UiO : Universitetet i Oslo
Enhet for intern revisjon

REVISJONSRAPPORT

Internkontroll klinikkdrift Psykologisk institutt (PSI)

Endelig rapport distribueres til:
Universitetsdirektøren
Dekan SV
Instituttleder PSI

Kopi:
Rektor

Gjennomført av Enhet for intern revisjon (EIR):
Seniorrådgiver Cecilie Thorberg
Seniorrådgiver Attilio Dell`Arte
Avdelingsdirektør Jørgen Bock

Blindern, 23.10 2017

SAMMENDRAG

Overordnet vurdering:
Helhetlig styring og kontroll ved virksomheten har ikke vært tilfredsstillende. Det er betydelige svakheter i internkontrollrutiner og etterlevelse av lover og regler. Det har ikke vært kontroll på hvem som har tilgang til personsensitive data. Journaler og helseregistre har vært åpne for betydelig flere enn det krav i lov og forskrifter tillater. Risikoen for uautorisert tilgang har eksponert pasienter og UiO for uønskede hendelser innen personvern. Det er iverksatt strakstiltak på området.

Det er på rapporteringstidspunktet ikke avklart om det er krav til konsesjon fra Datatilsynet vedrørende behandling av sensitive personopplysninger i undervisningsvirksomheten.

Det pågår et betydelig arbeid med å etablere rutiner og lukke svakheter. Tiltakene har ulik kompleksitet og omfang.

Årsakene til svakhetene skyldes etter vår vurdering mangel på helhetlig intern kontroll, ikke tydelige roller og ansvar og mangelfull kontrollbevissthet. Risikovurderinger er ikke utført og det er heller ikke stilt krav til det.

For oversikt over rapportens anbefalinger, se punkt 4 Vedlegg, bakerst i rapporten.

Innholdsfortegnelse

1 Bakgrunn og formål med revisjonen 4
1.1 Bakgrunn og formål 4
1.2 Revisjonskriterier 4
1.3 Metode/avgrensninger/omfang 4
2 Observasjoner 4
2.1 Fysisk sikkerhet 4
2.2 Internkontroll system / kvalitetsrutiner 5
2.3 Risikovurderinger 5
2.4 Roller og ansvar 6
2.5 Innføring av elektronisk journal 6
2.6 Rekruttering av pasienter 7
2.7 Tilgangskontroll pasientjournaler 8
2.8 Politiattester 9
2.9 Taushetserklæring 9
2.10 Samtykkeerklæringer 9
2.11 Spørsmål om konsesjonsplikt for bruk av helseopplysninger i undervisning 10
2.12 Melde- og konsesjonsplikt ved videopptak 11
2.13 Minnepinner 11
2.14 Årsaker 12
3 Om revisjonsrapporten 13
3.1 Om internrevisjonen 13
4 Vedlegg: Anbefalinger 14

1 BAKGRUNN OG FORMÅL MED REVISJONEN

1.1 Bakgrunn og formål

Universitetsdirektøren har bedt Enhet for internrevisjon (EIR) om å gå igjennom internkontroll[1] ved Psykologisk Institutts klinikkdrift (PSI). Oppdragsbeskrivelse ble godkjent 11.10.17. EIR skal kartlegge internkontroll ved klinikkdriften for å bidra i pågående vurdering av klinikkens drift og gi innspill til forbedringer.

1.2 Revisjonskriterier

Rammeverk for internkontroll, krav iht lover, regler og rutiner ved UiO.

1.3 Metode/avgrensninger/omfang

Prosjektet er gjennomført ved dokumentgjennomganger, besøk og intervjuer. Gjennomgangen dekker ikke juridiske og helsefaglige vurderinger. EIR har kun vurdert internklinikkene for voksne. Gjennomgangen er av tidshensyn avgrenset til underpunktene i kapittel 2. Revisjonen er gjennomført i perioden 11. til 18. oktober.

2 OBSERVASJONER

Flere av klinikkens utfordringer er tatt tak i av klinikkledelsen, PSIs ledelse og universitetsledelsen. Særlig de siste ukene er det etablert og planlagt mange risikoreduserende tiltak[2], herunder:

- Innføring av vaktordning på kveldstid (kl 16-18), slik at ikke studenter er alene ved behandling
- Begrense rekruttering av pasienter til dem som ikke er vurdert å være rettighetspasienter
- Etablert nettskjema for å få oversikt over behandlinger og hvem som er hvor og når
- Etablert nettskjema for avviksrutiner og klagebehandling
- Gjennomgått sidegjøremålsreglement, slik at privat praksis ikke skal utføres i UiOs lokaler eller med UiOs driftsmidler
- Igangsatt arbeid med å få oversikt over konsesjons- eller meldepliktige helseregistre/journaler
- Oppdatere kvalitetshåndbok
- Startet arbeid med klargjøring av roller og ansvar

Nye rutiner, som nettskjema for avvik og klager er ikke revidert, fordi det først ble etablert i oktober. Vi har sett på forhold som etter vår mening ikke er identifisert i tidligere gjennomganger eller som trenger ytterligere oppmerksomhet.

