjenesten*, Helse- og omsorgsdepartementet.)

2.3 Krav til behandlingsprotokoll

Akershus universitetssykehus HF skal som behandlingsansvarlig føre en protokoll over behandlingsaktivitetene, jamfør personvernforordningen artikkel 30. Dette er også omtalt i forordningens fortale (82): For å påvise samsvar med denne forordning bør den behandlingsansvarlige eller databehandleren føre protokoll over de behandlingsaktiviteter som de har ansvar for.

Artikkel 24 fastslår at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

I protokollen skal det være informasjon om blant annet:

- formålet med behandlingen
- kategoriene av registrerte og kategoriene av personopplysninger
- kategoriene av mottakere som personopplysningene utleveres til
- generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak.

En behandling av personopplysninger innebærer all bruk av personopplysninger (f.eks. innsamling, lagring, utlevering etc.) som gjøres for ett og samme formål.

Målet med behandlingsprotokollen er å bidra til etterlevelse av virksomhetens plikter og de registrertes rettigheter. Protokollen vil gjøre det enklere å besvare forespørsler fra pasienter og andre brukere som vil vite hva virksomheten har registrert om dem, hvor virksomheten har fått opplysningene fra, og med hvilket rettslig grunnlag virksomheten behandler opplysningene etter. Protokollen er også nyttig når foretaket skal oppfylle den aktive informasjonsplikten ved utarbeidelse av en personvernerklæring.

Datatilsynets mal for standard protokoll oppfyller minimumskravene etter personvernforordningen. Ikke desto mindre er det andre opplysninger, for eksempel om risikovurderinger, som er nødvendig for å kunne vurdere om man behandler personopplysningene i samsvar med regelverket. Dette er opplysninger som kan dokumenteres i protokollen for å gi bedre oversikt over behandlingen av personopplysninger. Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. All behandling av personopplysninger i virksomheten skal dokumenteres i en protokoll, jamfør personvernforordningen art. 30, nr. 1. Virksomheten må kunne vise til skriftlig dokumenta-

sjon som viser at prinsippene overholdes for alle behandlinger av personopplysninger som utføres av virksomheten, jamfør personvernforordningen art. 5, nr. 2. Virksomheten må gi alle registrerte informasjon om innsamling og behandlingen av personopplysninger, jamfør personvernforordningen, art. 13 og 14.

I tillegg har Sykehuspartner HF en selvstendig plikt som databehandler å føre protokoll over alle kategorier av behandlingsaktiviteter som utføres på vegne av Ahus, jamfør personvernforordningen artikkel 30, nr. 2. Denne protokollen skal gi informasjon om kategoriene av behandling utført på vegne av behandlingsansvarlig. Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at databehandler behandler personopplysningene kun på dokumenterte instrukser fra den behandlingsansvarlige.

3. Tilnærming

3.1 Metodisk tilnærming

Revisjonen er gjennomført ved bruk av dokumentundersøkelser og intervjuer. Oversikt over intervjuer og dokumentasjon framgår av vedleggene 1 og 2.

3.2 Omfang og avgrensning

Revisjonen har omfattet følgende områder:

- hvordan oppgaver og ansvaret for behandling av personopplysninger er definert, fordelt og implementert i helseforetaket
- rutiner for behandling av personopplysninger hos databehandler samt databehandleravtaler med dokumentasjon i protokoll
- rutiner som er etablert for å vedlikeholde oversikt over behandling av personopplysninger
- rutiner for risikovurderinger
- rutiner for sletting av personopplysninger samt dokumentasjon i protokoll
- rutiner for avvikshåndtering på personvernområdet
- sletting.

Det er også vurdert om helseforetaket har tilrettelagt for å samordne behandlingsoversikten med standardiserte prosesser i helseregionen, jamfør styringskravene i oppdrags- og bestillerdokumentet for 2019.

I Helse Sør-Øst har alternative modeller for regional og lokal oppgave--deling med hensyn til personvernombudsrollen vært til utredning i revisjonsperioden. På den bakgrunn har konsernrevisjonen avgrenset vurderingene knyttet til personvernombudet til å omfatte lovpålagte oppgaver og ansvar, og således ikke vurdert momenter som berører en eventuell oppgavedeling mellom lokale og regionale funksjoner.

Revisjonen har omfattet prosesser med roller og ansvar for at Ahus skal ha en oppdatert behandlingsprotokoll. Testing for å verifisere fullstendigheten av behandlingsoversikten har ikke vært en del av revisjonen.

3.3 Revisjonskriterier

Revisjonen har lagt til grunn følgende revisjonskriterier:

- Helseforetakets aktiviteter og oppgaver på personvernområdet er satt i system og er en del helseforetakets overordnede styringsprosesser. Virksomheten har etablert:
  - en risikobasert tilnærming for å vurdere behandlingsaktiviteter
  - et helhetlig rammeverk som dekker relevante prosesser, systemer og områder som behandler personopplysninger
  - relevante organisatoriske og tekniske tiltak for informasjonssikkerhet.
- Helseforetakets behandling av personopplysninger er definert, kjent og kommunisert med relevante aktører.
- Virksomheten har en periodisk oppfølging av etablerte prosesser som angår personvernområdet.
- Oppfølging av tiltak og handlingsplaner relatert til personvernområdet inngår i virksomhetens overordnende rapportering.

4. Organisering av ansvar og oppgaver

Revisjonen har undersøkt om styring og kontroll i Ahus er hensiktsmessig innrettet for behandling av personopplysninger. I dette inngår hvordan organisasjon, ansvar og roller er strukturert i prosesser som er tilpasset oppgavene som skal utføres. Revisjonen har gjennomgått dokumenterte roller og prosesser med helseforetakets øverste ledelse og med andre aktuelle, mer operasjonelle aktører i helseforetaket.

