AKERSHUS UNIVERSITETSSYKEHUS

Styresak

Dato dok.:	14.02.2019	Administrerende direktør	
Møtedato:	01.03.2019		
Vår ref.:	19/02679-1	Postadresse:	1478 LØRENSKOG
		Telefon:	+47 67 96 00 00
Vedlegg:	1 Sluttrapport fra GDPR-prosjektet 2 Handlingsplan fra GDPR-prosjektet 3 Strategi for informasjonssikkerhet og personvern 4 Oppsummering fra oppfølging av revisjoner		

Sak 14/19 Administrerende direktørs orienteringer

Administrerende direktør ønsker å orientere om følgende saker:

1. Overføring av Kongsvinger sykehusområde fra Sykehuset Innlandet HF til Akershus universitetssykehus HF 1. februar 2019
2. Sluttrapport fra GDPR-prosjektet og plan for overgang til drift
3. Strategi for informasjonssikkerhet og personvern
4. Oppsummering fra oppfølging av revisjoner

Administrerende direktørs innstilling til vedtak:

Styret tar saken til orientering.

Øystein Mæland
Administrerende direktør

Dokumentet er elektronisk godkjent

1. Overføring av Kongsvinger sykehusområde fra Sykehuset Innlandet HF til Akershus universitetssykehus HF 1. februar 2019

Foretaksmøtet i Helse Sør-Øst RHF behandlet foretakstilhørighet for Kongsvinger sykehus den 29. juni 2017. Arbeidet med overføringen kan deles i to hovedfaser:

1) Å sikre en trygg og god overføring
2) En balansert utvikling av virksomhetene på Kongsvinger

Trygg og god overføring

Virksomhetsoverføringen ble gjennomført som planlagt 1. februar 2019 kl. 00:00. Dette omfattet:

- Overføring ansvaret for spesialisthelsetilbudet for kommunene i Glåmdalen til Akershus universitetssykehus
- Overføring av ansatte, eiendom og eiendeler
- Tilknytning av IKT-løsninger på Kongsvinger til Akershus universitetssykehus' IKT-plattform og overføring av all historikk fra alle systemer til Akershus universitetssykehus' databaser
- Videreføring av det lokale tilbudet på Kongsvinger med tilpasning til prosedyrer og arbeidsprosesser for Akershus universitetssykehus
- Omlegging av pasientstrømmer for de oppgaver lokalsykehuset på Kongsvinger ikke tilbyr, fra Sykehuset Innlandet til øvrige virksomheter på Akershus universitetssykehus

Det vises til styresak 88/18, Virksomhetsoverdragelse Kongsvinger sykehus, for en utfyllende gjennomgang av selve virksomhetsoverføringen.

Overføringen ble symbolsk markert med en nøkkeloverrekkelse på Kongsvinger sykehus fredag 1. februar, med deltakelse fra statssekretær i Helse og omsorgsdepartementet, styreleder og ledelse i Helse Sør-Øst, Akershus universitetssykehus og Sykehuset Innlandet, samt representanter fra kommunene, brukere og ikke minst ansatte ved Kongsvinger.

Selve overføringshelgen 1.-3. februar var i stor grad konsentrert rundt IKT-overføringen. Overføringen innebar at DIPS og andre kliniske systemer ble satt i lesemodus ved Kongsvinger i 26-29 timer. De siste 12-13 timene av perioden ble systemene ved alle Akershus universitetssykehus' lokaliteter satt i lesemodus. Migreringsplanen definerte en rekke beslutningspunkter gjennom overføringshelgen (GO/NO-GO-møter). Det var på forhånd besluttet at kun feil i DIPS kunne utløse en eventuell Roll-Back. Ved eventuelle feil i andre systemer ville overføringen gjennomføres og feilretting iverksettes i etterkant.

Migreringen ble gjennomført på en god måte og helt i henhold til planen. Søndag 3. februar kl. 00:30 ble alle kliniske systemer satt i drift, med Kongsvinger som en del av IKT-plattformen for Akershus universitetssykehus. De aller fleste IKT-endringene er gjennomført som planlagt og løsningene er i stabil drift. I overføringshelgen oppsto enkelte utfordringer knyttet til noen få løsninger eller prosesser, men ingen feil som tilsa at prosessen måtte stanses. Feilene ble i stor grad løst i overføringshelgen. Gjenværende feil følges særskilt opp og søkes løst innen 1. mars, som er prosjektets ELS-periode fra Sykehuspartner (Early Life Support).

Den kliniske driften både på Kongsvinger, Nordbyhagen og ved øvrige enheter var godt planlagt og bemannet for. Ved hvert beslutningspunkt gjennom overføringshelgen rapporterte beredskapsleder ved Akershus universitetssykehus status i den kliniske driften.

Oppsummert har virksomhetsoverføringen vært godt forberedt og forankret i alle berørte miljøer. Det var satt på tilstrekkelig med ressurser og god kompetanse fra både Sykehuspartner og Ahus IKT gjennom overgangshelgen, som sikret at overføringen av Kongsvinger sykehus, DPS og BUP til Ahus sin IKT-plattform fungerte bra. Tilsvarende var

de kliniske miljøer godt forberedt. De papirbaserte nødrutinene fungerte som planlagt gjennom helgen og pasientsikkerheten var godt ivaretatt.

Balansert utvikling av virksomhetene på Kongsvinger
Når virksomhetsoverføringen er gjennomført, starter fase II av arbeidet; å planlegge en balansert utvikling av virksomhetene på Kongsvinger. Det vil etableres et nytt prosjekt for gjennomgang av pasientstrømmer og vurdering av virksomhetenes tilknytning i den samlede organisatoriske strukturen for Akershus universitetssykehus. Prosessen vil ta utgangspunkt i føringene gitt i foretaksmøtet, herunder i særlig grad målet om å utnytte kapasiteten på Kongsvinger. Løsningene vil kunne omfatte både flytting av oppgaver fra Kongsvinger til øvrige enheter i foretaket, men med hovedvekt på flytting av oppgaver fra øvrige virksomheter til Kongsvinger («sentralisere det vi må, desentralisere det vi kan»).

Arbeidet med mandatet er påbegynt, og prosjektet skal etableres i løpet av mars måned. Prosjektet vil ta utgangspunkt i det kapasitetsmessige potensialet på Kongsvinger, og beregne hvor mye og hvilken type aktivitet som skal til for å kunne utnytte kapasiteten på en god måte.

Forslaget til videre utvikling vil både omfatte vurdering av hovedmodeller pasientbehandling, for eksempel å utvide det geografiske opptaksområdet for lokalsykehuset og/eller å utvide elektiv virksomhet rettet mot hele opptaksområdet for Akershus universitetssykehus, og hovedmodeller for fremtidig organisering av virksomheten.

Mandatet og prosjektet vil legge til rette for god involvering av ansatte, brukere, kommuner og andre interessenter.

2. Sluttrapport fra GDPR-prosjektet og plan for overgang til drift

Akershus universitetssykehus har siden februar 2018 jobbet systematisk og målrettet gjennom et foretaksovergripende GDPR-prosjekt for å sikre at foretaket er i samsvar med personvernregelverket. Prosjektet har planlagt, koordinert, rapportert, kartlagt og iverksatt tiltaksarbeidet.

Prosjektets viktigste leveranser har blant annet vært å utarbeide en protokoll over sykehusets behandlingsaktiviteter, kartlegging av hvilke områder det er behov for å styrke personvernet, utarbeidelse av viktige maler og verktøy samt utarbeidelse av nødvendige prosedyrer og rutiner for å sikre riktig behandling av personopplysninger.