2.1 Fysisk sikkerhet

Klinikken har vært drevet uten god nok infrastruktur, som resepsjon og elektronisk booking. Pasienter har vært behandlet både av studenter i studentklinikkene og av ansatte i privat

[1] Krav og kriterier om internkontroll fremkommer av blant annet personvernlovgivning, kvalitets- og forbedringsforskriften og økonomireglementet. Vi benytter internkontroll i rapporten synonymt med virksomhetsstyring eller styring og kontroll. Et anerkjent rammeverk for internkontroll er COSO eller COSO ERM rammeverkene. (www.coso.org).

[2] Basert på tiltaksliste 12.10.17

regi. Studenter har behandlet pasienter alene eller sammen med veileder, unntaksvis også utenom ordinær arbeidstid.

Klinikklederne påpeker at studenter vanligvis behandler pasienter i klinikkens lokaler på dagtid, med veileder/ klinikkleder til stede. Etter en forsvarlighetsvurdering av behandlingsansvarlig (klinisk veileder) har studenter unntaksvis behandlet pasienter mellom 16.00 – 18.00. EIR har ikke hatt mulighet til å kontrollere dette.

Det er iverksatt tiltak for å styrke sikkerhet, jfr. tiltakene nevnt under 2 Observasjoner. Enhet for HMS og beredskap (HMSB) har imidlertid ikke vært involvert i særskilte sikkerhetsvurderinger for klinikkene.

Vurdering:
Risikoreduserende tiltak er innført, men vi mener likevel at HMSB bør involveres. Det bør også vurderes å konsultere eiendomsavdelingen for å avgrense og bedre tilrettelegge for virksomheten i lokalene, herunder forbedre resepsjonstjenesten.

Anbefaling:
- Det bør innhentes ytterligere bistand fra HMSB for å gjøre sikkerhets- og beredskapsvurderinger.
- Vurdere bistand fra eiendomsavdelingen for praktisk og sikker innretning av klinikk.

2.2 Internkontroll system / kvalitetsrutiner
Det er utført et betydelig arbeid med å dokumentere, foreslå og innføre nye internkontroll rutiner. Imidlertid er de nye rutinene dels under innføring og dels ikke avklart. Kvalitetshåndboken er ufullstendig, ikke oppdatert og ikke godt strukturert.

Vurdering:
Videreutvikling og drift av et tilfredsstillende internkontrollsystem er tidkrevende og omfattende, og krever mer kapasitet og kompetanse enn det PSI har for øyeblikket. Hvis internkontrollsystemet ikke er godt nok vil flere risikoer kunne oppstå, for eksempel som følge av uklare oppgaver og ansvarsområder eller at risikoer ikke blir fulgt godt nok opp. Et effektiv internkontrollsystem krever mer enn bare etterlevelse av lover og regler. Det må understøttes av kultur og et godt internt miljø.

Anbefaling:
- Styrke administrativ kapasitet.
- Styrke kompetanse om internkontroll og sikkerhet for ansatte og studenter.
- Etablere og vedta kvalitets-/internkontrollsystem, herunder kvalitetshåndboken
- Det bør settes opp tidsplan og ansvarlige for tiltaksliste etter midlertidig stenging, herunder for den helhetlige oppfølgingen.

2.3 Risikovurderinger
I henhold til krav i lover, forskrifter og anerkjent praksis innen virksomhetsstyring skal risikovurderinger utføres jevnlig. Risikovurderinger er en systematisk, dokumentert prosess der hendelser som truer virksomhetens mål identifiseres, prioriteres og tiltakssettes. Mål omfatter strategiske mål, driftsrelaterte mål, etterlevelse av lover og regler og mål knyttet til fullstendig og korrekt rapportering. Det er ikke utført risikovurderinger verken hos PSI eller på fakultetet, ut over ROS analyse på fakultetet utført med bistand fra HMSB.