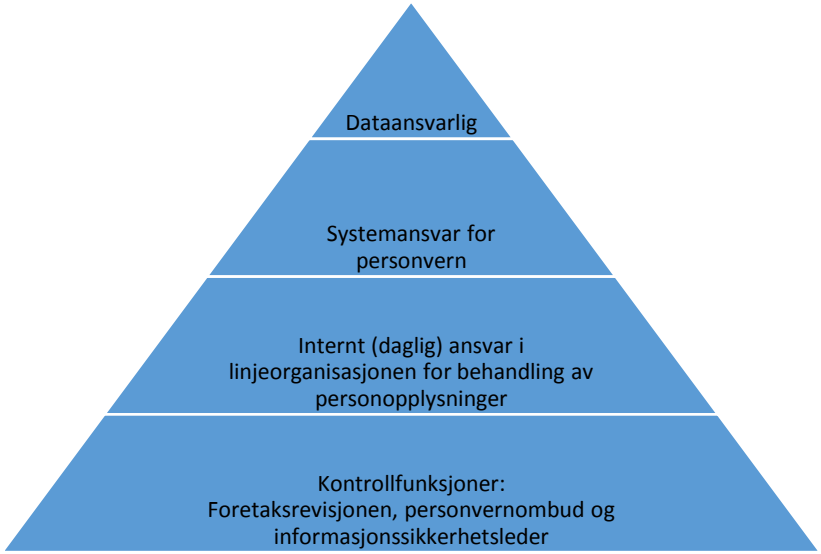
4.1 Observasjoner

Observasjonene er knyttet til følgende områder:

- modell for organisering av personvernarbeidet
- organisasjon
- retningslinjer og prosedyrer
- roller og ansvar
- rapportering til styret og ledergruppen

Modell for organisering av personvernarbeidet

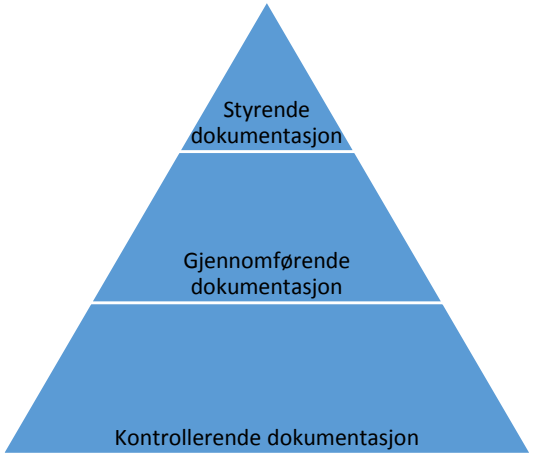
På et overordnet nivå bygger virksomhetsstyringen i Akershus universitetssykehus HF på definerte mål gitt av eier i oppdrags- og bestillingsdokumentet, strategisk plan for foretaksgruppen, samt målene i Ahus' strategiske plan og utviklingsplan. Med dette som bakteppe behandles personopplysninger etter følgende forenklede modell.



Figur 2: Modell for organisering av personvern

Akershus universitetssykehus HF er dataansvarlig. Daglig leder (administrerende direktør) har internt fordelt ansvar og oppgaver som dataansvaret innebærer. Et spesifikt internt ansvar for et helhetlig system som styrer og kontroller prosessene for all behandling av personopplysninger er plassert til viseadministrerende direktør. Videre er operativt ansvar fordelt i linjeorganisasjonen og støttefunksjoner.

Et styringssystem for personvern kan generelt deles i tre nivåer. Det vises til Datatilsynets veiledning om etablering av internkontroll, som for øvrig nevner at internkontroll i ulike sammenhenger kalles et kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk.



Figur 3: Dokumenthierarki

1. Styrende dokumentasjon retter seg i hovedsak mot ledelsen, herunder beslutninger og føringer ledelsen legger for internkontroll.
2. Gjennomførende dokumentasjon retter seg i hovedsak mot medarbeiderne, herunder beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.
3. Kontrollerende dokumentasjon bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Konsernrevisjonen har mottatt dokumentasjon på alle de tre nivåene fra Ahus.

Organisasjon

Daglig leder i Akershus universitetssykehus HF er administrerende direktør som sammen med viseadministrerende direktør og divisjons-, klinikk og stabsdirektørene utgjør helseforetakets ledelse.

Foretakssekretariatet er en foretaksovergripende støttefunksjon for personvern og informasjonssikkerhet under viseadministrerende direktørs ansvarsområde. Personvernombudet og informasjonssikkerhetsleder er innplassert i foretakssekretariatet, og enheten skal utvides ytterligere med en foretaksjurist som skal virke innenfor personvernområdet. I tillegg har stabsfunksjonen *Forskning og innovasjon* to personvernrådgivere.

Roller og ansvar

Administrerende direktør har det øverste ansvaret for virksomheten i Ahus. Helseforetaket har etablert en modell med intern ansvarsdeling til leder på nivå to (divisjonsdirektører og tilsvarende). I tillegg er det tverrgående roller og funksjoner med egnede definerte ansvarsområder som understøtter det sentrale og lokale lederansvaret.

Dataansvarlig

Ahus er dataansvarlig og administrerende direktør er øverste ansvarlige for organiseringen av personvernarbeidet på helseforetaket. Administrerende direktør godkjenner behandlingsprotokollen.

Det overordnede systemansvaret i Ahus for behandlingen av personopplysninger er plassert til viseadministrerende direktør. Direktøren er ansvarlig for at nødvendige styrende, gjennomførende og kontrollerende rutiner innen personvern er utarbeidet.

Internt ansvarlige og systemeier

Divisjons-, klinikk og stabsdirektørene og andre ledere på nivå to har ansvar for det utførende arbeidet innenfor sine respektive ansvarsområder. Dette ansvaret er knyttet opp mot ansvaret de har i egen linje og rollen de har

som systemeier. Systemeier har ansvar for den funksjonen eller det fagområdet hvor et IKT-system anvendes med hensyn til personvern, og eierskap til de applikasjonstjenestene som benyttes. Systemansvarlig støtter systemeier og ivaretar de operative oppgavene på vegne av systemeier. I forbindelse med behandling av personopplysninger er følgende ansvar særlig relevant:

- beslutte hvem som skal ha tilgang til et system og på hvilket nivå
- samarbeide med informasjonssikkerhetsleder og personvernombudet der det er nødvendig
- påse at systemet håndteres etter gjeldende lover og regler og at systemet oppfyller krav i lover og forskrifter.

Operativt ansvar

Alle ledere ved helseforetaket er ansvarlig for ivaretakelse av personvern innen eget område. Alle ansatte, brukere og medarbeidere og prosjektledere er ansvarlig for å kjenne til og etterleve gjeldende regler for personvern, samt interne prosedyrer og rutiner som regulerer behandling av helse- og personopplysninger. Ansvaret i forbindelse med prosjektaktivitet er beskrevet særskilt i egne rutiner.

Personvernombud og informasjonssikkerhetsleder

Personvernombudet og informasjonssikkerhetslederen er foretaksovergripende støtte- og kontrollfunksjoner. Disse to samarbeider på flere områder som behandling av avvik, sammenstilling av data i ledelsesrapporteringen og ivaretakelse av den registrertes rettigheter.