Gjennom handlingsplaner utarbeidet av hver enkelt fagenhet er gjenstående aktiviteter og arbeidsoppgaver identifisert, ansvars- og tidfestet. Gjenstående aktiviteter og arbeidsoppgaver er lagt ut i drift til de fagansvarlige. Systemeier ved personvernombudet og informasjonssikkerhetsleder vil gjennom sine funksjoner som kontrollere, følge opp og kontrollere at gjenstående arbeider gjennomføres.

3. Strategi for informasjonssikkerhet og personvern

Strategi for personvern og informasjonssikkerhet ble vedtatt av sykehusledelsen den 15. januar, og gjelder for 2019 til 2022.

For Akershus universitetssykehus er personvern og informasjonssikkerhet blant de viktige bærebjelkene for å kunne yte profesjonelle og tillitsvekkende helsetjenester. Befolkningen i opptaksområdet og brukere av tjenestene forventer at foretaket har god styring og kontroll på opplysningene de gir fra seg. Pasienter og brukere forventer at opplysningene er riktige og tilgjengelige, at de ikke brukes til mer enn det foretaket skal, og at kun personer med tjenstlig behov får tilgang til deres opplysninger.

Hensikten med en strategi for personvern og informasjonssikkerhet er å lage en plan for understøtte utviklingsplanens hovedmål, samt øke bevisstheten og forståelsen av fagområdene i organisasjonen. Strategien skal være et styrende plandokument og bidra til at det kan arbeides planmessig og strukturert på overordnet nivå over tid for å nå foretakets mål innen personvern og informasjonssikkerhet. Dette er viktig for å kunne bygge en god kultur for personvern og informasjonssikkerhet i alle ledd. Innholdet i denne strategien beskriver noen sentrale satsningsområder de kommende årene.

Det skal utarbeides en årlig handlingsplan i tidsperioden som konkretiserer aktiviteter innenfor de ulike hovedområdene strategien er inndelt etter. Det vil samtidig lages en langtidsplan som skisserer aktiviteter i hele strategiens tidshorisont, der hovedaktiviteter som strekker seg over flere år vil planlegges.

Strategiens innhold vil hvert år være gjenstand for revisjon og forbedring dersom det er interne og eksterne rammebetingelser som krever endringer av innholdet.

4. Oppsummering fra oppfølging av revisjoner

Konsernrevisjonen Helse Sør-Øst hadde et møte 29. november 2018 med de ansvarlige for forbedringsarbeidet etter revisjonene *Legemidler* og *Tiltaksarbeid etter revisjoner utført av konsernrevisjonen*. Det er også oversendt dokumentasjon på gjennomførte og pågående tiltak.

Konsernrevisjonen vurderer at Akershus universitetssykehus har prioritert og gjennomført et godt forbedringsarbeid på de områdene som revisjonene omfattet, og at tiltakene i all hovedsak er gjennomført. Konsernrevisjonen planlegger ingen videre oppfølging av de aktuelle revisjonene, og anser disse som avsluttet.

GDPR Prosjektet

Sluttrapport og videre arbeid

Tittel: *GDPR Prosjektet*		**Referanse:** *18/01302*
Beslutningsdato: *29.01.2019*	**Beslutning:** *Prosjektet avsluttes og overføres til drift*	
Besluttes av: *Sykehusledelsen*	**Sluttrapport utarbeidet av:** *Maria Teresa Espino Donnelly* *Kåre Magne Stennes*	**Prosjektleder:** *Dina Robsrud (til 20.06.2018)* *Maria Teresa Espino Donnelly (fra 10.09.2018)*

Innhold

1. Kort sammendrag

Prosjektet startet med en kartlegging av hvilke områder av personvernforordningen som ville få størst innvirkning for Ahus, der vi blant annet identifiserte et behov for å styrke personvernområdet innen behandling av pasientopplysninger, innen HR og behandling av ansattopplysninger, samt et behov for å styrke personvern innen forskningsområdet grunnet endring i regelverket. I tillegg er det utført en større kartlegging av hvilke IKT-systemer som benyttes for behandling av og personopplysninger, og hva hensikten med de enkelte systemene er.

Høsten/vinter 2018 har prosjektet fortsatt arbeidet og gjennomført en oppdatering på status og leveranser. Arbeidet som er gjennomført har hatt fokus på koordinering og samordning av leveranser fra de ulike fagenhetene. Hver enkelt enhet har et selvstendig ansvar for at deres ansvarsområder utføres i overensstemmelse med den nye personvernlovgivningen. I samsvar med dette har oppgavene som gjenstår å gjennomføre for å få sykehuset i samsvar med GDPR, blitt tydeligere fordelt ut ifra ansvarsområder. Dette er gjort gjennom desentrale handlingsplaner som nå er satt sammen til et felles dokument.

Prosjektet anbefaler å plassere ansvar for videre arbeid med GDPR til linjen, der de enkelte enhetene sine handlingsplaner danner grunnlaget for aktiviteter som planlagt.

2. Bakgrunn og rammer

Ny personopplysningslov trådte i kraft 20. juli 2018. Den nye loven:

- styrker ordningen med Personvernombud
- legger vekt på ansvarlighet og internkontroll hos virksomheten fremfor forhåndskontroll fra Datatilsynet
- skjerper kravene til avviksbehandling, varsling av berørte og kontinuerlig arbeid med informasjonssikkerheten
- dagens krav om internkontroll blir erstattet av formuleringer om den behandlingsansvarliges ansvar
- krever oversikt over behandlingsaktiviteter

Sykehuset har siden februar 2018 jobbet systematisk og målrettet gjennom GDPR prosjektet for å sikre at Ahus er i samsvar med personvernregelverket.

Formålet med prosjektorganiseringen har vært:

- å forberede organisasjonen på krav og plikter som følger av nytt lovverk, GDPR som trer i kraft fra 25. mai 2018.
- Videreutvikle og reimplementere et forbedret system for internkontroll og kvalitetsstyring innen området personvern og informasjonssikkerhet i sykehuset som i enda større grad kan:
    - sikre ledelsesforankring og tydeliggjøre linjeleders ansvar for personvern/informasjonssikkerhet
    - *oppfylle* krav til internkontroll og forbedringsarbeid som følger av personvernlovgivningen og alminnelige internkontrollprinsipper
    - *bidra til å forebygge* feil, svikt og mangler

- Vurdere og sikre gjennomføring av nødvendige tilpasninger og endringer i ulike IT-systemer som behandler personopplysninger for å kunne oppfylle krav til personvern og informasjonssikkerhet i GDPR (innebygd personvern).

Prosjektets forberedelser til GDPR har arbeidet etter mandat vedtatt av Sykehusledelsen 13.02.2018 i sak 18/18. Tidligere status i prosjektet er gitt i:

- Sak 32-18 «Status og videre prosess- forberedelse til ny personvernforordning (GDPR) 25. mai 2018
- Temasak 15.05.2018 «Status GDPR – hva betyr det for Ahus»
- Sak 62-18 «Status og leveranser fra GDPR-prosjektet»
- Temasak 25.09.2018 «Videre arbeid i GDPR-prosjektet og DPIA metode og mal»

3. Prosjektorganisering og styring

Prosjektet følger normal prosjektstruktur i Ahus, og er organisert slik:

- Styringsgruppe: Sykehusledelsen
- Prosjekteier: Viseadministrerende direktør
- Prosjektleder: Dina Robsrud (tom 20. juni 2018), og Maria Donnelly (fra 10. september 2018)
- Ulike arbeidsgrupper som jobbet med ulike temaer

Prosjektet gjennomførte ett møte i måneden (med unntak av et lite opphold ved skiftet av prosjektleder) til og med juni 2018 og hver 14. dag fra og med september – desember 2018. Ledere fra arbeidsgrupper deltok og rapporterte status. DFM og Kommunikasjon ble først involvert i prosjektet høsten 2018.

