

Akseptkriterier og risikonivå i Pasientreiser HF

Sannsynlighet: (angitt som antall pr år)

1 Usannsynlig	2 Mindre sannsynlig	3 Mulig 12/1	4 Sannsynlig	5 Svært sannsynlig
Sjeldnere enn en gang i året	1-2 ganger i året	En eller flere ganger i kvartalet	Ukentlig	Daglig eller oftere

Sannsynlighet for informasjonssikkerhet:

1 Svært lav	2 Lav	3 Moderat	4 Høy	5 Svært høy
Erfaringsgrunnlag Hendelsen har inntruffet sjeldnere enn hvert 5 år Tiltaksstatus Sikkerhetstiltak er fullt ut etablert i henhold til krav Omgåelse av etablerte tiltak krever nyeste teknologi og	Erfaringsgrunnlag Hendelsen har inntruffet 1 gang i løpet av 2 til 5 år Tiltaksstatus Sikkerhetstiltak er etablert og kun mindre mangler i henhold til krav - Omgåelse av etablerte tiltak krever betydelig verktøystøtte og betydelig kunnskap	Erfaringsgrunnlag Hendelsen har inntruffet 1 gang i løpet av 1 til 2 år Tiltaksstatus Sikkerhetstiltak er ikke implementert i henhold til krav og kompenserende tiltak er etablert Omgåelse av etablerte tiltak krever verktøystøtte	Erfaringsgrunnlag Hendelsen har inntruffet 1 - 5 ganger i året Tiltaksstatus Sikkerhetstiltak er ikke implementert i henhold til krav og kun få kompenserende tiltak er etablert Etablerte tiltak kan med begrenset	Erfaringsgrunnlag Hendelsen har inntruffet mer enn 5 ganger i året Tiltaksstatus Sikkerhetstiltak er ikke etablert Etablerte tiltak kan enkelt omgås av uautorisert personell Etablerte tiltak er lite robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell

inngående forkunnskap Trusselbilde Foreligger ingen identifiserte aktører med evne og vilje til å begå uønskede handlinger	Etablerte tiltak er meget robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell Trusselbilde Foreligger kun aktører med lav evne og lav vilje til å begå uønskede handlinger	og kunnskap av uautorisert personell Etablerte tiltak er nokså robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell Trusselbilde Foreligger aktører med moderat evne og moderat vilje til å begå uønskede handlinger	verktøystøtte og begrenset kunnskap omgås av uautorisert personell Etablerte tiltak er mindre robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell Trusselbilde Foreligger aktører med moderat evne og høy vilje til å begå uønskede handlinger	Trusselbilde Foreligger aktører med høy evne og høy vilje til å begå uønskede handlinger
---	--	--	---	---

Konsekvens:

Eksemplifisert konsekvens	1 Ubetydelig	2 Moderat	3 Alvorlig	4 Svært alvorlig	5 Kritisk
Uriktig eller mangelfull kommunikasjon med målgrupper	Alle målgrupper har tilgang til informasjon, men informasjonen er ikke lett tilgjengelig.	Pasientreiser kommuniserer ikke med enkelte målgrupper. F.eks. grupper med syns- hørsels- eller talehemming.	Pasientreiser kommuniserer ikke med flere målgrupper og mangler kanaler for kommunikasjon. Viktig informasjon er ikke kvalitetssikret eller oppdatert. Systemsvikt i en kommunikasjonskanal.	Ubevisst feilinformasjon. Informasjonen når få målgrupper.	Systemsvikt i alle kommunikasjonskanaler. Bevisst feilinformasjon og kommunikasjon.
Dårlig kvalitet eller ikke likebehandling i forvaltningen av pasientens rettigheter	Ulik praksis av regelverket som ikke gir konsekvenser for vedtak eller utbetaling	Feil vedtak for et lite antall personer som ikke fører til feilutbetaling. Pasienten forstår ikke deler av vedtaket	Feil vedtak til et stort antall personer. Feilutbetaling til enkelte pasienter. Pasienten forstår ikke vedtaket.	Feil vedtak og feilutbetaling til svært mange.	Alle får feil vedtak eller manglende vedtak. Ingen utbetaling eller feilutbetaling. Ingen får sine rettigheter iht pasient og brukerrettighetsloven § 2-6 med gjeldende forskrift.