Personvernombudets oppgaver er beskrevet i en egen funksjonsbeskrivelse. Rollen omfatter rådgivning om personvernspørsmål, kontrolloppgaver vedrørende regelverket samt å bistå i spørsmål vedrørende informasjonssikkerhet og personvern ved innføring av eller endring i digitale løsninger. Videre skal personvernombudet stå for opplæring og opplysning, og være et kontaktledd mellom foretakets ledelse, Datatilsynet og de registrerte. Personvernombudet rapporterer direkte til administrerende direktør med faste kvartalsvise møter. Ombudet har i tillegg faste månedlige møter med viseadministrerende direktør.

Informasjonssikkerhetsleder har fagansvaret for og er rådgiver på informasjonssikkerhetsområdet. Rollen skal utarbeide, vedlikeholde og forbedre Akershus universitetssykehus HFs strategiske og styrende dokumenter innen informasjonssikkerhet. Rollen skal videre kontrollere at de styrende dokumentene fungerer etter hensikten. Informasjonssikkerhetsleder skal også på vegne av administrerende direktør vurdere risiko ved nye eller endrede løsninger.

Foretaksrevisjonen

Foretaksrevisjonen forvalter styringssystemet for virksomhetsstyring og internkontroll som kalles Orden i eget Ahus. Foretaksrevisjonen har også ansvar for ledelsens gjennomgang, årlig gjennomgang av internkontroll, eksterne tilsyn og interne revisjoner. Retningslinjen for virksomhetsstyring og internkontroll er det overordnende styrende dokumentet som øvrige prosedyrer og rutiner i virksomheten skal bygge på. Retningslinjen er godkjent av administrerende direktør og forvaltes av foretaksrevisor. Foretaksrevisor koordinerer internkontrollprosessen med personvernombud og informasjonssikkerhetsleder.

Ny koordinerende funksjon for personvernarbeidet i foretaket

Det har fram til annet halvår 2020 vært uavklart hvor systemansvaret for den foretaksgripende protokollen skal plasseres. Ansvaret er nå avklart og plassert hos viseadministrerende direktør, hvor forvaltningsansvaret er plassert til foretakssekretariatet. Ahus opplyser at helseforetaket er i ferd med å etablere en funksjon i foretakssekretariatet som skal ivareta dette ansvaret.

Retningslinjer og prosedyrer

Ahus har utarbeidet en felles retningslinje for virksomhetsstyring og internkontroll. Dette dokumentet gjelder uavhengig av regelverk, og har også et grensesnitt mot personvernområdet som et av flere områder som er regulert i egen lovgivning.

På øverste nivå er det administrerende direktør som er ansvarlig for å etablere virksomhetsstyring og internkontroll i virksomheten, mens viseadministrerende direktør har et systemansvar som innebærer etablering, drift og vedlikehold av styringssystemet.

Ledere på alle nivåer har ansvar for at virksomhetsstyring og internkontroll innenfor eget ansvarsområde er etablert og gjennomføres i henhold til forutsetningene.

All behandling av personopplysninger på Ahus skal skje innenfor rammene av helseforetakets retningslinje for personvern. Retningslinjen er en del av det virksomhetsovergripende styringssystemet. Retningslinjen fastlegger den registrertes rett til vern av personopplysninger og grunnleggende prinsipper for personvern. Videre er ansvar og oppgaver fordelt og plassert til ledelsesfunksjoner og til sentrale roller. Det er definert prosedyrer og rutiner for:

- protokoll over behandlingsaktiviteter
- håndtering av uønskede hendelser
- personvernkonsekvensvurderinger
- databehandleravtaler
- overføring av personopplysninger til tredjestater
- innhenting av samtykke.

Rutinen for protokoll over behandlingsaktiviteter er under utforming og således ikke implementert på revisjonstidspunktet.

Rapportering til styret og ledergruppen

Akershus universitetssykehus HFs tilpasninger til personvernforordningen ble organisert gjennom GDPR-prosjektet, se avsnitt 2.1. Så lenge prosjektet var virksomt rapporterte det jevnlig til helseforetakets ledergruppe. Sykehusledelsen var i tillegg prosjektets styringsgruppe. Ved prosjektets avslutning ble sluttrapporten behandlet i ledergruppen og styret ble orientert. Personvern og informasjonssikkerhet inngår som en del av ledelsens gjennomgang og gjennomgang av internkontroll som gjennomføres hvert år. Det utarbeides årlig en presentasjon over avvik med hensyn til personopplysninger og informasjonssikkerhet. Resultatene fra ledelsens gjennomgang, gjennomgang av internkontrollen og avviksrapporteringen behandles i foretaksledelsen og styret og inngår i helseforetakets årlige melding.

Behandling av personopplysninger inngår også som en del i det ordinære rapporterings- eller oppfølgingsregimet til ledergruppen og styret. Aktuelle saker og temasaker som vedrører foretakets behandling av personopplysninger blir brakt inn for ledelsen ved behov.

Styrket personvern og informasjonssikkerhet

To initiativer har vært sentrale i forbedringen av personvern og informasjonssikkerhet ved Ahus: eSkjema i Forskning og innovasjon og PRIM.

PRIM

PRIM (Prosjekt oppfølging av tiltak etter analyse av risiko for brudd på informasjonssikkerhet og medisinteknisk utstyr) er et prosjekt ble nedsatt av Ahus' styre. Formålet var å styre og gjennomføre tiltak for å forbedre informasjonssikkerheten på bakgrunn av en ROS-analyse av medisinsk-teknisk utstyr (MTU) og informasjonssikkerhet på Ahus. Bakgrunnen var Riksrevisjonens undersøkelse fra 2015 om informasjonssikkerhet ved bruk av medisinsk-teknisk utstyr. Noen av prosjektets leveranser har vært:

- nye prosedyrer og reviderte prosedyrer ved innkjøp, bruk, forvaltning og avhending av MTU

- bevisst- og ansvarliggjøring av medarbeidere som til daglig bruker MTU gjennom nye opplæringsrutiner
- sårbarhetsanalyser
- styrking av rutiner for oppfølging av leverandører
- kontrollprogrammer.