Vurdering:
Risikovurderinger bør gjennomføres og oppdateres jevnlig. Årsaken til at risikovurderinger ikke er utført er at det ikke er stilt krav om det fra fakultetet og fordi risikostyring ikke er fullt ut iverksatt i tråd med anbefalinger fra DFØ på fakultetet og ved UiO.

Anbefaling:
- Risikovurderinger bør gjøres 1-2 ganger i året eller oftere ved behov, for å vurdere og følge opp om risikoreduserende tiltak har tilstrekkelig effekt.
- Fakultetet bør etterspørre kortfattede risikovurderinger fra underliggende enheter.
- LOS bør etterspørre kortfattede risikovurderinger fra fakultet.

2.4 Roller og ansvar
Tydelige roller og ansvar er en grunnleggende forutsetning for tilfredsstillende internkontroll. Roller og ansvar er ikke tilstrekkelig definert, vedtatt og implementert. Det omfatter ansvaret til veileder, klinikkleder, fagavdelingsleder, undervisningsleder, forskningsleder, instituttleder, fakultet og universitetsledelsen.

Vurdering:
Det bør tydeliggjøres hvem som har ansvaret for hele virksomheten til klinikken(e) og hva det omfatter. Det bør tydeliggjøres at i ansvaret inngår ikke bare et fagansvar, men også ansvar for at administrative rutiner og systemer følger lov, forskrift og UiOs rutiner. Det innebærer ansvar for klinikkens internkontroll (virksomhetsstyring) i stort. Ansvaret inkluderer å etablere tilfredsstillende internkontroll og ikke minst følge opp at dette fungerer tilfredsstillende. Ansvar for det påhviler alle nivåer fra institutt og fakultet, til universitetsledelsen og universitetsstyret.

Anbefaling:
- Roller og ansvar må tydeliggjøres i hele styringslinjen.
- Kvalitetshåndbok må forbedres mht roller og ansvar, jfr 2.2.

2.5 Innføring av elektronisk journal
Etter ny forskrift om IKT-standarder i helse- og omsorgstjenesten ble det innført et krav om elektronisk pasientjournal 1.9.2015.

PSI er i gang med å innføre elektronisk journal, et system utviklet av ansatte ved universitetet i Umeå. Systemet skal implementeres innen 1.1.2018. PSI er i ferd med å legge inn brukere og det er delvis tatt i bruk. Det har fremkommet synspunkter på at e-journal systemet som implementeres ikke er tilfredsstillende fordi:

- Det er begrensninger i antall ord som kan registreres
- Systemet vurderes ikke å være egnet til veiledning av studenter fordi endringsfunksjonalitet ikke er god nok, for eksempel slettemulighet
- Scanningfunksjonaliteten ikke er god nok
- Det ikke er god nok funksjonalitet for utskrift av sluttnotater og epikriser
- Det er ikke tilstrekkelig driftssupport

EIR er kjent med at systemet er lagt inn i TSD. På grunn av mangel på tid har ikke internrevisjonen hatt mulighet til å vurdere internkontrollen til løsningen, herunder hvem som er systemadministrator, hvordan tilgangsadministrasjon er, hvordan rutiner for logging er.

USIT vurderte om systemet kunne kjøres sikkert inne i TSD miljøet og har bistått ved implementeringen. Iht retningslinjene ved UiO for TSD skal systemeier forut for dette ha gjort

en generell risikovurdering og vurdert å gjøre en spesiell risikovurdering dersom fagspesifikke forhold ved prosjektet krever det. Det er ikke utført tilstrekkelige risikovurderinger av internkontroll og sikkerhet, og det ble heller ikke fanget opp av USIT. EIR får opplyst at USIT nå jobber sammen med PSI for å vurdere internkontroll som tilgangskontroller og logging.

Vurdering
Det er risiko for at innføring av system for e-journal ikke er god nok for å tilfredsstille funksjonelle krav. Det er usikkert om lovkrav til internkontroll og IT sikkerhet er oppfylt. Risikovurderinger av systemet mht internkontroll og sikkerhet er ikke gjort i tilstrekkelig grad ifm pilotering. Det er derfor risiko for at behandling av personopplysninger ikke er under tilfredsstillende kontroll ifm innføring og bruk.

PSI har etter EIRs mening førstelinjeansvaret for internkontroll. USIT har et andrelinjeansvar for internkontroll ved UiO. Årsaken til mangelfull risikovurdering er etter vår mening at det kan være gråsoner mellom hva som er fagansvar i førstelinjen, herunder internkontroll (funksjonelle krav) og hva som er et IT- og sikkerhetsansvar (såkalte «ikke- funksjonelle krav»), og at dette dermed «faller mellom to stoler».

