AKERSHUS UNIVERSITETSSYKEHUS

Styresak

Dato dok.:	14.04.2020	Administrerende direktør	
Møtedato:	22.04.2020		
Vår ref.:	20/02340-2	Postadresse:	1478 LØRENSKOG
		Telefon:	+47 67 96 00 00

Sak 29/20 Administrerende direktørs orienteringer

Administrerende direktør ønsker å orientere om følgende saker:
1. Uønskede hendelser innen personvern 2019
2. Tilsyn og revisjoner

Administrerende direktørs innstilling til vedtak:

Styret tar saken til orientering.

Øystein Mæland
Administrerende direktør

Dokumentet er elektronisk godkjent

1. Uønskede hendelser innen personvern 2019

I det videre vises en gjennomgang av avvik innen personvern og informasjonssikkerhet som ble meldt gjennom EQS i 2019. Dette er saker som håndteres av informasjonssikkerhetsleder og personvernombudet. Det kom inn 244 meldinger om uønskede hendelser innen personvern og informasjonssikkerhet i 2019. Tilsvarende tall for 2018 var 157, og i 2017 var det 103 meldinger.

Kategorisering av avvik

Avvik er en uønsket hendelse som er i strid med gjeldende regelverk. Det kan for eksempel være brudd på helselovgivningen, personvernregelverket, eller det kan være brudd på foretakets interne rutiner. For å forenkle hva et avvik er, kan man grovt sett kategorisere dem i tre kategorier; integritet (i), tilgjengelighet (ii) og konfidensialitet (iii).

i. Brudd på integritet vil si at det har skjedd en utilsiktet eller ulovlig endring av opplysninger. Det har innkommet få avvik i denne kategorien. Eksempel på slike avvik er hvor autorisert personell endrer opplysningene ved uhell/overlegg.

ii. Brudd på personopplysningers tilgjengelighet er tilfeller hvor det har vært et utilsiktet eller ulovlig tap av tilgang til, eller tilintetgjøring av opplysninger. Eksempler på slike brudd kan være hvor autoriserte brukere ikke får tilgang til systemer, eller tilfeller der opplysninger permanent blir tapt eller tilintetgjort. Planlagt systemvedlikehold, hvor opplysninger ikke er tilgjengelig i et begrenset tidsrom, er imidlertid ikke et avvik.

iii. Brudd på konfidensialitet vil si at det har vært en utilsiktet eller ulovlig utlevering av eller tilgang til opplysninger. Avvik som innkommer av denne typen, er ofte hendelser hvor utgående brev inneholder feil, for eksempel at brevet er adressert til feil henvisende lege, eller at brevet inneholder opplysninger om en annen pasient enn den pasienten brevet er stilet til. Dette kan også være avvik der ansatte, som har gått over i annen stilling, har tilganger til systemer den ikke lenger skulle hatt tilgang til. Fellestrekket for disse avvikene, er at det har forekommet brudd på taushetsplikten etter helsepersonelloven.

Et avvik kan omfatte én, eller en kombinasjon av disse tre kategorier av brudd.

Nedenfor vises en oversikt over innkomne avviksmeldinger fra mai – desember 2019.

Måned	Reelt antall avvik i kategorien (avvik totalt*)	Integritet**	Tilgjengelighet**	Konfidensialitet**
Mai	25 (28)	2	9	16
Juni	22 (25)	2	3	18
Juli	7 (14)	0	3	4
August	13 (15)	1	3	11
September	27 (29)	2	7	18
Oktober	30(31)	4	8	21
November	13(14)	1	0	12
Desember	23 (27)	6	2	17

* Noen avvik er meldt i feil avvikskategori, og derfor er det en differanse mellom totalt antall meldte avvik og reelt antall avvik innen kategorien personvern og informasjonssikkerhet.
** Et avvik kan omfatte én, eller en kombinasjon av disse tre kategorier av brudd. Derfor stemmer ikke summen av disse med reelt antall meldte personvern- og informasjonssikkerhetsavvik for måneden.

Flertallet av avvikene gjelder brudd på konfidensialitet – at uvedkommende har fått tilgang til sensitiv informasjon om pasienter, som vedkommende ikke skulle ha hatt tilgang til. Som regel gjelder det forlagte dokumenter eller feilsendinger internt, enten gjennom systemer, via

internposten eller gjenglemte dokumenter på møterom eller lignede. Noen ganger er også pasientinformasjon gjort tilgjengelig for uvedkommende utenfor foretaket. Dette skjer ofte ved feilsendinger av brev. Avvikene viser at man må ha gode rutiner ved postutsendelser der man avslutter en oppgave, før man tar fatt på den neste.