PRIM hadde oppstart i juni 2019 og ble sluttført i september 2020. Det er utarbeidet en implementeringsplan etter at prosjektet ble avsluttet.

eSkjema

Som et universitetssykehus har Ahus en omfattende aktivitet på forsknings- og innovasjonsområdet. Helseforetaket har en administrativ funksjon for forskningsstøtte som ivaretar rapportering og generell drift for all forskningsaktivitet ved helseforetaket. For å ivareta internkontrollen for denne aktiviteten, har helseforetaket som et av tiltakene utviklet eSkjema. eSkjema er et elektronisk meldeskjema som styrer prosessen som omgir prosjektene fra initiering til avslutning, og ivaretar en rekke kontrollaspekter forbundet med prosjektgjennomføringen. Følgende aspekter er særs relevant i forbindelse med behandling av personopplysninger:

- innmelding av prosjekt til avdeling Personvern forskning og intern kvalitetssikring
- innmelding av endringsmeldinger for prosjekt til personvern forskning og intern kvalitetssikring
- krav til arkivering av forskingsdokumentasjon i P360
- GDPR og artikkel 30-oversikt (behandlingsoversikt for personopplysninger)
- DPIA egenerklæring.

Opplæring

Behandling av personopplysninger inngår som en del av den organiserte opplæringen ved Ahus. Behandling av personopplysninger inngår som en del av ledelopplæringen og av opplæringen av kontorfaglig personell. Personvern inngår også som en del av den obligatoriske opplæringen for alle som har et forskningsprosjekt.

Avvikshåndtering

Det er etablert en overordnet prosedyre avvikshåndtering ved helseforetaket. Avvik knyttet til personvern og informasjonssikkerhetsavvik inngår som en del av denne overordnede prosedyren. Det elektroniske kvalitetssystemet EQS benyttes som systemstøtte.

Oppfølging av avvik er et delt ansvar mellom personvernombudet og informasjonssikkerhetsleder. Eventuell meldeplikt ved alvorlig avvik vurderes forløpende, og personvernombudet følger opp dialogen med Datatilsynet.

I helseforetakets årlig melding for 2019 informeres det om 244 uønskede hendelser i kategorien personvern/informasjonssikkerhet, hvorav 36 ble meldt til Datatilsynet. De fleste av disse gjelder brudd på personopplysningenes konfidensialitet.

Risikovurderinger og DPIA

Ahus har en prosedyre for risikostyring som en del av styringssystemet. Risikovurdering som inkluderer personvern og informasjonssikkerhet inngår som en del av styringssystemet for virksomhetsstyring og internkontroll.

Ahus har en egen prosedyre og mal for gjennomføring av personvernkonsekvensvurderinger. Ansvarlig for gjennomføring er system- eller prosjekteier. Personvernombudet gir råd om vurderingen av personvernkonsekvenser og skal kontrollere gjennomføringen av prosessen.

Sletting
Ahus har utarbeidet en prosedyre for lagring, arkivering og sletting av helse- og personopplysninger. Ved prosjektavslutning eller etter endt arkivering slettes eller anonymiseres alle helse- og personopplysninger. Instruksen retter seg mot alle ledere innen ulike enheter og områder og har som ansvar for å påse at instruksen er implementert og etterlevd innen eget ansvarsområde. Alle ansatte og innleide ved Ahus skal forholde seg til instruksen. Vedrørende sletting har personvernombudet og informasjonssikkerhetsleder et særskilt rådgivningsansvar.

I protokollen er det informasjon om planlagte tidsfrister for sletting av personopplysningene, og om lov- og forskriftsgrunnlaget for fastsettelse av fristene.

4.2 Vurderinger

Ansvaret for at det er et foretaksovergripende system for behandling av personopplysninger er lagt til viseadministrerende direktør og foretakssekretariatet. I den videre operasjonaliseringen er ansvaret for behandling av personopplysning fordelt og plassert i lederlinjen. Øvrige medarbeideres ansvar for å medvirke til prosessen er tydelig. Det er etablert fagfunksjoner, dels foretaksovergripende og dels divisjonsinterne, som ivaretar fagansvaret og som rådgir både helseforetakets øverste ledelse og de som har et operativt ansvar for behandlingen. Ansvars- og oppgavefordelingen mellom ledelsesfunksjoner og fagroller i Ahus synes formålstjenlig gjennom en klar og tydelig deling mellom utøvende lokalt ansvar på den ene side og kontroll- og oppfølgingsansvar i sentrale, tverrgående funksjoner på den annen side.

Personvernarbeidet i Ahus er nedfelt i styrende, gjennomførende og kontrollerende dokumentasjon. Dokumentasjonen er tilgjengelig for alle medarbeidere i helseforetaket.

Akershus universitetssykehus HF har en styrebehandlet strategi som gir uttrykk for ambisjon og retning i personvernarbeidet. Strategien følges opp gjennom årlige handlingsplaner. Behandlingen av personopplysninger er videre understøttet av retningslinjer og prosedyrer. Samlet sett skal disse ivareta helseforetakets forpliktelser og er integrert med øvrige styringsprosesser i helseforetaket.

En rutine for vedlikehold av protokollen for behandling av personopplysninger er under utarbeidelse. Rutinen vil sette i system samordningen av desentralt ansvar og oppgaver i forbindelse med behandling av personopplysninger med det sentrale ansvaret for å ha en samlet og oppdatert protokoll som omfavner hele helseforetaket. Rutinen bør konkretisere det sentrale oppfølgingsansvaret for en foretaksovergripende protokoll. Rutinen kan også omfatte videreutvikling av protokollen for at den i enda større grad gir relevant og oppdatert dokumentasjon av behandlingen av personopplysninger.

5. Behandlingsprotokollen

Revisjonen har undersøkt om helseforetakets protokoll er dekkende for Akershus universitetssykehus HFs behandling av personopplysninger. I dette inngår etablering av protokollen, protokollens oppbygning og struktur, roller og ansvar for protokollens informasjon og regionale avhengigheter.

5.1 Utgangspunktet for protokollen

Utgangspunktet for behandling av alle personopplysninger er et rettslig behandlingsgrunnlag med et definert formål som er dokumentert i en protokoll.

Formål

Før en virksomhet begynner å behandle personopplysninger, må det foreligge et eller flere angitte formål.

En virksomhet kan aldri samle inn eller lagre personopplysninger uten et formål. Dette er nedfelt i et av personvernprinsippene i personvernforordningen. Personopplysninger skal kun brukes til spesifikke, uttrykkelige, uttalte og legitime formål. Dette betyr at hvis virksomheten ønsker å bruke personopplysninger, må det starte med å formulere formålet før behandlingsaktivitetene identifiseres og vurderes.

Virksomheten har en plikt til å gi den enkelte informasjon om formålet med behandlingen av personopplysninger på en forståelig måte.