Dårlig omdømme	Lav andel av befolkningen har liten tillit eller sprer dårlig omdømme om Pasientreiser HF. (enkelte negative medieoppslag.	Svekket tillit i befolkningen (feil vedtak, dårlig service på reiser uten rekvisisjon, telefon 915 05 515, flere negative medieoppslag).	Lav tillit i befolkningen/eiere/ myndigheter (feil i mange vedtak, svært dårlig service på reiser uten rekvisisjon, telefon 915 05 515, svært mange negative medieoppslag, særskilt oppfølging i styret).	Svært lav tillit i befolkningen/eiere/ myndigheter (bevisst/alvorlige feil i saksbehandlingen, feilinformasjon reiser uten rekvisisjon, telefon 915 05 515) Adm. dir. risikerer å gå av/alvorlig sak i styret/AD.	Ingen tillit i befolkningen/eiere/ myndigheter. Foretaket står i fare for å bli avviklet.
-----------------------	--	--	---	---	---

Behandling av person- og helseopplysninger	Mulighet for innsyn i helse- og personopplysninger uten tjenstlig behov. Ingen kjente brudd på personvernet. Mulig mindre økonomisk tap som kan gjenopprettes, mulig tap av anseelse eller integritet for den det gjelder (for eksempel opplysninger den registrerte oppfatter som følsomme)	Innsyn i enkelte helse- og personopplysninger (gått fra pc uten å stenge, utskrift på printer). Mulig brudd på personvernet for et lite antall personer. Mindre økonomisk tap som kan gjenopprettes, eller tap av anseelse eller personlig integritet for den det gjelder (for eksempel opplysninger den registrerte oppfatter som følsomme)	Innsyn i enkelte helse- og personopplysninger, mulighet for endring og brudd på lov (tilgang til opplysningene og mulighet for manipulasjon av data). Brudd på personvernet for et stort antall personer Betydelig økonomisk tap som kan gjenopprettes, eller tap av anseelse eller personlig integritet for den det gjelder (for eksempel opplysninger den registrerte kan oppfatte som krenkende, eller som andre kan gjøre nytte av)	Innsyn i flere helse- og personopplysninger, stor mulighet for endring og brudd på lov (som 3, men gjelder flere personer eller i et større omfang). Brudd på personvernet for svært mange personer Tap av helse, uopprettelig økonomisk tap, eller alvorlig tap av anseelse og integritet for den det gjelder	Innsyn i eller mulighet for endring av alle helse og personopplysninger og brudd på lov (systemsvikt, ikke tilgangskontroll, åpent på internett, tilgang til behandlingsrettet helseregister for ekstern virksomhet blir misbrukt og helse og personopplysninger kommer på avveie). Mulig tap av liv eller vedvarende helsetap, betydelig og uopprettelig økonomisk tap, eller alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi for den det gjelder
---	--	--	---	--	--

Konfidensialitet	Interninformasjon er tilgjengelig for uautorisert innsyn i inntil 30 minutter	Data og informasjon som ikke kan knyttes til enkeltindivid er tilgjengelig for uautorisert innsyn i mer 30 minutter	Inntil 200 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer 30 minutter	Manglende systemmulighet til å etterkomme personvernrettighet er som sperring og sletting	Særlige kategorier av personopplysninger blir eksponert ut mot Internett eller andre eksterne slik at de ikke kan sikres fjerning/sletting.
		Mindre andel virksomhetssensitiv interninformasjon er tilgjengelig for uautorisert innsyn i mer enn 30 minutter	Særlige kategorier av personopplysninger inntil 0,5% av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter	Særlige kategorier av personopplysninger blir eksponert slik at pasienter motsetter seg fremover å dele slike opplysninger i behandlingsøyemed	Særlige kategorier av personopplysninger blir eksponert slik at pasienter motsetter seg fremover å dele slike opplysninger i kritisk behandlingsøyemed
			Stor andel virksomhetssensitiv informasjon er tilgjengelig for uautorisert innsyn i mer 30 minutter	Mellom 200-500 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer 30 minutter	Mer enn 500 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer enn 30 minutter
				Særlige kategorier av personopplysninger til mellom 0,5 - 1 % av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter	Særlige kategorier av personopplysninger til mer enn 1 % av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter–
					Stor andel virksomhetskritisk informasjon er tilgjengelig for uautorisert innsyn

				Mindre andel virksomhetskritisk informasjon er tilgjengelig for uautorisert innsyn i mer 30 minutter	
--	--	--	--	--	--

Integritet	Uautoriserte endringer i særlige kategorier av personopplysninger uten behandlingsmessige konsekvenser	Uautoriserte endringer i særlige kategorier av personopplysninger som leder til forsinkelser i pasientbehandling	Uautoriserte endringer i særlige kategorier av personopplysninger som leder til moderate pasientskader Uautoriserte endringer i personopplysninger som leder til moderate konsekvenser for de det gjelder	Uautoriserte endringer i særlige kategorier av personopplysninger som leder til alvorlige pasientskader Uautoriserte endringer i personopplysninger som leder til alvorlige konsekvenser for de det gjelder	Uautoriserte endringer i særlige kategorier av personopplysninger som leder til tap av liv og alvorlige pasientskader
-------------------	--	--	--	--	---

