

		Utgitt med støtte av:  HelseDirektoratet
Norm for informasjonssikkerhet www.normen.no		
Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet		Støttedokument Faktaark nr 5 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/sikkerhetskordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Virksomhetens leder har ansvar for å fastsette akseptkriterier (nivå for akseptabel risiko) for virksomhetens informasjonssystemer.		
Gjennomføring	Nivå for akseptabel risiko skal fastsettes før behandling av helse- og personopplysninger startes og før risikovurderinger gjennomføres.		
Formål	<ul style="list-style-type: none"> Dokumentere målbare størrelser på sikkerhetsmålene som er fastsatt Kunne kontrollere om sikkerhetsmålene nås ved at resultat fra risikovurdering sammenlignes med nivå for akseptabel risiko 		
Omfang	Alle virksomheter i helsesektoren skal fastsette nivå for akseptabel risiko.		
Hjemmel	Personopplysningsforskriften § 2-4.		
Referanser	<ul style="list-style-type: none"> Norm for informasjonssikkerhet, kap 4.4 Nivå for akseptabel risiko Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner 		

Handling/Utførelse

Nr.	Aktivitet/Beskrivelse
1	Utarbeide akseptkriterier for akseptabel risiko a) Bakgrunnen for å utarbeide nivå for akseptabel risiko er etablerte mål og strategier for informasjonssikkerhet b) Utarbeide nivå for akseptabel risiko som størrelser på sikkerhetsmålene. Det skal utarbeides akseptkriterier for konfidensialitet, integritet, tilgjengelighet og kvalitet. (Se eksempel under)
2	Gjennomføring a) Det skal henvises til nivå for akseptabel risiko ved gjennomføring av risikovurderinger slik at det er tydelig hvorfor risikoen vurderes som den gjør (brudd på nivåene eller ikke) b) All risiko som identifiseres ifm risikovurderinger skal vurderes ift nivå for akseptabel risiko c) Hvis risiko overstiger fastsatt nivå for akseptabel risiko skal ledelsen vurdere om det skal iverksettes tiltak for å bringe sikkerheten innenfor akseptabelt nivå d) Det må vurderes om summen av flere risikoer (innen samme problemområde) som har lav sannsynlighet, men stor konsekvens til sammen overstiger nivå for akseptabel risiko
3	Kontroll og oppfølging a) Det fastsatte nivå for akseptabel risiko skal evalueres ifm gjennomføring av risikovurderinger og ledelsenes gjennomgang hvor bl.a. mål for informasjonssikkerhet vurderes

Eksempel

Ved utarbeidelse av nivå for akseptabel risiko anbefales det å ta utgangspunkt i en skala for konsekvens og sannsynlighet. Gjennom en vurdering av hvilke type konsekvenser virksomheten ikke kan akseptere (se eksempel i tabellen under) fastsettes betydningen av skalaen for verdiene 1 til 4 (Ubetydelig til Kritisk). Samme vurdering gjøres for sannsynlighetsskalaen slik at betydningen av verdiene 1 til 4 (Usannsynlig til Sannsynlig) fastsettes.

Ved å kombinere (multiplisere) maksimal akseptabel konsekvensen (for eksempel 3) med maksimal akseptabel sannsynlighet (for eksempel 2) gir dette nivå for akseptabel risiko (i dette eksempelet 6). For all risiko som er høyere enn nivå for akseptabel risiko skal det iverksettes tiltak for å bringe sikkerheten innenfor et akseptabelt nivå.

Arbeidet med å fastsette akseptabel risiko skal gjøres med utgangspunkt i de enkelte behandlingene av helse- og personopplysninger virksomheten gjør.

Eksempel på skala for sannsynlighet (1-4) og konsekvens (1-4) er illustrert i tabellen under. Den enkelte virksomhet må ta utgangspunkt i sin situasjon og gjøre egne vurderinger.