4. Leveranser og gjenstående arbeid

Dette kapittelet vil beskrive de viktigste leveransene utført i prosjektet gjennom 2018. De beskrevne leveransene er viktige grunnlag for det videre arbeidet med personvern og informasjonssikkerhet på Ahus de kommende årene. Hver enhet som deltar i prosjektet har utarbeidet egne handlingsplaner med arbeidsoppgaver/aktiviteter i 2019 som også er ansvars- og tidfestet.

4.1 Artikkel 30 Protokoll

En viktig del av arbeidet med personvernforordningen er å lage en protokoll for behandlingsaktiviteter, der det skal fremgå hva vi bruker personopplysninger til, hvilke personopplysninger som brukes og hvor personopplysninger brukes. Begrepet «bruk» i denne sammenhengen må forstås med alt vi gjør med personopplysninger i våre arbeidsprosesser. Deler av denne protokollen skal kunne legges ut som åpen informasjon. Ahus har brukt Datatilsynets mal for protokollen.

Foretakssekretariatet har hatt ansvaret for innhenting av informasjon og etablering av protokollen. Dette har vært en tidkrevende prosess som involverte alle systemeiere og deres systemansvarlige.

Personvernombudet vil få ansvaret med å forvalte denne protokollen som en av sine arbeidsoppgaver.

Versjon 1.0 er ferdig utarbeidet, men det gjenstår fortsatt arbeid for å komplettere protokollen med ulike detaljer. Blant annet gjenstår det å kartlegge biobanker (forskning) og nasjonale medisinske kvalitetsregistre (enhet for medisin og helsefag). Dette arbeidet pågår akkurat nå, og forventes å være sluttført innen sommeren 2019. Ahus har en protokoll for forskningsprosjekter og lokale medisinske kvalitetsregistre gjennom løsningen for eSkjema utviklet av Forskningsstøtte i 2018.

Endelig versjon av protokoll for behandlingsaktiviteter skal etter planen flyttes over i digital løsning utviklet av Avdeling for analyse i løpet av første halvdel av 2019.

Arbeid som gjenstår:

- Utarbeide et eget system og en rutine for oppdatering (prosessen med dette har startet)
- Sammenstille protokoll for:
    - Forskningsprosjekter
    - Lokale og nasjonale medisinske kvalitetsregistre
    - Biobanker
    - Avklare detaljer i ordinær protokoll

4.2 Kartlegging og GAP-analyse

Prosjektet har gjennomført en overordnet kartlegging som er rapport tidligere til sykehusledelsen, se sak 18/01302-3. I etterkant har HR, Forskning, Kommunikasjon og Foretakssekretariatet startet en kartlegging og GAP-analyse på et mer detaljert nivå. Aktiviteter som fremkommer etter dette arbeidet er beskrevet i enhetsvise handlingsplaner.

Arbeid som gjenstår:

- Alle enheter fortsetter kartlegging og GAP-analyse på detaljert nivå
- Sikre at relevante prosedyrer og rutiner i EQS oppdateres slik at disse samsvarer med krav i GDPR

4.3 Ansvarsroller og arbeidsflyt

Gjennom internkontrollprosjektet ble det utformet en ny prosess for håndtering av avvik, samt det ble laget en ny EQS rutine for avvikshåndtering innen personvern og informasjonssikkerhet. Den nye rutinen for avvik stiller krav til tidsfrister for når Datatilsynet og eventuelt berørte parter av avviket skal varsles. Særskilt kravet om å varsle Datatilsynet om avviket innen 72 timer gir mindre rom for å granske avviket og innhente faktaopplysninger fra enheter på Ahus før vi må sende varselet. I praksis har dette medført en to-trinns varsling, der første varselet kun beskriver en mulig hendelse, og det andre varselet enten bekrefter avviket og utdyper dette, eller avkrefter at avviket har funnet sted.

Prosjektet har revidert funksjonsbeskrivelsen til personvernombudet ved Ahus slik at stillingsinnholdet nå er tilpasset krav i personvernforordningen og at dette nå blir en fulltidsstilling.

Det er utarbeidet en arbeidsflyt for vurdering av personvernkonsekvenser (DPIA) som kan deles i to faser:

1. Fase 1: Prosjekteier eller systemeier må sørge for at det gjøres en prekvalifisering tidlig i prosjektet (konseptfasen) eller endringsprosessen om det er behov for å gjennomføre en DPIA. Denne fasen involverer personvernombudet som rådgiver og kvalitetssikrer.
2. Fase 2: Dersom det besluttes at DPIA skal gjennomføres, skal prosjekteier eller systemeier sørge for at det utpekes en prosessleder og en arbeidsgruppe for gjennomføring av DPIA. Arbeidsgruppen må minst bestå av kompetanse fra IKT, juridisk, informasjonssikkerhet, fag – eventuelt flere ved behov. Personvernombudet skal kontrollere om DPIA er utført korrekt, og at vurderinger er faglig forsvarlige. En DPIA avsluttes enten med å godkjenne restrisiko eller ikke godkjenne restrisiko, noe som medfører at DPIA må forhåndsdrøftes med Datatilsynet.

Ansvaret for utførelse av en DPIA legges til prosjekteier eller systemeier, som begge har et «sørge for» ansvar i gjennomføring av arbeidet samt ansvar for å godkjenne restrisiko ved avslutning av DPIA-arbeidet.

I forskningsprosjekter legges ansvaret for en DPIA til prosjektleder.

Divisjon for forskningsstøtte og innovasjon har ansatt en personvernrådgiver for å ivareta personvernspørsmål og –vurderinger i forskningsprosjekter.

Følgende arbeid gjenstår:

- Ettersom prosesser, prosedyrer og maler er nye og/eller oppdatert for avvikshåndtering og DPIA, vil det være behov for å gjøre en revisjon rundt Q3-Q4 2019 for å vurdere om endringene har vært hensiktsmessige og at områdene fungerer slik de skal.

4.4 Verktøy/Maler

Prosjektet har utviklet og levert flere prosedyrer og maler som skal bidra til at sykehuset etterlever nye og oppdaterte regler etter ny personvernforordning. Listen under viser de viktigste prosedyrene og malene som er utviklet gjennom prosjektet. I parentes står det hvem som har deltatt i arbeidet.

- Prosedyre for vurdering av personvernkonsekvenser (DPIA) (DDT og Foretakssekretariatet (FS))
- Utkast til DPIA mal (DDT og FS)
- Utkast DPIA mal forskning (FS og Forskning)
- Mal innebygd personvern (FS)
- Brevmaler i forbindelse med avvikshåndtering (FS)
- Samtykkemal forskning (Forskning)

Arbeid som gjenstår:

- Få prosedyre og DPIA-mal godkjent i EQS
- Ferdigstille utkast til maler og oppdatere maler etter behov
- Maler/verktøy på ikke overordnet nivå ettersom behov melder seg eller viser seg gjennom kartlegging GAP-analyse

4.5 Opplæring og bevisstgjøring

Det er gjennomført og avholdt flere foredrag der personvern har vært hovedtema. Slike foredrag har vært holdt eller er planlagt for ledermøter i klinikker og internt i avdelinger der dette er relevant. For bedre å nå ut med informasjon pågår det et arbeid der Kommunikasjon er ansvarlig for en intranettside som de faglige enhetene kan publisere nyheter og faglig innhold. Det arbeides også med en opplæringsplan der blant annet bruk av e-læring er ett av flere virkemiddel.