Tilgjengelighet	Autoriserte mangler tilgang til hele eller deler av andre typer tjenester, herunder kritikalitet 3 tjenester	Autoriserte mangler tilgang til hele eller deler av kritikalitet-2 tjenesten som berører pasientbehandling i inntil 24 timer	Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører kritisk pasientbehandling i inntil 12 timer	Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører kritisk pasientbehandling mellom 12 - 24 timer	Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører kritisk pasientbehandling i mer enn 24 timer
			Autoriserte mangler tilgang til hele eller deler av kritikalitet-2 tjenesten som berører pasientbehandling i mer enn 24 timer–		
			Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører virksomhetskritiske funksjoner, herunder konsekvenser for ansatte, i inntil 12 timer		
			Autoriserte mangler tilgang til hele eller deler av kritikalitet-2 tjenesten som berører virksomhetssensitive funksjoner,		
				Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører virksomhetskritiske funksjoner, herunder konsekvenser for ansatte, mellom 12 - 24 timer	Autoriserte mangler tilgang til hele eller deler av kritikalitet-1 tjenesten som berører virksomhetskritiske funksjoner, herunder konsekvenser for ansatte, i mer enn 24 timer

			herunder konsekvenser for ansatte, i mer enn 24 timer		
--	--	--	--	--	--

Brudd på etiske retningslinjer, fare for økonomisk kriminalitet og brudd på lov ifm anskaffelser	Ubetydelig tap av renommé, rykte og faglig integritet.	Moderat tap av renommé, rykte og faglig integritet virksomheten har ovenfor foretakets interessenter (feil i utlysning ifm anskaffelser, ubevisst holdning vis à vis info fra/til leverandør/PRK/eier).	Alvorlig tap av renommé, rykte eller faglig integritet (ukritisk/ubevisst tildelingsprosess ifm anskaffelser, ukritisk/ubevisst holdning til info man får tilgang til i kraft av sin stilling).	Svært alvorlig tap av renommé eller rykte (bevisst feil anskaffelsesprosess en, misbruk av info man får tilgang til).	Uopprettelig økonomisk tap (korrupte handlinger/bestikkelser, salg av info en får tilgang til).
Stabil drift med oppetid på 99,3 % for systemene NISSY, PRO. Oppetidskrav på 95% for CTRL og Radar	- Nedetid i PRO i mindre enn 150 minutter totalt for en måned nasjonalt med manuelle rutiner eller workaroud. - Nedetid i Nissy i mindre enn 150 minutter totalt for en måned nasjonalt med manuelle rutiner eller workaroud. - Nedetid i CTRL og Radar i mindre enn 150 minutter totalt for en måned men med mulighet	- Nedetid i PRO i mer enn 150 minutter og mindre enn 370 minutter nasjonalt men med workaroud og manuelle rutiner. - Nedetid i Nissy i mer enn 150 minutter og mindre enn 370 minutter nasjonalt men med workaroud og manuelle rutiner. - Nedetid i CTRL og Radar i mer enn 150 minutter og mindre enn 370 med mulighet til å hente ut data manuelt.	- Nedetid i PRO i mer enn 150 minutter og mindre enn 370 minutter nasjonalt uten workaroud og manuelle rutiner. - Nedetid i Nissy i mer enn 150 minutter og mindre enn 370 minutter nasjonalt uten workaroud og manuelle rutiner. - Nedetid i CTRL og Radar i mer enn 150 minutter og mindre enn 370 minutter uten mulighet til å hente ut data manuelt.	- Nedetid i PRO i mer enn 3 dager nasjonalt. - Nedetid i Nissy i mer enn 370 minutter nasjonalt. - Nedetid i CTRL og Radar i mer enn en uke.	- Nedetid i PRO i mer en uke nasjonalt og som fører til saksbehandlingstid over tre uker. - Nedetid i Nissy i mer en tre dager nasjonalt. - Nedetid i CTRL og Radar i mer en uke og tap av datagrunnlag.