Det har også forekommet brudd på tilgjengeligheten, ved nedetid av systemer som ikke gjennomgår planlagt vedlikehold. Integritetsbrudd har også forekommet ved at vi har hatt feil telefonnummer registrert på pasient eller notert feil henviser, slik at timeinnkallinger eller prøvesvar er sendt uriktig mottaker.

Det er i den senere tid gjort flere endringer hva gjelder håndtering av uønskede hendelser innen personvern og informasjonssikkerhet:

- Det er gjort endringer i EQS-rutinen for personvern og informasjonssikkerhet hva gjelder fristen meldingsansvarlig har til å starte håndteringen av avviksmeldingen. Dette for å etterkomme lovkravet om at brudd på personopplysningssikkerheten som utgjør moderat eller høy risiko for de registrertes rettigheter eller friheter, skal meldes til Datatilsynet innen 72 timer.
- Når man melder uønskede hendelser i EQS innen personvern og informasjonssikkerhet, er det nå flere felter til utfylling i skjemaet enn tidligere. Disse feltene er ikke obligatoriske å fylle ut, men dersom melder besitter informasjonen og fyller ut feltene, hjelper det oss med raskere å få den informasjon vi behøver for å kunne vurdere om det foreligger et brudd på personopplysningssikkerheten og i så fall alvorlighetsgraden av bruddet.
- Det er videre gjort endringer i påminnelser som sendes meldingsansvarlig per e-post etter at uønskede hendelser i denne kategorien er meldt. De mottar to e-poster der de får opplyst frister opp mot Datatilsynet. En frist sendes umiddelbart avviket er meldt, og opplyser om 72-timersfristen man har overfor Datatilsynet ved enkelte hendelser. Dernest sendes det en påminnelse 48 timer etter mottatt EQS-melding, som sier at det kun er 24 timer igjen til hendelsen kanskje skal meldes Datatilsynet.

<u>Uønskede hendelser som er meldt til Datatilsynet</u>
Det er meldt 37 avvik til Datatilsynet i 2019. Av de meldte avvikene, gjelder samtlige blant annet brudd på konfidensialitet, der personopplysninger er gjort tilgjengelig for uvedkommende, for eksempel ved feilsendinger av opplysninger i brev. Noen av konfidensialitetsbruddene, er også en kombinasjon av tilgjengelighets- eller integritetsbrudd.

For to av hendelsene som ble meldt i 2019 har Datatilsynet bedt om nærmere redegjørelse:

- Den ene saken gjelder avloggingsproblematikk knyttet til bruk av Regional Arbeidsflate, der en bruker får tilgang til en annen brukers mail og/eller arbeidsøkt i kliniske applikasjoner. Saken har vært behandlet i sykehusledelsen 13. august 2019, samt redegjort for i KPU nivå 1 18. desember 2019. Denne saken er nå avsluttet fra Datatilsynets side med følgende merknad:

Vi har forståelse for at Ahus i en overgangsfase med modernisering og oppgradering av infrastrukturen må ta i bruk løsninger som er felles for HSØ.

Vi synes likevel at det er beklagelig, siden vi tror deres sikkerhetstiltak var mer *effektive* (jf. artikkel 25) med hensyn til brukergruppene deres som er «mobile», og som må ha tilgang til fagsystemer fra flere og ulike lokaler og der endepunktet benyttes av differensierte yrkesgrupper som har ulikt tilgangsnivå. Vi tror også at deres sikkerhetstiltak er mer i henhold til *«state-of-the art»* (jf. artikkel 32 og 25). Vi forventer at endelig løsning og tilgang i HSØ, innfører sikkerhetstiltak som er effektive og er «state-of-the-art», og tilpasset brukergruppene i HF-ene som mobil yrkesgruppe.

- Den andre saken gjelder et forskingsavvik, der spørsmålet er om opplysninger har vært behandlet uten tilstrekkelig rettslig grunnlag. Vi har frist til 1. april 2020 med å besvare Datatilsynets krav om redegjørelse.