Arbeid som gjenstår:

- Utarbeide e-læringsmoduler tilpasset ulike brukergrupper
- Ferdigstille opplæringsplan
- Ferdigstille intranettside og oppdatere denne etter behov

4.6 Oppdatering/utarbeidelse av prosedyrer/rutiner

Dokumentasjon av oppdaterte prosedyrer og rutiner er sentralt for å kommunisere med relevante brukere hvordan nytt regelverk påvirker eksisterende arbeidsprosesser. Ahus har deltatt i det regionale arbeidet med å oppdatere regionalt styringssystem for informasjonssikkerhet, slik at regionale krav samsvarer med GDPR.

Følgende prosedyrer i EQS eller interne rutiner er oppdatert etter gjeldende regelverk:

- Rutine for innsyn i personalmappe (intern rutine for HR)
- Oppdatering EQS rutine rekruttering (intern rutine for HR)
- EQS 35113: Retningslinjer for sletting og lagring av personopplysninger ansatte (HR)
- Flere EQS prosedyrer: Utarbeidet sentrale EQS prosedyrer for de registrertes rettigheter i forskningsprosjekter (Forskning)
- Regionalt styringssystem for informasjonssikkerhet: https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet#regionalt-styrende-dokumenter

Arbeid som gjenstår:

- Styrende dokumenter om personvern vil bli utarbeidet
- Relevante prosedyrer vil oppdateres fortløpende for å samsvare med gjeldende rettslige reguleringer

4.7 Oppdatering/utarbeidelse av skriv

Prosjektet har utarbeidet en personvernerklæring som skal gjelde ansatte. Denne vil få dokument ID EQS 35111, og er i prosess for ferdigstilling.

4.8 Oppdatering av IKT systemer

Dette arbeidet henger sammen med kartlegging av IKT-systemer utført som del av protokoll over behandlingsaktiviteter (artikkel 30), nærmere beskrevet i kapittel 4.1. Protokollen inneholder en oversikt over IKT-systemer som behandler personopplysninger, og inneholder ikke IKT-systemer som behandler virksomhetskritisk informasjon.

Oppdatering av IKT systemer omfatter følgende aktiviteter:

- Samsvarsvurdering av IKT-systemer for å sikre at tekniske og organisatoriske tiltak er i henhold til kravet om innebygd personvern
- Basert på resultatet av samsvarsvurderingen, iverksette en endringsprosess for eksisterende systemer eller anskaffelse av nytt IKT-system

Ahus har både regionale og lokale IKT systemer, der de regionale systemene er innført som del av Helse Sør Øst sin strategi om å konsolidere systemporteføljen. Oppdatering av de regionale systemene må koordineres gjennom regionale fora som forvalter de ulike løsningene.

Det er planlagt et møte ultimo februar for å starte planleggingen av dette arbeidet. Det bør påregnes at omfanget av dette arbeidet kan være omfattende og berøre flere systemeiere.

5. Overføring til linje

Hver enkelt enhet i prosjektet har utarbeidet egne handlingsplaner for å følge opp arbeidet videre i linjen. Gjennom handlingsplanene, er gjenstående aktiviteter/arbeidsoppgaver identifisert og ansvars- og tidfestet. Det anses derfor som mest hensiktsmessig at gjenstående aktiviteter/arbeidsoppgaver legges ut i drift til de fagansvarlige. Systemeier ved personvernombudet og informasjonssikkerhetsleder vil gjennom sine funksjoner som kontrollere, følge opp og kontrollere at gjenstående arbeider gjennomføres.

FELELS HANDLINGSPLAN – GDPR Prosjektet

HR:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	• Egen forespørsel			Ferdig utfylt. OK
Kartlegging og GAP-analyse:	• Gjøre GAP-analyse mot overordnede prosedyrer • Opprette tiltakslister for å tette GAP • Oppdatere prosedyrer og rutiner	Nygård	01.04.2019	Må avklares etter at øvrige dokumenter er ferdigstilt.
Ansvarsroller og arbeidsflyt:	Avklare beslutningskompetanse omkring GDPR med prosjektet	Nygård	01.12.2019	Avklart. OK
	Avklare med foretaksrevisor hvordan gjøre revisjon om makulering av kopier sykemeldinger samt om regelverket for arkivering av personalinformasjon følges	Nygård	01.01.2019	Pågående prosess.
	Avklare med Sekretariatet og DDT hvordan vi følger opp kravet om arkivering av personalinformasjon på epost, samt sikrer sletting av slik informasjon når den ikke lenger er nødvendig.	Nygård	01.01.2019	Pågående prosess.
Verktøy/maler:	Etablere rutine for sletting av roller når ansatte slutter eller endrer stilling, samt etablere bedre rutine for kontroll med tildelte roller i Personalportalen, Webcruiter og GAT.	Nygård	01.03.2019	Pågående prosess.

Opplæring:	• Arrangere foredrag for HR personell	Nygård		Gjennomføres i februar 2019
	• Sende ut informasjon til ledere i HR-Nyhetsbrev	Nygård		Informasjon sendes ut i februar 2019
Oppdatering rutiner/prosedyrer:	• Utarbeidelse av Retningslinje for lagring og sletting av personopplysninger om ansatte	Nygård	04.12.2019	Avklart. OK
	• Utarbeide rutine for innsyn i personalmappe	Nygård	04.12.2019	Avklart at det ikke er behov for endring av overordnede innsynsrutine. Utarbeide egen intern rutine i HR pågår.
	• Oppdatere EQS-prosedyrer for rekruttering	Nygård	04.12.2019	Avklart. OK
Oppdatering skriv:	• Personvernerklæring ansatte	Nygård	04.12.2019	Avklart. OK
Oppdatering IKT systemer:	• Må sees i sammenheng med art. 30 kartlegging			Uavklart

EMH:

Kategori av oppgaver	Foreslåtte oppgaver basert på tidligere arbeid	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 protokoll	Egen forespørsel	EMH v/ Hilde/ Monique	Avventer	Delvis fylt ut
Kartlegging og GAP-analyse	Vurdere prosedyrer som berører personvern	EMH v/ Hilde/ Monique	31.01.19 (Tentativ frist)	Det er ønskelig å vurdere våre prosedyrer mot OUS sine prosedyrer (pågående prosess v/ OUS) Gjelder sentrale og overordnede prosedyrer under fagområdet Se eget skjema
	Oppdatere prosedyrer der hvor resultat av vurdering tilsier det	EMH v/ Hilde/ Monique	15.06.19 (Tentativ frist)	Gjelder sentrale og overordnede prosedyrer under fagområdet Se eget skjema
	Utarbeide prosedyrer der hvor resultat av vurdering tilsier det	EMH v/ Hilde/ Monique	15.06.19	Gjelder sentrale og overordnede prosedyrer under fagområdet Se eget skjema
Deling og bruk av regionale prosedyrer for regional EPJ-standard	Vurdere om og hvordan regionale prosedyrer og brukerveiledninger ev skal tas i bruk ved Ahus	Fag-direktør	Pågående prosess	Ref. tema Kartlegging og GAP-analyse Publisering av regionale anbefalinger flyttes til RHF-ets EK-system januar 2019, uklart hvordan prosedyrer ev kan lastes ned og godkjennes i EQS derfra, avventer videre prosess
Ansvarsroller og arbeidsflyt	Vurdere om det er behov for egen matrise i forhold til ansvarsroller/arbeidsflyt opp mot de registrertes rettigheter	EMH v/ Hilde/ Monique	15.06.19 (Tentativ frist)	Vurdere behov for å utarbeide utkast til flytskjema for innsyn, retting, sperring, sletting
EPJ-systemer som ikke dekker regelverkets krav	Må sees i sammenheng med resultat av art. 30 kartlegging		Avventer	