Dokumentasjon av behandlingsaktiviteter i protokoll

Det er ikke stilt noen formkrav til hvordan protokollen skal føres. Behandlingsansvarlig bestemmer hvordan dette skal gjøres, så lenge kravet til obligatorisk innhold blir med i en samlet skriftlig og elektronisk tilgjengelig oversikt.

Dette temaet er også omhandlet under avsnitt 2.3 Krav til behandlingsprotokoll.

5.2 Observasjoner

Observasjonene er knyttet til følgende områder:

- protokoll over behandlingsaktiviteter
- roller og ansvar
- innretning av protokollen
- differensiering av behandlingsaktiviteter
- rapportering til styret og ledergruppen.

Protokoll over behandlingsaktiviteter

Behandlingsprotokollen som konsernrevisjonen har mottatt dokumenterer behandlingsaktivitetene ved Ahus. Protokollen er utarbeidet med utgangspunkt i Datatilsynets anbefalte mal. Protokollen består av tre deler: en del for helsehjelp, en generell del og en del for forskning og innovasjon. Delen for helsehjelp omfatter all den kliniske virksomheten, den generelle delen omfatter personaladministrasjon og -ledelse, varsling, kameraovervåkning og diverse behandling av personopplysninger. Den tredje delen omfatter forskning, innovasjon og kvalitetsstudier.

Delprotokollen for helsehjelp og den generelle delprotokollen føres samlet i et regneark. For forskning og innovasjon er protokollen integrert i systemløsningen eSkjema, nærmere omtalt i kapittel 4. Ahus benytter ikke en tilrettelagt elektronisk systemløsning for en samlet protokoll.

De tre områdene som delprotokollene omhandler har ulik dynamikk. Forskning og innovasjon er preget av at behandlingsaktivitetene stadig er i endring etter som nye prosjekter kommer til mens andre igjen blir avsluttet. HR-området på den annen side, er preget av relativt stabile prosesser, systemer, omgivelser og rammebetingelser.

Protokollen er strukturert etter formålet med behandlingen. Et prinsipp i personvernforordningen er at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Formålet i Ahus er eksempelvis pasientjournal, pasientbehandling, blodgivning, eller opplæring og undervisning. For et gitt formål er det informasjon om blant annet følgende:

- hva gjelder behandlingen av personopplysninger
- internt ansvarlig
- kategorier av registrerte
- kategorier av personopplysninger
- kilde for personopplysningene
- kategorier av mottakere
- behandlingsgrunnlag, det vil si behandlingens lovlige grunnlag, jamfør personvernforordningen artikler 6 og 9.
- informasjonssystemer der behandlingen foregår
- databehandleravtaler.

For det medisintekniske utstyret vises det i protokollen til Medusa. Medusa et informasjonssystem som understøtter forvaltning, drift og vedlikehold av medisinsk utstyr.

Protokollen har i tillegg annen informasjon som anses som nyttig i en utvidet sammenheng.

Akershus universitetssykehus HFs protokoll omfatter behandling av personopplysninger på følgende områder:

Figur 4: Elementene i Ahus' behandlingsprotokoll

Roller og ansvar

Ansvaret for innholdet i protokollen er fordelt på de internt behandlingsansvarlige. Rollen som systemansvarlig plasseres til ledere på nivå to. Som en del av denne rollen er ledere på nivå to ansvarlig for å vurdere konsekvensene ved nye og endrede behandlingsaktiviteter og påse at protokollen blir oppdatert.

Det helhetlige ansvaret for forvaltning av protokollen har, etter at protokollen ble etablert, ikke blitt operasjonalisert. Vedlikeholdsrutiner for en foretaksovergripende protokoll er under utarbeidelse og den sentrale oppfølgingen skal utføres av en nyopprettet stilling i foretakssekretariatet.

Innretning av protollen

Innholdet i Akershus universitetssykehus HFs protokoll bygger på en intern kartlegging av behandling av personopplysninger. Kartleggingen ble utført i regi av GDPR-prosjektet. Alle informasjonssystemer som innbefatter behandling av personopplysninger har en systemeier som også er internt behandlingsansvarlig. Systemeierne har gjennomgått og dokumentert sine respektive systemer. Kartleggingen omfatter også behandling av ustrukturerte data. Resultatene fra kartleggingen har blitt innarbeidet i helseforetakets protokoll, strukturert etter prosess eller formål.

Variasjon i angivelsen av formål og tilhørende behandlingsaktiviteter i protokollene

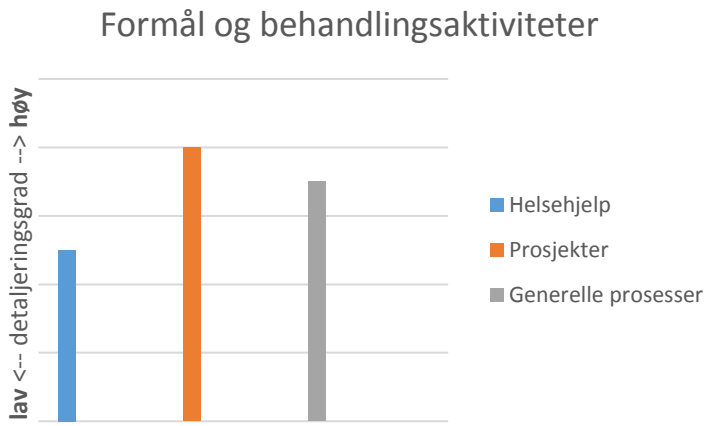
Konsernrevisjonen observerer at det er stor variasjon i detaljeringsgraden på angivelsen av formål og de tilhørende behandlingsaktivitetene mellom de tre delprotokollene.

I delprotokollen som omfatter forskning og innovasjon er hvert prosjekt definert som en behandlingsaktivitet med tilhørende formål. Dette innebærer at risikovurderinger, lagring, overføring, databehandling, og tekniske og organisatoriske tiltak beskrives på et relativt detaljert nivå.

I den generelle delprotokollen er hver hovedprosess i virksomheten i realiteten definert som en overordnet behandlingsaktivitet med hvert sitt tydelige formål. I delprotokoll for helsehjelp er aktivitetene imidlertid gruppert i felles funksjonsområder, eksempelvis "pasientjournal" og "pasientbehandling" som gjelder flere behandlingsaktiviteter. Behandlingsaktivitetene innenfor disse to gruppe er dermed definert som like uten at det skilles mellom pasientadministrasjon og klinisk virksomhet for øvrig, og som ikke hensyntar eventuelle forskjeller i prosesser og bruk av andre registre i behandlingsaktivitetene. I visse tilfeller vil behandlingsgrunnlaget være likt innenfor samme formål, og derfor kan noen behandlingsaktiviteter likevel grupperes under ett, under forutsetning av at man har forsikret seg om at dette er tilfellet.