Anbefaling:
- Målbilder og kravspesifikasjoner i ny IT-løsning bør tydeliggjøres og forankres, herunder sikre at systemet dekker funksjonelle krav og krav gitt i lov og forskrift
- Gå opp grensen mellom - og tydeliggjøre hva som er funksjonelle krav/ikke funksjonelle krav mht internkontroll / sikkerhet, herunder vurdere rutiner for å styrke internkontrollen i andrelinjen (USIT), for å fange opp tilfeller der førstelinjen ikke har gjennomført nødvendige internkontrolltiltak.

2.6 Rekruttering av pasienter
Vurdering av pasienter som søker om behandling er en nøkkelkontroll.

Ved Klinikk for nevropsykologi vurderes henviste pasienter (i all hovedsak henvist fra lege/psykolog ved Sunnaas sykehus) av psykologspesialistene ved Sunnaas sykehus som er ansatt i II-stillinger ved PSI, og i dialog med pasientenes behandlere ved Sunnaas. Pasienter er alltid henvist fra lege/psykolog; aldri rekruttert via annonsering.

Rekruttering til de andre klinikkene utføres av klinikklederne og har skjedd på ulike måter, via henvisning og annonsering, for eksempel på Facebook. Fra Facebook lenkes det til PSIs hjemmeside om terapitilbud fire ganger årlig. I følge annonseringen tilbys veiledning av spesialist i klinisk psykologi. Det er opplyst at søknadsdialog i noen tilfeller kan ha foregått via e-post når potensiell klient har initiert kontakt.

Det er påpekt av klinikkleder at dialogen avgrenses til besvaring av spørsmål om behandlingstilbudet, tidspunkt etc. for avtaler, og inkluderer ikke utveksling av personsensitive helseopplysninger. EIR har ikke hatt mulighet kontrollere dette.

Vurdering:
Ukryptert e-post er ikke egnet som verktøy for utveksling av personsensitiv informasjon ifm rekruttering og søknadsdialog. Det kan utgjøre risiko for at sensitive personopplysninger kommer på avveie. Det bør også vurderes om annonseringen i større grad skal gjenspeile begrensningene som er innført ifm rekrutteringen, slik at det tydelig fremkommer at tilbudet ikke gjelder «tyngre tilfeller».

Anbefaling:

- PSIs hjemmeside og Facebookside bør uttrykkelig opplyse om at personsensitive opplysninger ikke må sendes via e-post.
- Det bør vurderes å etablere en sikker elektronisk kanal for pasientdialog – for eksempel om sikkert nettskjema kan utvikles og brukes.
- Annonsering bør bedre gjenspeile tilbudet og målgruppe.

2.7 Tilgangskontroll pasientjournaler

Pasientjournaler og studentens arbeidsmateriale oppbevares i låste skap i 3 låste rom på PSI, hvorav 2 ble besøkt av EIR.

Rom V1U-02 - Studentenes arbeidsrom med PCer og arkivskap:
I arkivskapene finnes journaler/arbeidspapirer og minnepinner med bl.a. videomateriale av pasienten.

- Det kreves autorisert tilgang til rommet. Administrasjonen sender lister over nye studenter pr. semester til vaktsentralen, som åpner tilgang for årets kull (i underkant av 100 studenter på semester 11 og 12). Pr. i dag har man ingen rutiner på å avslutte tilganger. EIR fant under revisjonen at det står oppført 756 studenter og 436 ansatte, totalt 1192 personer med tilgang. I tillegg finnes et tosifret antall utlånskort og tilgang for vakt og renhold, herunder upersonlige utlånskort. Det er brukt en enkel kortleser på døren. Døren låses ikke automatisk når den lukkes. Det har vært hendelser hvor døren har blitt stående ulåst.
- I rommet finnes et nøkkelskap som åpnes med firesifret kode. Dette inneholder nøkkel til et annet skap som inneholder samtlige nøkler til ulike arkivskap (benyttet av hver klinikk eller hver veiledningsgruppe) som brukes til oppbevaring av pasientjournaler. Studenter får utlevert kode til nøkkelskapet ved semesterstart og har dermed tilgang til alle nøkler til arkivskap med journaler. Det har ikke vært rutiner for å skifte kode jevnlig.

Som følge av observasjonene ble strakstiltak iverksatt 18.10. Kode til nøkkelskap ble endret, kortleser i dør skiftet ut og ny nøkkellås er satt inn midlertidig.