Foretakssekretariatet:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	• Ansvar for å koordinere og oppdatere	Kåre	Løpende	Tar utgpk i mottatt info fra bestilling våren 2018. Pågående
	• Eget system for informasjonsinnhenting, oppbevaring og oppdatering (database)	Kåre	Q1 2019	I dialog med Lars Åge om ressurser
	• Nødvendige rutiner/prosedyrer for å ivareta krav til behandlingsprotokoll	Kåre	Q1 2019	Starter opp parallelt med arbeidet med å ferdigstille v1.0
	• Sende ut forespørsel art. 30 – oppfølging etter bestilling våren 2018	Kåre	Ved behov frem til 31.12.2018	Ferdigstilt
	• Ferdigstille v.1.0	Kåre	31.12.2018	Ferdigstilt
	• Informasjon ut i organisasjonen om protokollen, og når man skal melde inn nye register, hvordan og hva (intranett, Sak i shl (rapport fra prosjektet), foredragsrunde nivå 2, nyhetsbrev fra HR)	Kåre	1Q 2019	
Kartlegging og GAP-analyse:	• Prosedyrer og rutiner: Kartlegging av hva vi har, hva trengs å oppdateres og hva trengs av nye innen ansvarsområdet til foretakssekretariatet	Hilde	15.02.2019	Kartlegging er gjennomført og nødvendige oppdateringer er gjort. Løpende vurdering av evt nye behov
Ansvarsroller og arbeidsflyt:	• Utarbeide matrise forslag som behandles i prosjektet o Avvik o DPIA o innebygd personvern	 Maria Kåre Kåre	30.11.2018	Delvis ferdigstilt

	o rådgivning/anbefaling på PVO &IS opp mot andre hensyn	Kåre		
	• Forberedelse til utarbeidelse av styrende dokumenter			
	•			
Verktøy/maler:	• Innebygd personvern	Kåre	28.02.2019	Nærmer seg ferdig
	• Brevmaler avvik	Maria	30.11.2018	Ferdigstilt
	• DPIA forskning	Kåre	30.11.2018	V. 01 ferdigstilt
	• DPIA andre prosjekt, leveranser	Kåre	løpende	Ferdigstilt
Opplæring:	• Ledere (ny som leder, HR nyhetsbrev) og systemeiere (presentasjon i alle divisjons/klinikkledergrupper)	Maria	Pågående	Pågående – har ikke mottatt svar fra alle på invitasjon
	• PVO allmøte/alle ansatte?	Maria		Må vurderes etter opprettelse av intranettside
	• E-læringsprogram	PVO Hilde S	Q2 2019	
Oppdatering rutiner/prosedyrer:	• Overordnede prosedyrer/rutiner (styringssystem for personvern)	Maria	28.02.2019	
	• P360	Monica	Q1 2019	Pågår
	• Utarbeidelse/oppdatering av rutiner/prosedyrer	De som jobber innen fagområdet	31.03.2019	Avhengig av god kartlegging
Oppdatering skriv:	• Intranett og Ahus.no om personvern og personvernombudets rolle og ansvar	Maria		
	• Personvernerklæring/policy	HR (ansatte) og EMH (pasienter og brukere)		Ansatte er på plass, men ikke for pasienter og brukere.
Oppdatering IKT systemer:	• Sees i sammenheng med Art. 30 protokoll			

Forskning:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	• Utarbeide egen protokoll mtp forskningsprosjekter	Alle avdelinger/ avd.leder	31.12.2018	Arbeid i gang
	• Art. 30 protokoll biobank?	Avd. for forskningsstøtte/ Randi Kristoffersen	01.03.2019	
Kartlegging og GAP-analyse:				
Ansvarsroller og arbeidsflyt:	• Avklaring mtp tilsyn og kontroll av forskningsprosjekter	Avd. for forskningsstøtte v/ Karin Vassbakk/ Lisbeth Johnsen	28.februar 2019	Må avklares med foretaksrevisjonen om hvilke oppgaver som tilfaller avdeling for forskningsstøtte.
Verktøy/maler:	• DPIA forskning	Egen arb. Gruppe / Line M. Samuelsen og Mariann G. Davidsen	Pågående	Arbeidsgruppen er i gang, jobber med mal og beslutningsprosess DPIA forskning.
	• **Mal for å svare ut innsynsbegjæringer evt andre henvendelser?**	Egen arb. Gruppe v / Line M. Samuelsen	31.01.2019	Avventer at overordnet prosedyrer og mal for innsynsbegjæringer er klar før det kan utarbeides spesifikt for forskningsområdet.
	• Mal for endringsmeldinger	Avd. for forskningsstøtte/ Line m.	31.12.2018	Lagt ut mal for

		Samuelsen, Mariann G. Davidsen, Randi Kristoffersen		endringsmeldinger på nettside for eSkjema. Alle endringer som innebærer personvern må sendes inn som endringsmelding til personvernrådgiver.
Opplæring:	• Foredrag forskere/ prosjektledere	Avd. for forskningsstøtte Alle forskningsrådgivere/personvernrådgiver	29.11.18	Må senest være gjennomført innen 15.12.18
	• E læring?	GDPR prosjektgruppen?	Fremtidig	Lage moduler for e-læring innen flere områder. Kommer dette overordnet fra GDPR prosjektgruppen?
Oppdatering rutiner/prosedyrer:	• De registrertes rettigheter (EQS)	Avd. for forskningsstøtte Line M. Samuelsen	31.01.2019	Må avvente overordnet prosedyre på Ahus
	• Innhenting og håndtering av samtykke (EQS)	Avd. for forskningsstøtte Line M. Samuelsen	31.01.2019	Utarbeidet en prosedyre, må få avklart med jurist før den kan legges ut i EQS og brukes
	• Organisering av pvo forsking - saksflyt	Avd. for forskningsstøtte Line/Lisbeth/Karin	31.01.2019	Under omorganisering hos avdeling for forskningsstøtte
Oppdatering skriv:	• Samtykkeskriv (basert på REK mal)	Line	Etablert	Bruker REK mal
	• Informasjon ut i ikke-samtykkebaserte prosjekter	Line M. Samuelsen	Januar/februar 2019	Må finne en løsning mtp å informere om disse studiene på aktuell nettside? Enkeltstående vurderinger i prosjektsøknader gjøres av personvernrådgiver fortløpende.
Oppdatering IKT systemer:	• Må sees i sammenheng med art. 30 protokoll	Karin Vassbakk /Lisbeth Johnsen	31.01.2019	Pågår arbeid ut i avdelingene frist 31.12.2018 med mulighet

				for forlengelse ved behov. Må isåfall meldes fra.