Det er videre tre saker fra 2019 der vi ikke har mottatt tilbakemelding fra Datatilsynet. Dette gjelder to systemavvik, samt et avvik innen forskning. De øvrige sakene fra 2019 er avsluttet fra Datatilsynets side, der de forutsetter at de tiltakene vi har iverksatt fungerer og at de er tilstrekkelige.

Avvikshåndtering ved Ahus

Det har vært en jevn økning i innkomne avviksmelding innen kategorien personvern og informasjonssikkerhet. Det foreligger ikke indikasjoner på at det skjer flere uønskede hendelser nå enn tidligere, men økningen skyldes trolig at meldekulturen har blitt bedre. Informasjonssikkerhetsleder og personvernombudet oppfordrer ansatte, blant annet i fora som Kontorfaglig kompetanseprogram og Ny som leder, å melde inn avvik. På den måten kan foretaket forbedre seg, og hindre at lignende hendelser skjer igjen. Det gis også tilbakemeldinger fra ansatte om at det fra lederhold har vært kommunisert at avvik skal meldes.

Det blir lagt merke til at foretaket har et velfungerende avvikssystem. Datatilsynet har under Normen-konferansen vist oversikt over mottatte avviksmeldinger fra helsesektoren, og trukket frem Akershus universitetssykehus. Av helseforetakene hadde Datatilsynet mottatt flest avviksmeldinger fra Akershus universitetssykehus. Datatilsynet har bekreftet at meldingene som mottas er relevante.

I personvernforum, der personvernombudene i Helse Sør-Øst samles, har andre personvernombud tilkjennegitt mangler ved avvikshåndteringen ved sine sykehus, og at dette er bakgrunnen for at de ikke melder avvik i særlig grad. Andre helseforetak ønsker å lære hvordan Ahus' avvikssystem er bygget opp. Det har blitt avholdt telefonmøte med personvernombud og informasjonssikkerhetsleder i Helse Bergen HF, som ønsker å lære hvordan rutine- og avvikshåndteringssystemet er bygget opp for uønskede hendelser innen personvern og informasjonssikkerhet.

2. Tilsyn og revisjoner

Statens helsetilsyn

Det er igangsatt tilsyn med medisinsk og helsefaglig forskning på mennesker. Bakgrunn for tilsynet er at tilsynsmyndigheten ofte ser at det svikter ved innhenting av forhåndsgodkjenning fra den regionale komiteen for medisinsk og helsefaglig forskningsetikk (REK), ved at vilkårene i REK-godkjenningen ikke følges, ved innhenting av informert samtykke fra deltakerne i forskningsprosjektene og i virksomhetenes styring og organisering av forskningen (internkontroll). Tilsynet skal gjennomføres som en egenvurdering med gjennomgang av 30 forskningsprosjekter fra de siste to årene, og gjennomgang av

virksomhetens organisering, oppgavedeling og etablerte rutiner. Fristen for oversendelse av dokumentasjon var 17.03.2020.

Konsernrevisjonen

Konsernrevisjonen skal gjennomføre en revisjon av behandling av personopplysninger. Målet er å vurdere om helseforetakene har utarbeidet en samlet oversikt over sin behandling av personopplysninger og om det er etablert prosesser for å holde oversikten oppdatert. Konsernrevisjonen vil også vurdere om oversikten legger til rette for standardiserte prosesser i helseregionen som helhet. Det ble gjennomført oppstartsmøte i mars, men på grunn av situasjonen med Covid-19 er videre arbeid utsatt inntil videre.

Riksrevisjonen

- Det skal gjøres en forvaltningsrevisjon av investeringer i bygg og medisinsk-teknisk utstyr (MTU) i helseforetakene. Målet er å undersøke om spesialisthelsetjenesten gjennom investeringer i MTU og bygg legger til rette for effektiv drift og god pasientbehandling. Resultatet planlegges rapportert til Stortinget våren 2021. Fristen for oversendelsen av dokumentasjon var 06.03.2020, og supplerende informasjon vil bli etterspurt i løpet av våren 2020. Utvalgte helseforetak vil bli valgt ut for intervjuer i løpet av høsten 2020.

- Videre gjør Riksrevisjonen en utvidet 3-årsoppfølging av medisinsk kodepraksis i helseforetakene. Hensikten er å undersøke hvilke tiltak som er iverksatt på bakgrunn av rapporterte funn og kontroll - og konstitusjonskomiteens merknader. Revisjonen er satt i bero inntil videre grunnet situasjonen med Covid-19.