Rom S02-33 – Kontor sekretær med arkivskap
Her oppbevares noen av journalene til enkelte av klinikkene i låst arkivskap fra pasienter som har avsluttet behandlingen.

- Rommet har vanlig nøkkellås. Det finnes 71 nøkler.
- Arkivskapet er låst. Vi har ikke undersøkt dette nærmere.

Iht pasientjournalloven §18 skal pasienten kunne få innsyn i journal og hvem som har hatt tilgang til vedkommendes helseopplysninger. Det føres pr. i dag ikke logg over hvem som har sett og brukt journalene og når det har funnet sted.

Vurdering:
EIR har fått opplyst at det er i underkant av 100 studenter / 30 studentgrupper i 11. og 12. semester. Antall faktiske tilganger til arkivrom er iht vaktsentralen nærmere 1200. Det har vært risiko for uautorisert tilgang til sensitive personopplysninger og at disse kommer på avveie og/eller kan bli misbrukt. Det har ikke vært god adgangskontroll til pasientjournalene inkludert arbeidsmateriale og minnepinner. Studenter og ansatte bør kun ha tilgang til «egne» pasientjournaler og det må føres logg over hvem som har hatt innsyn og når. Det er i dag krav til at pasientjournal skal være elektronisk.

Anbefaling:

- Elektronisk journal med tilfredsstillende internkontroll, særlig tilgangskontroll og logger.
- Innføre rutine slik at man 1-2 ganger i året gjennomgår autorisasjoner, tilganger og logger.
- Innføre rutine som sperrer nøkkelkort for studenter og ansatte som ikke skal ha tilgang, herunder når de slutter på PSI.

2.8 Politiattester

PSI samler inn politiattest for studenter som skal behandle pasienter og registrerer at attest er mottatt i FS-systemet. Selve attesten makuleres deretter. Fullstendighet i innlevering skal sikres gjennom at navnene på studentene som leverer inn attest, blir markert på en utskrift med årets studenter. Da internrevisjonen sjekket listene 17.10, var det mange som ikke hadde levert attest. Kravene til politiattest i helsepersonelloven, er så langt EIR har forstått, først og fremst nødvendig for behandling av barn og unge. For helsepersonell underlagt spesialisthelsetjenesteloven er det krav om politiattest generelt.

Vurdering:

EIR støtter PSIs vurdering om behov for politiattest, men det er viktig å sikre at studentene har innlevert politiattest før behandling igangsettes.

Anbefaling:

- Følge opp at alle studenter leverer politiattest før behandling av pasienter.

2.9 Taushetserklæring

Studentene signerer taushetserklæring i 2 omganger. EIR ble forelagt disse listene med signaturer.

Den ene listen: studenten erklærer å ha lest og være innforstått med de faglige etiske retningslinjene som inkluderer informasjon om taushetsplikt. Listen ligger i resepsjonen og er pr. 17.oktober langt fra komplett.
Klinikkleders kommentar til ufullstendige lister: «Alle studenter skal ha undertegnet taushetserklæring. Så vidt vi forstod på kommunikasjonen med administrasjonen (da dere var der) er taushetserklæringene lagret et annet sted. Så vidt vi vet, er det ikke anledning til å gå opp til eksamen hvis ikke denne er levert.» EIR har ikke hatt anledning til å kontrollere påstanden, men oppfatter kommunikasjonen annerledes.

Den andre listen: Ukentlig gjennomføres «staffmøter», der selekterte utdrag fra sladdede videoer benyttes for faglig drøfting, under ledelse av veileder og staffleder. Alle studenter på de kliniske semestrene har adgang til staffene og må signere taushetserklæring før undervisningen starter.

Vurdering:

EIR synes det er uheldig dersom det forekommer at behandling av pasienter har skjedd uten at det er underskrevet taushetserklæring. I tillegg kommer taushetsplikten ikke veldig tydelig frem i informasjonsarket med etiske retningslinjer. Det bør vurderes å fremheve dette mer.

Anbefaling:

- Kontrollere at alle taushetserklæringer er innhentet fra alle før pasientbehandling.

2.10 Samtykkeerklæringer

Samtykkeerklæringer ligger arkivert sammen med papirjournaler. Internrevisjonen testet sammen med klinikklederne et par samtykkeerklæringer, (navn på pasient ble skjult for EIR).