Innenfor noen formål, for eksempel blodgivning, er det en nokså tydelig knytning mellom formålet og behandlingsaktivitetene. Innenfor andre formål, kanskje særlig pasientbehandling, er det liten grad av differensiering mellom de ulike behandlingsaktivitetene. Dette innebærer at eventuelle forskjeller i behandlingsgrunnlag, risikovurderinger, lagring, overføring, databehandling, og tekniske og organisatoriske tiltak ikke fanges opp og reflekteres i oversikten over behandlingsaktivitetene og videre antas det at det er samme formål for disse behandlingsaktivitetene.

I noen sammenhenger vises det til opplysninger i andre informasjonssystemer, for eksempel Medusa. I andre sammenhenger grupperes flere løsninger sammen uten at det er noen direkte henvisning til detaljert informasjon.



Figur 5: Ahus' tre delprotokoller - relativ vurdering

Konsernrevisjonens relative vurdering av dokumenterte behandlingsaktiviteter i foretakets protokoll viser stor variasjon i detaljeringsnivå på områdene helsehjelp, generell del (støtteprosesser) samt forskning og innovasjon, se figur 5. Dette er en innbyrdes vurdering av de forskjellige protokollene i foretaket og i hvilken grad behandlingsaktiviteter og tilhørende vurderinger av tiltak, risiko og personvernkonsekvensvurdering kan sammenstilles eller fremkommer som en del av foretakets samlede oversikt over behandlingsaktiviteter.

Databehandleravtaler

Noen leverandører skal ha tilgang til Akershus universitetssykehus HFs informasjonssystemer. Før tilgang blir gitt, etablerer Sykehuspartner HF underdatabehandleravtale for systemer som driftes av dem.

Regional protokoll

I oppdrag og bestilling 2019 for Ahus er det oppgitt at Sykehuspartner HF i løpet av 2019, i samarbeid med Regionalt Sikkerhetsfaglig Råd, skal utarbeide og implementere en regional mal og standard for protokollen, slik at hvert enkelt foretak kan fylle ut sine behandlinger. Sykehuspartner HF har med utgangspunkt i sin egen tjenesteportefølje utarbeidet en løsning som skal være klar for innføring på helseforetakene innen utløpet av 2020. Løsningen forutsetter samordnede prosesser mellom Sykehuspartner HF og de øvrige helseforetakene for forvaltning av informasjon i protokollen.

Akershus universitetssykehus HF gir uttrykk for noe usikkerhet om forutsetningene for Sykehuspartner HFs løsning for regional protokoll er til stede. Ahus opplyser at de ikke har vært involvert i en prosess for kartlegging av behov og krav som grunnlag for utvikling av protokollen. Ahus vurderer at det ligger en systemorientert tilnærming til grunn for løsningen, som ikke uten videre kan understøtte en prosessorientert protokoll på Ahus. På den bakgrunn stiller Ahus spørsmål om systemløsningen vil imøtekomme Ahus' behov for oversikt over personopplysninger med behandlingsformål.

Fullstendighet med hensyn til dokumentasjon av behandlinger i registre og fagsystemer

En nærmere gjennomgang av enkelte deler av protokollen viser noen tilfeller av at behandlingen ikke er tilstrekkelig dokumentert. Dette skyldes blant annet at endringer i helseforetakets systemportefølje ikke har blitt fanget opp etter etablering av protokollen.

5.3 Vurderinger

Protokoll for behandling av personopplysninger er et viktig fundament i personvernarbeidet. Uten nødvendig oversikt over behandlingsaktivitetene er det vanskelig å etablere målrettede og risikobaserte tiltak. Akershus universitetssykehus HF har utarbeidet en protokoll som skal gi obligatorisk informasjon om behandlingsaktivitetene i tillegg til støtteinformasjon. Det understrekes at revisjonen ikke har hatt til formål å bekrefte protokollens fullstendighet eller riktighet, jamfør avsnitt 3.2 *Omfang og avgrensninger*.

Protokollen skal gi en samlet oversikt over Akershus universitetssykehus HFs behandlingsaktiviteter. Protokollen dekker helsehjelp, forskning og innovasjon, personal og andre administrative områder. Ansvaret for vedlikehold av informasjon i behandlingsprotokollen er fordelt ut over i linjeorganisasjonen. Men det mangler en rutine for løpende forvaltning som støtter opp under og for oppfølging av dette ansvaret. Fravær av en effektiv forvaltningsrutine som grunnlag for vedlikehold av informasjon vil føre til at informasjon i protokollen gradvis vil miste aktualitet.

Akershus universitetssykehus HF skal sikre og påvise en forsvarlig behandling av personopplysninger ved at man ivaretar den registrertes rettigheter og friheter, samtidig som man ivaretar helseforetakets mål ved behandlingen. Etter personvernforordningens artikkel 24 innebærer det en forholdsmessighet hvor man ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter. Ut fra det gjennomfører man egnede tekniske og organisatoriske tiltak. Internkontroll skal være ledelsens verktøy for å ivareta ansvaret sitt og for å kunne demonstrere etterlevelse etter personvernregelverket. Det skal også være de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte. Tiltakene skal dokumenteres og oppdateres ved behov.

I utformingen av protokollen må ulike hensyn balanseres for å få en riktig detaljeringsgrad. Det er få faste holdepunkter for hvor detaljert en protokoll skal være, men det er et grunnleggende prinsipp av personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. I Akershus universitetssykehus HFs protokoll er enkelte av formålene (prosessene) gitt på et svært overordnet nivå, for eksempel "pasientbehandling". Dette gjelder særlig delprotokollen for helsehjelp. Konsernrevisjonen stiller spørsmål ved om Akershus universitetssykehus HF gjennom denne overordnede tilnærmingen kan dokumentere at opplysningene er samlet inn for spesifikke, uttrykkelig angitte og berettigede formål. Konsernrevisjonen er av den oppfatning at de mest overordnede kategoriene av behandlinger (prosesser) kan brytes ned i mer detaljerte kategorier. Mer detaljert informasjon om behandlingsaktivitetene vil bedre innsikt i hvilke personopplysninger som behandles, i hvilken sammenheng de behandles, det lovlige grunnlaget for behandlingen og tekniske og organisatoriske tiltak.