DDT:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	**Egen forespørsel**	Janne, Cecilie og Hege	01.01.2019	Delvis besvart
Kartlegging og GAP-analyse:	**Prosedyrer/rutiner som berører personvern**			
	Kartlegge hvilke DDT-rutiner som er relevante	Cecilie og Hege med innspill fra avdelingene	01.01.2019	
	Gjøre GAP-analyse mot overordnede prosedyrer			
	Opprette tiltakslister for å tette GAPs			
	Oppdatere prosedyrer og rutiner		01.04.2019	
Ansvarsroller og arbeidsflyt:	**Egen ansvarsmatrise for endringshåndtering**			
	Kartlegge prosess for endring som involverer SP	Saeed/Cecilie/Hege		
	Workshop (WS) med SP for gjennomgang av endringsprosess			
	Oppdatere prosedyre/forespørselskjema i tråd med resultater fra WS prosedyrer/retningslinjer			
Verktøy/maler:	**Risikovurdering av MTU opp mot informasjonssikkerhet og personvern**	Trine Brenna	Frist satt av prosjekteier	Egen prosjektplan

Opplæring:	**Foredrag merkantilt personell**		Siste frist for gjennomføring 15.12.18	
	Ferdigstille foredrag	Cecilie og Hege	04.12.2018	
	Kalle inn relevant personell	Cecilie og Hege	04.12.2018	
	Gjennomføre opplæring	Cecilie og Hege	15.12.2018	
	Forberede foredrag for annet personell	Cecilie og Hege		
	Kalle inn relevant personell	Cecilie og Hege		
	Gjennomføre opplæring	Cecilie og Hege	01.04.2019	
Oppdatering rutiner/prosedyrer:	Se punkt under kartlegging/ GAP-analyse			
Oppdatering skriv:	Se punkt under kartlegging/ GAP-analyse			
Oppdatering IKT systemer:	Må sees i sammenheng med art. 30 kartlegging	Janne, Cecilie og Hege		

Kommunikasjon:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	• Er Kommunikasjon eier av noen systemer (nei	Svend		Ikke behov
Kartlegging og GAP-analyse:	• Kartlegging av rutiner/prosedyrer som er relatert til personvern	Geir	Vår 2019	

	• Finne ut av behov for nye rutiner/prosedyrer	Geir	Vår 2019	
	• Kartlegging av (samtykke)skriv/kontrakter som er relatert til personvern og om disse er i samsvar med GDPR	Geir	Vår 2019	
Ansvarsroller og arbeidsflyt:	N/A			
Verktøy/maler:				
Opplæring:	• Utarbeide intranettside basert på notater tilsendt	Svend	fortløpende	Går «live» så fort all har levert
	• Assistanse i forhold til øvrig opplæring på forespørsel	Svend	N/A	
Oppdatering rutiner/prosedyrer:	• Oppdatering av rutiner/prosedyrer som ikke er i samsvar med GDPR	Geir	Vår 2019	
	• Utarbeide nye rutiner/prosedyrer der det er kartlagt behov	Geir	Vår 2019	
Oppdatering skriv:	• Oppdatering av (samtykke)skriv/kontrakter der et er kartlagt behov	Geir	Vår 2019	
Oppdatering IKT	N/A			

systemer:				

DFM:

Kategori av arbeidsoppgaver:	Foreslåtte arbeidsoppgaver basert på tidligere arbeid:	Ansvarlig	Foreslått frist	Kommentar/status
Art. 30 Protokoll:	• Egen besvarelse levert 2018			Ferdig utfylt
	• Oppdatere ved behov etter gjennomgang av system og endring av informasjon som «lagres»		01.06.2019	
Kartlegging og GAP-analyse:	• Kartlegge hvilke prosedyrer vi har som berører personvern i forhold til våre ulike systemer	DLG – Ruth Ann og Rune bistår	01.04.2019	Tidsplan utarbeides internt – ansvarlig Ruth Ann
	• Oppdatere/utarbeide nødvendige prosedyrer og rutiner, på bakgrunn av kartlegging	DLG	14.06.2019	
Ansvarsroller og arbeidsflyt:	• Definere ansvarsroller for de ulike systemer (Eiere, databehandlere, etc, innsynsansvarlige…)	DLG		
	• DPIA	DLG – Rune og Ruth Ann bistår	Q3	Konsulentbistand?
Verktøy/maler:	• Se under pkt. prosedyrer			

Opplæring:	• Opplæring av ledere (nivå 3-5)		Q1	Nivå 3 utført av Maria i DLG 16.01.2018
	• Opplæring av personell med særskilt ansvar		Q1	Personell med ansvar for tilganger/utlevering
	• Opplæring av øvrig personell		Q3	E-læring sentralt
Oppdatering rutiner/prosedyrer:	• Utarbeidelse av nye rutiner/prosedyrer	DLG	14.06.2019	
	• Oppdatering av rutiner/prosedyrer	DLG	14.06.2019	
	• Utarbeide prosedyre/mal for behandling av innsynsbegjæringer/anmodning av sletting av opplysninger innen divisjonen	DLG	14.06.2019	Felles prosedyre med lokal tilpasning av mal
	• Innhente evt. samtykke som mangler	DLG	Q3	
Oppdatering skriv:				
Oppdatering IKT systemer:	• Avklares ved gjennomgang av systemer, og der vi avdekker behov for endringer for å oppfylle lovkrav		14.06.2019	

AKERSHUS UNIVERSITETSSYKEHUS

Strategi for personvern og informasjonssikkerhet 2019 - 2022

Det handler om tillit og respekt

Personvernombudet og informasjonssikkerhetsleder

09.01.2019

Innholdsfortegnelse

1 Innledning

1.1 Om strategi for personvern og informasjonssikkerhet

«*I tiden fremover vil det være enorme muligheter knyttet til digitaliseringen av samfunnet, men dette vil også intensivere bruken av folks opplysninger i en helt annen skala enn vi har sett tidligere. Det oppleves, og vil gjøre det i stadig større grad fremover, juridiske og etiske dilemmaer hvor potensialet for betydelig samfunnsgevinst må veies opp mot grunnleggende personvernhensyn*»[1].

For Ahus sitt vedkommende vil slik samfunnsgevinst kunne eksemplifiseres i utvikling av nye medikamenter, nye IKT-systemer, standardiserte pasientbehandlingsforløp, metoder og tjenester som kommer pasientene til gode, og der personopplysninger og digitaliserte løsninger er kritiske komponenter for å hente ut gevinstene. I tiden fremover vil Ahus derfor måtte ta stilling til og veie opp gevinstene ved f. eks digitalisering av pasientbehandlingsforløpene opp mot personvern og informasjonssikkerhet.

For Ahus er personvern og informasjonssikkerhet blant de viktige bærebjelkene for å kunne yte profesjonelle og tillitsvekkende helsetjenester. Befolkningen i vårt opptaksområde og brukere av våre tjenester forventer at vi har god styring og kontroll på opplysningene de gir fra seg. Våre pasienter og brukere forventer at opplysningene er riktige og tilgjengelige, at vi ikke bruker deres opplysninger til mer enn vi skal og at kun personer med tjenstlig behov får tilgang til deres opplysninger.

I tillegg til befolkningens og brukernes forventninger, har også egne ansatte, ledelsen, det regionale helseforetak og tilsynsmyndigheter forventninger til oss som sykehus.

1.2 Hensikten med strategi for personvern og informasjonssikkerhet

Hensikten med en strategi for personvern og informasjonssikkerhet er å lage en plan for og understøtte utviklingsplanen til Ahus sine uttrykte hovedmål samt øke bevisstheten og forståelsen av fagområdet i organisasjonen. Strategien skal være et styrende plandokument og bidra til at det kan arbeides planmessig og strukturert på overordnet nivå over tid for å nå våre mål innen personvern og informasjonssikkerhet. Dette er vi avhengig av for å kunne bygge en god kultur i alle ledd innen personvern og informasjonssikkerhet. Innholdet i denne strategien beskriver noen sentrale satsningsområder de kommende årene.

Følgende forhold vil i ulik grad kunne påvirke fagområdene personvern og informasjonssikkerhet:

- Krav til høyere produktivitet, effektivisering av pasientforløp og forbedret pasientbehandling
- Krav til konsolidering av IKT løsninger og modernisering av infrastrukturen i regionen
- Nye teknologiske løsninger
- Høyere krav og forventninger til forskning og innovasjon
- Nye regulatoriske krav
- Digitale innsynstjenester

[1] Fra Datatilsynets høringssvar på innspill til mandat for Personvernkommisjonen

Nye rettslige reguleringer, som f.eks personvernforordningen, setter krav om å ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette medfører et behov for å vurdere endringer i arbeidsprosesser og ressursbruk. De neste årene vil infrastrukturplattformen til Ahus og regionen oppgraderes, noe som vil føre til krevende prosesser for og tilstrekkelig ivareta personvernet og informasjonssikkerheten. Også forskningsprosjekter vil kreve mye av personvernområdet i årene fremover.

