

Personvern, risikoanalyse og tiltak

Vurdering av risiko for de klinikk-brukeres rettigheter og friheter, og planlagte tiltak for å håndtere risikoene. Kun risiko og konsekvens for klinikk-brukeres vurderes, og ikke risiko og konsekvens for UiO/virksomheten.

4.1 Risiko for klinikk-brukere

Vurdering av risikoens opprinnelse, art, særegenhet og alvorlighetsgrad. Vurderingen skal gjøres fra brukernes perspektiv for hver risiko:

- Manglende reell medbestemmelse
- Manglende reell åpenhet
- Manglende forutsigbarhet
- Risiko for brukerne hvis opplysninger kommer på avveie
- Bortfall eller svekkelse av andre rettigheter etter andre lover (for eksempel studierett, klagerett, ytringsfrihet, trygderett, religionsfrihet, rett til godt arbeidsmiljø).

Avklar potensielle konsekvenser, anslå alvorlighetsgrad, identifiser trusler og anslå sannsynlighet.

Hendelse	Konsekvenser	Alvorlighetsgrad	Trusler	Sannsynlighet
Manglende reell medbestemmelse – innsyn og endring av journal.	Brukere skal ha fullstendig og enkel mulighet til innsyn i sin journal, og andre lagrede opplysninger. Brukere har rettigheter til å kreve endring, tillegg og sletting av sine opplysninger. Konsekvensen hvis dette ikke	Høy	At brukeren ikke får korrekt informasjon ang. sine rettigheter, herunder at klinikkens web-sider ikke er tydelige nok, eller at klinikkens medarbeidere ikke er informert om forholdene	Lav. Informasjon om rettigheter blir gitt på nettsider i kvalitetshåndboka, og til alle klinikkmedarbeidere ved oppstart. Klinikens journalsystem legger også til rette for å kunne endre/slette tidligere oppføringer.

	<p>overholdes er at klinikken begår lovbrudd, at det er feilaktig informasjon i systemet, og at brukeren føler seg krenket.</p>		<p>eller er utydelige i sin kommunikasjon. I tillegg er det viktig å legge til rette for enkel tilgang og endring av journaler.</p>	
<p>Manglende reell åpenhet – innsyn i journal og journalsystemets tekniske drift.</p>	<p>Se punkt ang. medbestemmelse ovenfor. I tillegg kommer brukernes rettigheter til å vite hvordan journalsystemet opererer teknisk sett. Brudd på denne rettigheten kan medføre at klinikken begår lovbrudd.</p>	<p>Høy.</p>	<p>Manglende informasjon på klinikkens nettsider, og på brukernes samtykkeskjema.</p>	<p>Lav. Informasjon blir gitt på nettsidene (kvalitetshåndboka) og på brukernes samtykkeskjema.</p>
<p>Manglende forutsigbarhet</p>	<p>Brukerne skal ha gode og tydelige muligheter til å melde fra om sine behov, som inkluderer klager, spørsmål, avtaler, avmelding, og interessepåmelding. Konsekvens av</p>	<p>Høy</p>	<p>Manglende informasjon på klinikkens nettsider, og på brukernes samtykkeskjema.</p>	<p>Lav. Informasjon blir gitt på nettsidene og på brukernes samtykkeskjema. Nettsiden har tydelige knapper og lenker der man kan sende inn klager, trekke seg, stille spørsmål, og lignende.</p>

	manglende systemer for dette kan være at klinikken begår lovbrudd.			
Risiko for brukerne hvis opplysninger kommer på avveie	Kan medføre alvorlige konsekvenser for brukerne, siden opplysningene vi samler inn kan være av høyst personlig karakter. Slike hendelser kan være lovbrudd.	Høy	<p>a) Data-angrep (hacking) på journalsystemet.</p> <p>b) Sensitive opplysninger nedføres utenfor journalsystemet.</p> <p>c) Svikt i tilgangskontrollen på brukernes opplysninger.</p>	<p>a) Lav. Klinikken bruker TSD til lagring og behandling av journal og andre opplysninger. TSD er spesifikt laget for å kunne håndtere lagring av sensitive opplysninger.</p> <p>b) Medium. Følgende tiltak gjennomføres for å redusere risiko:</p> <p>1) Alle opplysninger skal om mulig nedføres i TSD uten mellomledd. Rutinen for nedføring på papir er at papirnotater kun skal eksistere i en kort periode før de blir skannet og makulert, eller midlertidig innlåst i skap/safe. 2) Lyd og video-opptak Lyd og video-opptak strømmes</p>

				<p>og lagres direkte inn til TSD. 3) Klinikkens studenter og veiledere blir skriftlig informert bl.a. gjennom TSD samtykkeskjema om alvorligheten av sensitive opplysninger på avveie og at dette er strengt forbudt ved klinikken.</p> <p>c) Lav. Klinikken bruker TSDs løsninger på tilgangsstyring, slik at hver enkelt person ved klinikken kun har tilgang til de elektroniske mappene tilknyttet spesifikke klinikkbrukere. Tilgang til mappe opprettes kun når klinikkstudent/veileder har fått tildelt en bruker av klinikkleder og/eller administrator.</p>
--	--	--	--	--

<p>Bortfall eller svekkelse av andre rettigheter etter andre lover (for eksempel studierett, klagerett, ytringsfrihet, trygderett, religionsfrihet, rett til godt arbeidsmiljø).</p>	<p>Medfører alvorlige konsekvenser.</p>	<p>Høy</p>	<p>Ingen</p>	<p>Lav</p>
<p>Opplysninger som feilaktig er endret eller slettet ikke kan gjenopprettes med minst en måneds historikk.</p>	<p>Kan medføre brudd på journalloven og/eller andre lover.</p>	<p>Høy</p>	<p>Feilaktig sletting/ending gjøres mellom to backup-sykluser.</p>	<p>Lav. Daglige backup av TSD lagres i 90 dager.</p>