Når det ikke er noen formkrav til protokollen kan det være noe usikkerhet knyttet til hva som konkret kreves og hvordan dette skal løses. Over tid vil etablert praksis gjøre dette tydeligere og kravene vil bli presisert gjennom uttalelser fra Datatilsynet og kjennelser fra domstolene. Siden ansvaret for vedlikehold av protokollen ikke tydelig har vært plassert, har ikke Akershus universitetssykehus HF tatt stilling til hva dette innebærer for helseforetaket som helhet.

En protokoll skal være skriftlig og elektronisk. Akershus universitetssykehus HF har ikke et formålsrettet forvaltningsverktøy for protokollen i sin helhet. Delprotokollen for forskning og innovasjon forvaltes i eSkjema, mens de øvrige delene føres i et regneark etter mal fra Datatilsynet. Med tanke på kompleksiteten i sammenstilling og vedlikehold av informasjon fra flere prosesser, grensesnitt og behandlingsaktiviteter har noen helseforetak valgt å benytte en tilpasset verktøystøtte for å dokumentere og synliggjøre

sammenhengen mellom formål, behandling, rettslig grunnlag, risikovurderinger og prosesser.

Riktig nok er behandlingen av personopplysninger et ledd i den medisinske behandlingen i en eller annen form, men det vil være forskjeller i rettslig grunnlag, risikovurderinger, lagring og overføring av data til databehandler og tekniske og organisatoriske tiltak. Siden graden av differensiering er lav, vil disse forskjellene i liten grad framgå uten et klart og tydelig formål slik behandlingsaktivitetene er dokumentert i protokollen for tiden.

Vedlegg 1

Tabell 1: Informasjonsgrunnlag

Dokumentasjon	
Organisasjonskart Ahus	EQS-rutiner for utlevering av prøvesvar mv
Strategi for personvern og informasjonssikkerhet 2019 - 2022	Interndatabase og eSkjema – artikkel 30
Ahus - Forvaltningsprinsipp - Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet	Orden i eget Ahus
Ahus - Gjennomførende - Innsyn i ansattes e-post og personlig hjemmekatalog	Styresak 12-19 Sluttrapport GDPR prosjektet
Ahus - Gjennomførende - Utlevering av helse- og personopplysninger	Styresak 12-19 Vedlegg 1 Sluttrapport GDPR prosjektet
Ahus - Høsting, lagring og utlevering av person- og helseopplysninger fra IKT-systemer	Styresak 12-19 Vedlegg 2 Handlingsplan
Ahus - Lagring, arkivering og sletting av helse- og personopplysninger	Styresak 25-18 Rapport over informasjonssikkerhetsavvik meldt i EQS for 2017
Ahus - Kontrollerende - Risikovurdering ved nye og endrede IKT-løsninger og databehandlinger	Styresak 75-19 Avvik IS og PV 2018 tom mai 2019
Ahus - Kontrollerende - Gjennomføring av revisjon og avvikshåndtering	Styresak 75-19 Avvik på PV og IS meldt i 2018 tom mai 2019
Ahus - Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet	Styresak 93-20 Avvik innen informasjonssikkerhet og personvern 2019
HSØ - Ledelsessystem for informasjonssikkerhet	Styresak 93-20 Uønskede hendelser innen personvern og informasjonssikkerhet - tall fra 2019
Ahus - protokoll for behandlingsaktiviteter - artikkel 30	Funksjonsbeskrivelse personvernombud
Ansvar i forskning ved Akershus universitetssykehus HF	Tjenestekatalog Applikasjonsliste v. 5.02

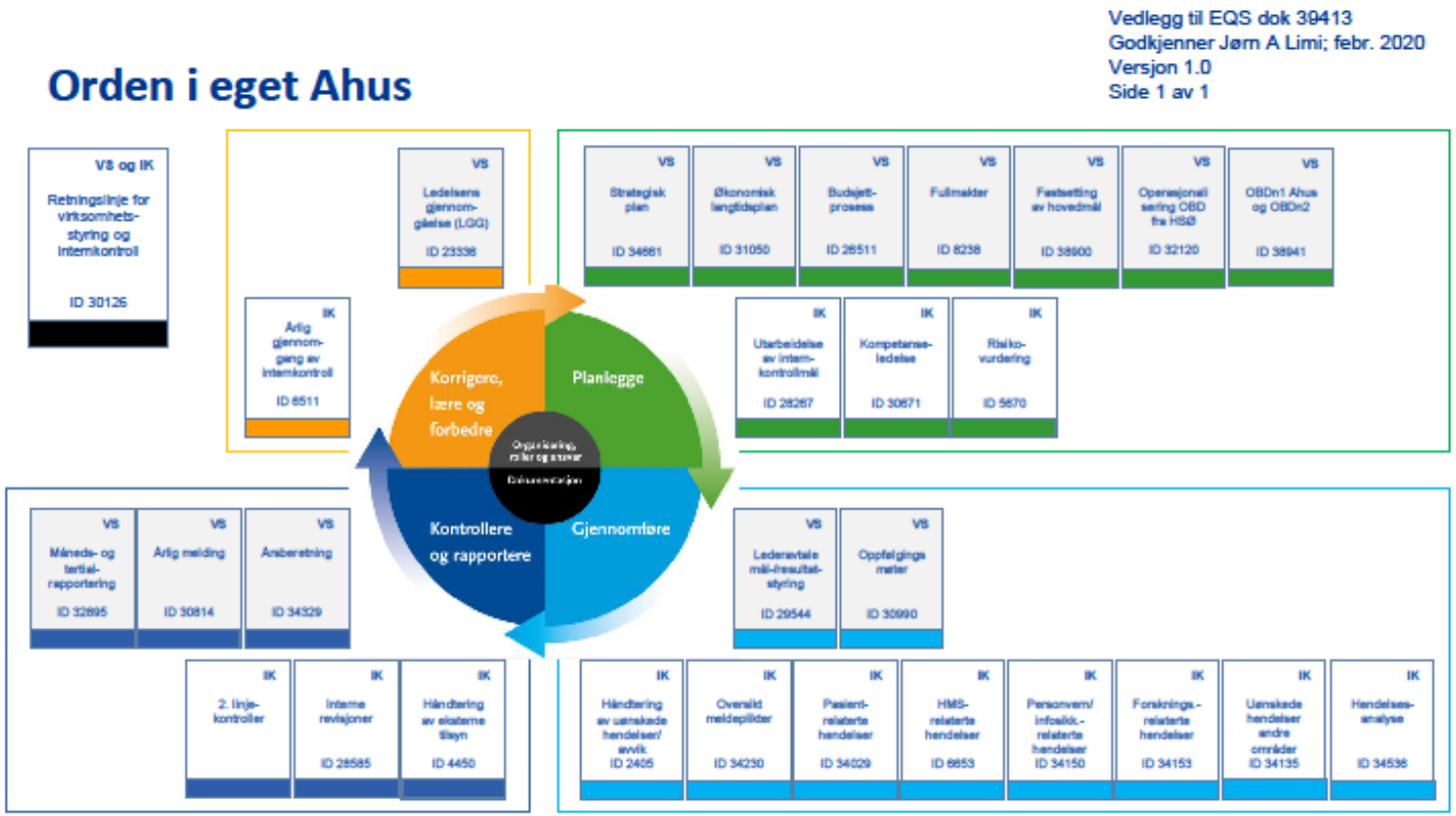
Dokumentasjon	
Ahus - Vurdering av personvernkonsekvenser (DPIA)	Årlig gjennomgang. Sjekkliste 4 – Personvern og informasjonssikkerhet
Ahus - Retningslinje for virksomhetsstyring og internkontroll	Ahus – Retningslinje for personvern
Ahus - Virksomhetsstyring og internkontroll - dokumentoversikt	Veileder ved vurdering og håndtering av risiko. v.1.0
Årlig gjennomgang. Sjekkliste 1 – Generell	Oversikt over behandlingsoversikt for Ahus - Fase 3 v01