Samtidig som det er viktig å fokusere på digitalisering, er det vel så viktig å fokusere og forsterke kulturen og bevisstheten i Ahus knyttet til informasjonssikkerhet og personvern i vårt daglige virke. Dette vil forsterke holdninger til de ansatte, slik at alle blir mer bevisst på og ikke legge igjen pasientopplysninger i åpne rom, sende pasientopplysninger til feil personer o.l. Det er viktig å se forbedringsmuligheter i de daglige aktivitetene vi gjør, samtidig som vi planlegger for de kommende fabelaktige mulighetene teknologien gir oss.

Denne strategien vil derfor være et viktig virkemiddel for å organisere og skalere arbeidet med personvern og informasjonssikkerhet slik at vi møter morgendagens behov og krav, samtidig som virksomhetens risiko kan håndteres på en tilfredsstillende måte.

2 Organisering og arbeidsmåte

Personvernombud (PVO) og informasjonssikkerhetsleder er to fulltidsstillinger organisert i Foretakssekretariatet med linje rett til administrerende og viseadministrerende direktør. Enhet for forskning og innovasjon har ansatt en personvernrådgiver som har det operative ansvaret for personvern på forskningsområdet. Divisjon for diagnostikk og teknologi har ansatt en informasjonssikkerhetsrådgiver som har det operative ansvaret med informasjonssikkerhet innen IKT-løsninger.

I strategiprosessen er det fremkommet et mål og ønske om at PVO og informasjonssikkerhetsleder skal jobbe mer langsiktig og strategisk på et overordnet nivå. Gjennom dette kan de bistå ledelse i foretaket i strategiske beslutninger. Dette krever høyt kompetansenivå og tid til å jobbe langsiktig. De som tar strategiske beslutninger må oppleve at PVO og informasjonssikkerhetsleder kommer med gode råd og innspill slik at man kan ta kvalifiserte avgjørelser.

Det er behov for gode saksbehandlingsrutiner av innkommende henvendelser, og etablere gode forløp for saksbehandlingen. PVO og informasjonssikkerhetsleder må sitte på god veilederkompetanse samtidig som organisasjonen må læres opp til hvordan og når slike henvendelser skal komme. Det må skilles mellom de korte forespørsler og spørsmål knyttet til strategiske avgjørelser.

PVO og informasjonssikkerhetsleder må være organisert på en måte som gjør at beslutningstakere i organisasjonen ber om veiledning og lytter til råd som gis.

PVO og informasjonssikkerhetsleder har ikke bare en rådgivende funksjon, men også en kontrollfunksjon. De skal sikre etterlevelse av personvernet og ivareta informasjonssikkerheten i virksomheten. Det må lages gode rutiner for hvordan slike kontroller skal gjennomføres og planer for hva som jevnlig skal kontrolleres.

Ahus skal:

- Utarbeide og implementere styringssystem for informasjonssikkerhet og personvern
- Utarbeide informasjon om hvilke tjenester PVO og informasjonssikkerhetsleder kan tilby ut i organisasjonen (synliggjøring av funksjonene)
- Styrke tilsyns- og kontrollfunksjonen på fagområdene
- Utarbeide gode forløp for saksbehandling

3 Digitalisering av Ahus

Ahus som resten av samfunnet gjennomgår en økende digitalisering. Det teknologiske skiftet innebærer endringer også i måten vi jobber på og hvordan vi gjennomfører pasientbehandling. Dette betyr i praksis at fagområdene personvern og informasjonssikkerhet blir særlig viktige. Flere avdelinger starter prosjekter der pasientene får behandling hjemme og selv utfører målinger digitalt som rapporteres til behandler. Slik behandling innebærer også økt samhandling mellom pasienten, kommunehelsetjenesten og helseforetaket - noe som betyr større utfordringer med hensyn til journaltilgang og ytterligere bruk av velferdsteknologi.

Strategiprosessen har avdekket et ønske om en tydeligere interesseavveining mellom pasientsikkerhet og personvernet. Flere opplever at pasientsikkerheten ikke veies tungt nok i beslutninger der informasjonssikkerhet og personvern er med i vurderingene. Det kan synes å være en oppfatning at tilgang til journal må veies tyngre enn personvern og informasjonssikkerhet nettopp fordi tilgang til journal styrker pasientsikkerheten og det å kunne yte nødvendig helsehjelp.

Videre har interesseavveiningen mellom pasientens personvern og ansattes personvern også vært et tema i strategiprosessen. Det er en oppfatning om at ansattes personvern ikke veies i tilstrekkelig grad opp mot personvernet til pasientene og da særlig i forhold til digitalisering av tjenester (f.eks innsyn i logg).

Mange synes å være av den oppfatning at den største personvernrisikoen ved foretaket er menneskelig svikt ved blant annet behandling av fysisk papir. Derfor kan digitalisering bidra til å redusere personvernrisikoen.

Ahus skal:

- Arbeide for tidligere involvering av fagområdene personvern og informasjonssikkerhet i digitaliseringsprosjekter
- Styrke forståelsen av hvordan digitalisering påvirker interne arbeidsprosesser og resultater av arbeidet
- Sikre tettere og tidligere samarbeid mellom fagmiljøene helse, jus og IKT i utvikling av nye systemer, løsninger og tjenester

4 Gode prosesser for risikohåndtering

Kjennskap til og håndtering av risiko er en sentral komponent i arbeidet med personvern og informasjonssikkerhet. Dokumentasjon av risiko skal brukes for å dokumentere behov for tiltak og styrken på de enkelte tiltakene. Utfordringen med metoden som brukes for å dokumentere risikovurderinger i dag er at selve vurderingene fremstår som subjektive og uten veldefinerte beskrivelser av hvordan sannsynlighet og konsekvens skal vurderes. Det kommuniseres ikke i tilstrekkelig grad at det er fremtidige og potensielle sikkerhetsbrudd som vurderes og ofte kommer ikke avveininger mellom pasientsikkerhet og personvern godt nok frem.

Risikovurderinger blir svært ofte brukt for å vise at virksomheter tar ansvar for egen risiko. I outsourcingssaken til Helse Sør-Øst ble manglende risikovurderinger brukt som argument for å påvise at ledelsen ved sykehusene ikke tok ansvar for egen risiko. Det er derfor sentralt for Ahus å beskrive risiko på en slik måte at fremstillingen gir mening og tiltakene er relevante.

Interne arbeidsprosesser bruker informasjon lagret i IKT-systemer, der vi benytter en hovedleverandør (Sykehuspartner) og mange mindre leverandører for drift og support av slike IKT-systemer. Risikovurderinger av slike interne arbeidsprosesser vil derfor kunne brukes til å stille tydelige krav og styre leverandørene våre på en god måte. I dag styres mange premisser fra vår hovedleverandør, og dette påvirker styringsmekanismene vi er avhengig av for håndtering av egen risiko.