EIR hadde ikke kapasitet / mulighet til å teste om alle samtykkeerklæringer forelå, men har anbefalt at PSI kontrollerer dette i forbindelse med tiltaket om å kontrollere diagnoser i pasientporteføljen for å sikre at rettighetspasienter er henvist videre og at porteføljen kun består av pasienter i tråd med lavterskel tilbudet.

Internrevisjonen har fått kopi av malene for skjemaene for samtykke (2 forskjellige for de 3 klinikkene). Disse inneholder ordene «beskytte klientens identitet» og «problemstillinger fra timene presenteres anonymisert». Pasientene skal underskrive på samtykkeerklæring som beskriver at helsedata kan brukes i «undervisningsklinikken» eller at de brukes «i forbindelse med veiledning i gruppe»

Vurdering:
Selv om videoopptak sladdes (hele kroppen), så vil stemmen være gjenkjennbar. Etter vår vurdering er tiltaket ikke tilstrekkelig. Pasienten er ikke anonym og PSI har ikke gjort nok for å beskytte pasientens identitet. EIR mener samtykkeerklæringen ikke beskriver den faktiske rutinen godt nok da pasienten trolig oppfatter «gruppe» som noe annet enn hele kullet. Det kan også være noe tvil om pasienten er klar over hvor mange som faktisk kan sitte på et staffmøte.

Anbefaling:
- Gå gjennom samtykkeerklæringene med hensyn på om det må angis mer nøye hvilke personer/grupper som får tilgang til personopplysninger og i hvilken form. Det bør for eksempel opplyses om at sladding ikke er det samme som anonymisering.
- Gå gjennom videosladdingsrutinene og anonymisering av personer.

2.11 Spørsmål om konsesjonsplikt for bruk av helseopplysninger i undervisning
Kluge skriver i rapport av 17.10.17 at behandling av personsensitive helseopplysninger krever konsesjon. Klinikkene behandler sensitive helserelaterte personopplysninger ved å bruke manuelle og elektroniske registre og journaler. Registre og journaler til helseformål var inntil 1.1.2017 meldepliktige.

Det er så langt EIR forstår likevel uavklart om bruk av personsensitive helseopplysninger til undervisning kan gjøres i medhold av samtykke eller om det krever konsesjon etter personopplysningsloven §33[3]. UiO skal kontakte Datatilsynet for å avklare dette.

Klinikkleder påpeker: Journaler brukes ikke i undervisning. Journalen brukes som et verktøy i pasientbehandlingen. Veileder gir den enkelte student veiledning på hvordan den skal utformes i henhold til lovverket, og at den er pasientens eie (f.eks. unngå ordlyd som kan være støtende).

Vurdering:
Det er viktig å avklare om bruk av personsensitive data fra journaler og registre brukt i undervisning trenger konsesjon, eller om det er tilstrekkelig med uttrykkelig forutgående samtykke. EIR kan ikke ta stilling til juridisk skille mellom undervisning og pasientbehandling.

[3] Basert på informasjon EIR har fått etter diskusjoner mellom UiO og advokatfirma Kluge 20.10.-22.10.

Anbefaling:

- Avklare med Datatilsynet om det er krav til konsesjon for bruk av personsensitive data fra helseregistre og journaler eller om det er tilstrekkelig med forutgående samtykke.

2.12 Melde- og konsesjonsplikt ved videopptak

Behandling av sensitive helseopplysninger omfatter også opptak fra terapitimer som lagres på minnepinne eller direkte i TSD, til gjenbruk i undervisningssituasjon. Det er antatt at dette krever konsesjon fra Datatilsynet, jf rettslig vurdering fra Kluge nevnt over, og vurderinger gjort av USIT. Konsesjon foreligger ikke, og minnepinner ble derfor inndratt. Vi viser i denne sammenhengen også til avsnitt 2.10, der vi vurderte at samtykkeerklæringen omfattet anonymitet, som etter vår vurdering ikke var godt nok ivaretatt. Bruk av personsensitive helseopplysninger til undervisning er så langt EIR forstår likevel ikke fullt ut avklart med hensyn til konsesjonsplikt etter personopplysningsloven §33, jfr over. UiO skal kontakte Datatilsynet for å avklare dette.

Vurdering:

Det er viktig å avklare om bruk av personsensitive data i forbindelse med videoopptak brukt i undervisning trenger konsesjon, eller om det er tilstrekkelig med uttrykkelig forutgående samtykke.

Anbefaling:

- Avklare om videoopptak krever konsesjon
- Videreføre implementeringsarbeidet med direkte overføring til TSD i forbindelse med konsesjonssøknad.