Vedlegg 2

Tabell 2: Gjennomførte samtaler

Dato	Navn og stilling/funksjon
15. september 2020	Hilde Schultz. Personvernombud
15. september 2020	Kåre Magne Stennes. Informasjonssikkerhetsleder
15. september 2020	Karl-Helge Storhaug. Leder foretaksrevisjonen
5. oktober 2020	Jan Inge Pettersen. Direktør HR - felles Anne-Gry Kolstad. Avdelingsleder Personal Vibeke Wingerei. Seniorrådgiver HR. Avdeling lederrådgivning
7. oktober 2020	Janne Pedersen. Direktør Divisjon for diagnostikk og teknologi
14. oktober 2020	Helge Røsjø. Direktør Forskning og innovasjon Anne Karin Vassbakk. Leder avdeling for forskningsstøtte
14. oktober 2020	Pål Wiik. Fagdirektør Trond Jacobsen. Systemansvarlig DIPS
30. oktober 2020	Hilde Alstad. Direktør foretakssekretariatet Hilde Schultz. Personvernombud
6. november 2020	Jørn Limi. Viseadministrerende direktør
18. november 2020	Hilde Schultz. Personvernombud Kåre Magne Stennes. Informasjonssikkerhetsleder

Vedlegg 3


Vedlegg til EQS dok 39413
Godkjenner Jørn A Limi; febr. 2020
Versjon 1.0
Side 1 av 1
Orden i eget Ahus
VS og IK
Retningslinje for virksomhets-styring og internkontroll
ID 30126
VS
Ledelsens gjennom-gåelse (LGG)
ID 23338
IK
Årlig gjennom-gang av internkontroll
ID 6511
VS
Strategisk plan
ID 34881
VS
Økonomisk langtidsplan
ID 31050
VS
Budsjett-prosess
ID 28511
VS
Fullmakter
ID 8238
VS
Fastsetting av hovedmål
ID 38900
VS
Operasjonali sering OBD fra HSØ
ID 32120
VS
OBDn1 Ahus og OBDn2
ID 38941
IK
Utarbeidelse av intern-kontrollmål
ID 28267
IK
Kompetanse-ledelse
ID 30671
IK
Risiko-vurdering
ID 5670
Korrigere, lære og forbedre
Planlegge
Kontrollere og rapportere
Gjennomføre
VS
Måneds- og tertial-rapportering
ID 32695
VS
Årlig melding
ID 30814
VS
Årsberetning
ID 34329
IK
2. linje-kontroller
IK
Interne revisjoner
ID 28585
IK
Håndtering av eksterne tilsyn
ID 4450
VS
Lederavtale mål-/resultat-styring
ID 29544
VS
Oppfølgings møter
ID 30690
IK
Håndtering av uønskede hendelser/ avvik
ID 2405
IK
Oversikt meldepliktar
ID 34230
IK
Pasient-relaterte hendelser
ID 34029
IK
HMS-relaterte hendelser
ID 8853
IK
Personvern/ Informasjk.-relaterte hendelser
ID 34150
IK
Forsknings.-relaterte hendelser
ID 34153
IK
Uønskede hendelser andre områder
ID 34135
IK
Hendelses-analyse
ID 34536

Om konsernrevisjonen i Helse Sør-Øst

Konsernrevisjonen er organisert direkte under styret i Helse Sør-Øst RHF og rapporterer funksjonelt til styrets revisjonsutvalg og administrativt til administrerende direktør i det regionale helseforetaket. Våre rapporter behandles av styret i det reviderte helseforetak.

Konsernrevisjonen ble etablert i 2005, og er fra 1. januar 2013 hjemlet i helseforetaksloven §37a.

Konsernrevisjon skal på vegne av styret i Helse Sør-Øst bidra til forbedring i risikostyring, internkontroll og virksomhetsstyring i Helse Sør-Øst RHF og underliggende helseforetak.

Vår visjon

Konsernrevisjonen skal være en etterspurt bidragsyter til læring og for-bedring i Helse Sør-Øst.
Dette skal vi oppnå gjennom:

- Relevante revisjons- og rådgivningsoppdrag som skaper innsikt
- Effektiv kommunikasjon og godt samarbeid
- Deling av erfaringer og læringspunkter på tvers av helseforetakene

Om revisjonsprosjektet

Revisjonsperiode: September til desember 2020
Virksomhet: Akershus universitetssykehus HF
Oppdragsgiver: Styret i Helse Sør-Øst RHF

Revisorer:

- Espen Anderssen (oppdragseier)
- Anders Blix (oppdragsleder)
- Mazhar Ahmad (internrevisor)

Rapporten er oversendt til:

- Styrets revisjonsutvalg
- Administrerende direktør i Helse Sør-Øst RHF
- Styret i Akershus universitetssykehus HF
- Administrerende direktør i Akershus universitetssykehus HF

Konsernrevisjonens rapporter

Rapporter er tilgjengelig på følgende web-adresse:
https://www.helse-sorost.no/om-oss/styret/konsernrevisjonen