Ahus skal:

- Styrke forståelsen av risiko ved å dokumentere hvilke informasjonsverdier vi har og hvilke trusler og sårbarheter som kan påvirke våre informasjonsverdier
- Styrke beslutningstakeres dokumentasjonsunderlag ved å synliggjøre konsekvens av brudd på personvern og informasjonssikkerhet
- Synliggjøre avveininger mellom pasientsikkerhet, personvern og andre forhold
- Synliggjøre og kommunisere prosessen for risikohåndtering

5 Kommunikasjon og bevisstgjøring

Personvern og informasjonssikkerhet er viktige områder for sykehuset. I strategiprosessen kom det frem at mange ledere er usikre hvordan man kan kontakte personvernombud og informasjonssikkerhetsleder. Det var også usikkerhet rundt hva disse kan bistå med i ulike prosesser. Det er også et behov for å heve den generelle kompetansen rundt temaene i organisasjonen som helhet og sikre en bevisstgjøring hos den enkelte ansatte, leder og systemeier.

Hoveddelen av avvik innfor personvern og informasjonssikkerhet skyldes menneskelig svikt. Eksempelvis glemmes utskrifter med pasientopplysninger i møterom og pasientopplysninger sendes til feil person. Ved å øke bevisstheten og arbeide for en bedre sikkerhetskultur og styrket personvern, vil antall menneskelige feil og uhell kunne reduseres.

For å nå målet om en bevisst, kompetent og lærende organisasjon på området er det behov for personvernombud og informasjonssikkerhetsleder å lære opp organisasjonen og i større grad synliggjøre fagområdene. I tillegg er det behov for å tydeliggjøre utfordringer knyttet til taushetsplikt, oppslag i journal (når oppslaget ikke gjelder direkte pasientbehandling), deling av erfaringer i forhold til pasientbehandlingen, bruke opplysninger i undervisning og læring og andre spørsmål som ansatte søker svar på.

Ahus skal:

- Styrke bevissthet og sikkerhetskultur til ansatte på Ahus
- Øke synligheten i organisasjonen ved å etablere og vedlikeholde en fagside på intranett der ansatte, linjeledere og systemeiere enkelt finner svar på spørsmål
- Styrke opplæringsprogrammer og informasjon om fagområdene som øker bevisstheten i organisasjonen

6 Internkontroll

Internkontroll innen personvern og informasjonssikkerhet skal dekke den interne styringen og kontrollen i vår virksomhet innen disse fagområdene. Måten internkontrollen gjennomføres på skal samsvare og tilpasses Ahus sine krav til internkontroll. Difi sin «veileder for internkontroll - informasjonssikkerhet i praksis» vil benyttes for utførelsen av aktivitetene.

Gjennomføring av aktiviteter relatert til internkontroll for personvern og informasjonssikkerhet vil typisk være ledelsens styring og oppfølging, risikovurdering og –håndtering, hendelseshåndtering, evaluering og revisjon, kompetanse- og kulturutvikling og skriftlig / muntlig kommunikasjon. Ulike roller er involvert i internkontrollarbeidet, der ansvaret fordeles slik at noen sørger for at oppgavene gjøres, noen utfører de konkrete oppgavene, og noen påser at oppgaven er utført. Det er viktig at fordelingen av dette ansvaret er tydelig og kommunisert.

Ahus skal:

- Innta personvern og informasjonssikkerhet i årlig gjennomgang av styringssystem for internkontroll som gjennomføres på alle nivå i organisasjonen
- Styrke arbeidet med å strukturere og planlegge oppgaver knyttet til personvern og informasjonssikkerhet
- Tydeliggjøring av roller og ansvar i arbeidet med internkontroll, i særlig grad skille mellom kontrollfunksjoner, utøvende funksjoner og beslutningsfunksjoner

7 Forhold til eksterne samarbeidspartnere

Vi skal være en kompetent kravstiller til våre leverandører, og vi skal ta sterkt eierskap for håndtering av egen risiko. Vi skal være en aktiv premissgiver og ikke en passiv mottager.

Ahus sitt ansvar for behandling av personopplysninger fremkommer svært tydelig i Datatilsynets endelige vedtak etter Helse Sør Øst sin outsourcingssak: «*Lovpålagte krav om klare ansvarslinjer, sikkerhetsledelse, ledelsesforankring og kontroll er nødvendige for å sikre at den behandlingsansvarlige behandler personopplysninger i samsvar med prinsippet om ansvarlighet.*». Selv om regionen koordinerer initiativ og prosjekter på tvers av flere helseforetak, fritar ikke dette Ahus for å håndtere egen individuell risiko og ansvar.

Ahus deltar i flere regionale fagråd og ulike fora. Dette er viktige arenaer for faglig koordinering, og å kunne påvirke det regionale samarbeidet i ønsket retning.

Ahus skal:

- Kreve at våre eksterne samarbeidspartnere setter personvern i fokus blant annet gjennom innebygget personvern i løsninger.
- Styrke vår kontrollfunksjon for oppfølging av eksterne leverandører
- Være en tydelig og profesjonell kravstiller overfor regionale prosjekter og eksterne leverandører.

HELSE SØR-ØST

Helse Sør-Øst RHF Telefon: 02411
Postboks 404 Telefaks: 62 58 55 01
2303 Hamar postmottak@helse-sorost.no
Org.nr. 991 324 968

Akershus universitetssykehus HF
Postboks 1000
1478 LØRENSKOG

v/administrerende direktør Øystein Mæland

Vår referanse:
15/00270-23

Deres referanse:

Dato:
22.01.2019

Saksbehandler:
Torun Melhus Vedal

Oppsummering fra oppfølging av revisjoner

Vi viser til brev av 30. oktober 2018 om oppfølging av tiltaksarbeidet som Akershus Universitetssykehus HF (Ahus) har igangsatt etter følgende utførte revisjoner:

- *Legemidler* (rapport 12/2016)
- *Tiltaksarbeid etter revisjoner utført av konsernrevisjonen* (rapport 4/2017)

Konsernrevisjonen gjennomførte 29. november 2018 et oppfølgingsmøte med de ansvarlige for forbedringsarbeidet etter revisjonene i Ahus, og har i tillegg fått tilsendt dokumentasjon på gjennomførte og pågående tiltak.

Revisjon *Legemidler* omhandlet Ahus sin interne styring og kontroll knyttet til anvendelse av kostbare legemidler. Rapport fra revisjonen og administrasjonens handlingsplan ble styrebehandlet ved Ahus 14. desember 2016. Konsernrevisjonen har også tidligere gjennomført oppfølging av revisjon *Legemidler*, ved møte 12. januar 2018. På det tidspunktet var sentrale deler av forbedringsarbeidet pågående, og i møtet 29. november 2018 ble det presentert oppdatert status på dette. Det er konsernrevisjonens vurdering at Ahus har prioritert forbedringsarbeidet. Tiltakene i etterkant av revisjonen er i all hovedsak gjennomført, og er i tråd med anbefalingene som fremkom i revisjonsrapporten.

Revisjon *Tiltaksarbeid etter revisjoner utført av konsernrevisjonen* omhandlet helseforetakets system for oppfølging av revisjoner. Rapport fra revisjonen og helseforetakets handlingsplan ble styrebehandlet ved Ahus 18. mai 2017. Konsernrevisjonens vurdering er at det er gjennomført et godt forbedringsarbeid på de områdene som revisjonen omfattet. Tiltakene i handlingsplanen er i all hovedsak gjennomført.

Resultatet fra konsernrevisjonens oppfølging vil inngå i en samlet rapportering til styrets revisjonsutvalg i Helse Sør-Øst RHF. Konsernrevisjonen planlegger ikke videre oppfølging av revisjonene *Legemidler* og *Tiltaksarbeid etter revisjoner utført av konsernrevisjonen* i Ahus.

Med vennlig hilsen
Helse Sør-Øst RHF

Espen Anderssen
konsernrevisor

Torun Melhus Vedal
internrevisor

Kopi: Administrerende direktør Cathrine M. Lofthus