	for å hente ut data manuelt.				
Endringer i systemer Pasientreiser HF har systemeierskap for til avtalt tid, kvalitet og kostnad.	- Endringer levert med riktig kvalitet og kostnad men mindre enn to uker forsinket.	- Endringer levert med riktig kvalitet men mer enn to uker forsinket.	- Endringer levert uten tilstrekkelig kvalitet der endringene ikke løser behovet.	- Endringer levert uten tilstrekkelig kvalitet og endringen fører til nedetid for bruker.	- Endringer levert uten tilstrekkelig kvalitet, for sent og fører til nedetid for bruker og løser ikke behovet i endringen. Endringer fører til store negative konsekvenser for pasient. (Eksempel at pasienten ikke får transport, ikke får utbetalinger, får feil informasjon).
Prosjekter til avtalt tid, kvalitet og kostnad.	- Prosjekt levert med riktig kvalitet og kostnad men forsinket, der forsinkelsen ikke er forankret i prosjektets styringsgruppe og i revidert fremdriftsplan.	- Prosjekt levert med riktig kvalitet og kostnad men vesentlig forsinket, der forsinkelsen ikke er forankret i prosjektets styringsgruppe og revidert fremdriftsplan.	- Prosjekt levert uten tilstrekkelig kvalitet og prosjektet løser ikke behovet.	- Prosjekt levert uten tilstrekkelig kvalitet og fører til nedetid for bruker.	- Prosjekt levert uten tilstrekkelig kvalitet, for sent og fører til nedetid for bruker og løser ikke behovet i prosjektet eller gir ikke gevinst. Prosjektet fører til store negative konsekvenser for pasient.

HMS - Ikke opplevelse av høy tilfredshet blant medarbeiderne, og utnyttelse av humankapital.	Sykefravær(definisjon: Sykefravær antall sykedager (kort og lang (-sykebarn)/mulige arbeidsdager i perioden) < 1% Turnover 1 – 5 % Medarbeidertilfredshet > 5	Sykefravær >1% < 5% Turnover < 10 % > 5 % Medarbeidertilfredshet < 5 > 4	Sykefravær > 5 % < 10% Turnover > 10 % < 15 % og < 1 % Medarbeidertilfredshet < 4 > 3,5	Sykefravær > 10 % < 25 % Turnover >15 % < 25 % Medarbeidertilfredshet < 3,5 > 2	Sykefravær > 25% Turnover > 25 % Medarbeidertilfredshet < 2
Utbetalingsfil genereres ikke	Utbetalingsfil genereres ikke innen 7 timer (forsinket utbetaling 1 dag)	Utbetalingsfil genereres ikke innen 1dag (forsinket utbetaling 2 dager)	Utbetalingsfil genereres ikke innen 3 dager (forsinket utbetaling 4 dager)	Utbetalingsfil genereres ikke på 5 dager (forsinket utbetaling 6 dager)	Utbetalingsfil blir ikke generert i mer enn en uke
Svingninger i arbeidsmengde	Manglende ressurser fører til at SLA kravene overskrides med 1 time	Manglende ressurser fører til at SLA kravene overskrides med 24 timer	Manglende ressurser fører til at SLA kravene overskrides med 2 dager	Store problemer med å finne kvalifiserte vikarer fører til at SLA kravene overskrides med 5 dager	Ingen tilgang på kvalifiserte vikarer fører til at SLA kravene overskrides kontinuerlig i mer enn 1 uke

Forsinket utsendelse av vedtaksbrev	Forsinkelse i generering av utskriftsfil på mer enn 8 timer fører til 1 dags forsinkelse av utsendelsen	Utsendelse forsinkes i mer enn 2 dager	Utsendelse forsinkes i mer enn 4 dager	Utsendelse forsinkes i mer enn 6 dager	Utsendelse forsinkes i mer enn en uke nasjonalt og dersom saksbehandlingstid er over tre uker
Økonomisk kriminalitet/ Korrupsjon/ underslag for verdi	Økonomisk tap/underslag under kr 1 000 for foretaket.	Økonomisk tap/underslag over kr 1 000 for foretaket.	Økonomisk tap/underslag over kr 300 000 for foretaket.	Økonomisk tap/underslag over kr 500 000 for foretaket.	Økonomisk tap/underslag under kr 1 000 000 for foretaket.

Risikonivå

Modell for risikovurdering og nivå for akseptabelt risikonivå

I Pasientreiser HF benytter en modell med en skala fra 1-5 for konsekvens og sannsynlighet som multipliseres for å finne risikonivå. Figur 1 viser modellen for risikovurdering. Områder som defineres i grønn sone (verdi 1-4) har ingen vesentlige mangler (akseptabelt risikonivå). Områder i gul sone (verdi 5-12) betyr at mye er på plass, men det fortsatt er noen mangler og tiltak bør igangsettes (moderat risikonivå). Områder i rød sone (verdi 13-25) har vesentlige mangler og det bør igangsettes strakstiltak (kritisk risikonivå).

Figur 1: Tabell for risiko (konsekvens x sannsynlighet)

		Sannsynlighet				
		1	2	3	4	5
Konsekvens	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	10	8	10
	1	1	2	3	4	5