2.13 Minnepinner

Minnepinner brukes til å lagre videoopptak og annen informasjon fra terapitimer for gjenbruk med veileder og i undervisning. Minnepinnene utleveres med godkjent krypteringsløsning, merkes med et unikt nummer og har unikt passord for bruk. Prosedyre for bruk og oppbevaring av minnepinnene er utarbeidet.

Det foreligger avvik i minnepinnerutinen. 4 av 75 minnepinner hadde ikke kryptering. Da er innholdet ikke lenger sikret med passord. I tillegg var 8 av minnepinnene «døde», 3 var umerket og noen minnepinner hadde passordet liggende ved siden av. Det ble avdekket da minnepinnene ble sikret av USIT-personell 17.10.2017.

Vurdering

Det kan være ulike årsaker til at minnepinner ikke lenger er passordbeskyttet. Bruk av minnepinner uten passord øker risiko for autorisert tilgang og at personsensitive opplysninger kan komme på avveie. Risikoer ved bruk av minnepinner knytter seg også til at minnepinner er små, lette å ta med seg, lette å miste/glemme eller enkle å stjele. Det er også risikoer knyttet til overføring av datavirus.

Anbefaling:

- Følge opp observerte avvik for minnepinner som ikke har kryptering, undersøke årsaker. Vurdere konsekvens av eventuelt brudd på rutine og eventuelt sanksjoner og oppdatere retningslinjer med konsekvenser av brudd i sikkerhetsprosedyre.
- Følge opp at rutiner for bruk av krypterte minnepinner og passord etterleves. Minnepinner uten passord må innleveres med en gang for å etablere nødvendig beskyttelse.

2.14 Årsaker

EIR har ikke mulighet til å gjøre en omfattende analyse av årsaker til utfordringene. Etter vår vurdering har følgende forhold spilt inn:

- Utydelige roller og ansvar
- Ikke tilstrekkelig kunnskap om krav og behov for å gjøre risikovurderinger
- Ikke god nok kunnskap og kompetanse om internkontroll og sikkerhet
- Regelverksutvikling innen helse- og personvern har ikke i tilstrekkelig grad blitt fanget opp
- Det har vært for svak oppfølging av internkontroll i styringslinjene
- Ikke tilstrekkelig administrativ kapasitet

3 OM REVISJONSRAPPORTEN

Rapportutkast inneholder forslag til tiltak og endelig rapport omforente tiltak. Ansvarlig enhet må vurdere forslagene og velge en av følgende:

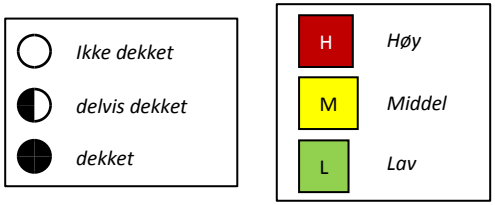
- Akseptere forslag til tiltak
- Foreslå et annet tiltak som tar ned risiko
- Akseptere risiko og ikke iverksette tiltak

Dersom enheten ikke iverksetter tiltak og dermed aksepterer risikoen, ber vi om at det begrunnes. Internrevisjonen må drøfte forholdet med toppledelsen og rapportere til styret dersom risikoen for organisasjonen er uakseptabel høy.

3.1 Om internrevisjonen

Internrevisjonens formål er *å fremme og beskytte UiOs verdier gjennom å gi risikobaserte og objektive bekreftelser, råd og innsikt*. Vårt arbeid er fastsatt i instruks fra universitetsstyret som vi rapporterer til faglig. Alle rapporter skal iht instruks stiles til universitetsdirektør. Mer informasjon om internrevisjonen finner du på våre nettsider.
http://www.uio.no/om/organisasjon/los/eir/index.html

4 VEDLEGG: ANBEFALINGER



Anbefalinger	Er dekket i det fortløpende forbedringsarbeidet[4]	Kompleksitet i gjennomføring[1]	Frist	Ansvar
(2.1) Fysisk sikkerhet				
1. Det bør innhentes ytterligere bistand fra HMSB for å gjøre sikkerhets- og beredskapsvurderinger				
2. Vurdere bistand fra eiendomsavdelingen for praktisk og sikker innretning av klinikk				
(2.2) Internkontroll system / kvalitetsrutiner				
3. Styrke administrativ kapasitet				
4. Styrke kompetanse om internkontroll og sikkerhet for ansatte og studenter				
5. Etablere og vedta kvalitets-/internkontrollsystem, herunder kvalitetshåndboken				
6. Det bør settes opp tidsplan og ansvarlige for tiltaksliste etter midlertidig stenging, herunder for den helhetlige oppfølgingen				
(2.3) Risikovurderinger				
7. Risikovurderinger bør gjøres 1-2 ganger i året eller oftere ved behov, for å vurdere og følge opp om risikoreduserende tiltak har tilstrekkelig effekt				