Sannsynlighet: (Angitt som antall pr år)	1 Usannsynlig <=1/5 (En gang hvert 5. år eller sjeldnere)	2 Mindre sannsynlig 1/1 (En gang hvert år)	3 Mulig 12/1 (En gang hver måned)	4 Sannsynlig >= 365/1 (Daglig eller oftere)
Konsekvens: (Eksempler angitt for Tilgjengelighet, Konfidensialitet, Integritet og Kvalitet)	1 Ubetydelig - Stans i <system> <= 10 minutter - Ingen uautorisert innsyn i helse- og personopplysninger - Journal er komplett - Ikke fare for pasienters helse - Intet brudd på personvernet - Ubetydelig økonomisk tap - Intet tap av renommé eller rykte	2 Moderat - Stans i <system> i 30 minutter - Uautorisert innsyn i enkelte helse- og personopplysninger og lovbrudd - Noen mangler i journal slik at helse- og personopplysninger ikke er fullstendige og ajourført i forhold til behandlingen av opplysningene - Ikke fare for pasienters helse - Brudd på personvernet for et lite antall pasienter - Gjenopprettelig økonomisk tap - Moderat tap av renommé eller rykte ovenfor virksomhetens omgivelser - Moderat tap av renommé eller rykte virksomheten har ovenfor pasienten	3 Alvorlig - Stans i <system> 4 timer - Uautorisert innsyn i enkelte helse- og personopplysninger, mulighet for endring og brudd på lov - Viktig informasjon mangler i journal og brudd på lov - Det gis tilgang til en bruker i en ekstern virksomhet som ikke har tjenstlig behov for EPJ for en eller flere pasienter - Fare for pasienters helse og liv - Brudd på personvernet for et stort antall pasienter - Alvorlig økonomisk tap - Alvorlig tap av renommé eller rykte	4 Kritisk - Stans i <system> 8 timer eller mere - Fullt uautorisert innsyn i eller mulighet for endring av alle helse- og personopplysninger og brudd på lov - Kritisk informasjon mangler i journal og brudd på lov - Diagnoser blir kodet feil iht. kodeverket der det benyttes kodeverk - Medikament, dosering eller behandlingstiltak blir feilregistrert - Helse- og personopplysninger skal henføres til rett identifisert person - Tilgang til behandlingsrettet helseregister (inkl. EPJ) for ekstern virksomhet blir misbrukt og helse- og personopplysninger kommer på avveie - Tap av liv - Uopprettelig økonomisk tap

Tabell 1

Ved gjennomføring av risikovurderinger (se Faktaark 7 – Risikovurderinger) skal den samme skalaen benyttes og sannsynlighet og konsekvens for den vurderte hendelsen fastsettes. Ved å beregne risiko (sannsynlighet multiplisert med konsekvens) for hendelsen og sammenligne resultatet med nivå for akseptabel risiko, er det mulig å avgjøre om hendelsen er under, lik eller over nivå for akseptabel risiko.

I matrisen under er det illustrert et eksempel med en hendelse som gir en risiko på 8. Nivå for akseptabel risiko for denne typen hendelser er fastsatt til 6 og det er sannsynligvis nødvendig å gjennomføre tiltak for å bringe risikoen ned på et akseptabelt nivå.

Sannsynligh	4 Sannsynlig		8		
	3 Mulig		6	9	
	2 Mindre Sannsynlig			6	
	1 Usannsynlig				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

Tabell 2 - Vurdering av risiko

Følgende vil være en norm for vurdering av risiko. Uønskede hendelser som havner i område:

- Rødt skal det gjennomføres tiltak for
- Gult skal det vurderes om det skal gjennomføres tiltak for
- Grønt er ikke nødvendig å gjennomføre tiltak for

Eksempler på nivå for akseptabel risiko (ift Tabell 1 over):

Tilgjengelighet

- Det aksepteres ikke stans i tilgang til pasientrettede systemer med mer enn 4 timers varighet mer enn 1 gang pr år (S = 2 og K = 3 gir nivå for akseptabel risiko på 6)

Konfidensialitet

- Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger mer enn en gang per år (S = 2 og K = 3 gir nivå for akseptabel risiko på 6)

Integritet

- Registrerte helse- og person opplysninger skal ikke gå tapt oftere enn en gang per måned (S = 3 og K = 2 gir nivå for akseptabel risiko på 6)

Kvalitet

- Det aksepteres ikke at diagnoser kodes feil oftere enn en gang per måned med fare for tap av liv og helse (S = 3 og K = 3 gir uakseptabel risiko på 9)