Anbefalinger	Er dekket i det fortløpende forbedringsarbeidet[4]	Kompleksitet i gjennomføring[1]	Frist	Ansvar
8. Fakultetet bør etterspørre kortfattede risikovurderinger fra underliggende enheter				
9. LOS bør etterspørre kortfattede risikovurderinger fra fakultet				
(2.4) Roller og ansvar				
10. Roller og ansvar må tydeliggjøres i hele styringslinjen				
11. Kvalitetshåndbok må forbedres med hensyn til roller og ansvar, jfr 2.2				
(2.5) Innføring av elektronisk journal				
12. Målbilder og kravspesifikasjoner i ny IT-løsning bør tydeliggjøres og forankres, herunder sikre at systemet dekker funksjonelle krav og krav gitt i lov og forskrift				
13. Gå opp grensen mellom - og tydeliggjøre hva som er funksjonelle krav/ikke funksjonelle krav mht internkontroll / sikkerhet, herunder vurdere rutiner for å styrke internkontrollen i andrelinjen (USIT), for å fange opp tilfeller der førstelinjen ikke har gjennomført nødvendige internkontrolltiltak.				
(2.6) Rekruttering av pasienter				
14. PSIs hjemmeside og Facebookside bør uttrykkelig opplyse om at personsensitive opplysninger ikke må sendes via e-post				

Anbefalinger	Er dekket i det fortløpende forbedringsarbeidet[4]	Kompleksitet i gjennomføring[1]	Frist	Ansvar
15. Det bør vurderes å etablere en sikker elektronisk kanal for pasientdialog – for eksempel om sikkert nettskjema kan utvikles og brukes				
16. Annonsering bør bedre gjenspeile tilbudet og målgruppe				
(2.7) Tilgangskontroll pasientjournaler				
17. Elektronisk journal med tilfredsstillende internkontroll, særlig tilgangskontroll og logger				
18. Innføre rutine slik at man 1-2 ganger i året gjennomgår autorisasjoner, tilganger og logger				
19. Innføre rutine som sperrer nøkkelkort for studenter og ansatte som ikke skal ha tilgang, herunder når de slutter ved PSI				
(2.8) Politiattester				
20. Følge opp at alle studenter leverer politiattest før behandling av pasienter				
(2.9) Taushetserklæring				
21. Kontrollere at alle taushetserklæringer er innhentet fra alle før pasientbehandling.				
(2.10) Samtykkeerklæringer				
22. Gå gjennom samtykkeerklæringene med hensyn på om det må angis mer nøye hvilke personer/grupper som får tilgang til				

Anbefalinger	Er dekket i det fortløpende forbedringsarbeidet[4]	Kompleksitet i gjennomføring[1]	Frist	Ansvar
personopplysninger og i hvilken form. Det bør for eksempel opplyses om at sladding ikke er det samme som anonymisert				
23. Gå gjennom videosladdingsrutinene og anonymisering av personer				
(2.11) Spørsmål og konsesjonsplikt for bruk av helseopplysninger i undervisning				
24. Avklare med Datatilsynet om det er krav til konsesjon for bruk av personsensitive data fra helseregistre og journaler eller om det er tilstrekkelig med forutgående samtykke.				
(2.12) Melde- og konsesjonsplikt ved videopptak				
25. Avklare om videoopptak krever konsesjon				
26. Videreføre implementeringsarbeidet med direkte overføring til TSD i forbindelse med konsesjonssøknad				
(2.13) Minnepinner				
27. Følge opp observerte avvik for minnepinner som ikke har kryptering, undersøke årsaker. Vurdere konsekvens av brudd eller eventuelt sanksjoner og oppdatere retningslinjer med konsekvenser av brudd i sikkerhetsprosedyre				
28. Følge opp at rutiner for bruk av krypterte minnepinner og passord etterleves. Minnepinner uten passord må innleveres men den gang for å etablere nødvendig beskyttelse.				

[1]*Basert på grov vurdering av endringen og innvirkning på organisasjon, prosesser og ressursbehov. Tiltakene må vurderes i lys av fremtidig organisering og plassering.*