Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Fastsette nivå for akseptabel risiko

Støttedokument
Faktaark nr 5
Versjon: 3.1
Dato: 19.09.2018

Formål	• Dokumentere målbare størrelser på sikkerhetsmålene som er fastsatt • Kunne kontrollere om sikkerhetsmålene nås ved at resultat fra risikovurdering sammenlignes med nivå for akseptabel risiko		
Ansvar	Dataansvarlig har ansvar for å fastsette 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.		
Omfang	Alle virksomheter i helsesektoren skal fastsette nivå for akseptabel risiko.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder	☐ Ansatt / medarbeider ☐ Forsker ☒ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☐ Leverandør
Hjemmel	• Personvernforordningen artikkel 32 • Pasientjournalloven § 22		
Referanser	• Norm for informasjonssikkerhet, kap. 3 • Faktaark 7 – Risikovurdering • www.difi.no med modell for risikovurdering		

Merknad 19.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Nr.	Aktivitet/Beskrivelse
1	**Utarbeide nivå for akseptabel risiko** a) Bakgrunnen for å utarbeide nivå for akseptabel risiko er virksomhetens sikkerhetsmål og de overordnede kravene for virksomhetens behandling av helse- og personopplysninger som er fastsatt i Normens kapittel 4.4 (se kapittel 4.4.1, 4.4.2, 4.4.3 og 4.4.4) b) Utarbeide nivå for akseptabel risiko for konfidensialitet, integritet og tilgjengelighet som skal gjelde for virksomheten (se eksempel nedenfor)
2	**Bruk av nivå for akseptabel risiko** a) Ved gjennomføring av risikovurderinger skal det henvises til nivå for akseptabel risiko 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 e) Det fastsatte nivå for akseptabel risiko skal evalueres ifm gjennomføring av risikovurderinger og ledelsenes gjennomgang hvor bl.a. sikkerhetsmålene 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 Tabell 1 nedenfor) 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 verdien 2) med maksimal akseptabel sannsynlighet (for eksempel verdien 2) gir dette nivå for akseptabel risiko (i dette eksempelet verdien 4). 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 Tabell 1 og Tabell 2 nedenfor. Den enkelte virksomhet må ta utgangspunkt i sin situasjon og gjøre egne vurderinger.

Eksempel på skala for sannsynlighet				
Sannsynlighet:	1 Usannsynlig	2 Mindre sannsynlig	3 Mulig	4 Sannsynlig
Angitt som antall ganger	En gang hvert 5. år eller sjeldnere	En gang hvert år	En gang hver måned	Daglig eller oftere
Angitt som letthets-betraktning. Alternativ måte å komme frem til sannsynlighet på ved å bedømme hvor enkelt det er å bryte sikkerhets-tiltakene	- Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten - Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/ fullstendig kjennskap til tiltakene - Eksternt personell kan ikke omgå/bryte tiltaket	- Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten - Tiltakene kan likevel omgås/brytes av egne medarbeidere med små til normale ressurser, som i tillegg har normal kjennskap til tiltakene - Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse	- Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter hensikten - Egne medarbeidere trenger kun små til normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene - Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke prosedyrer som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale ressurser	- Sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale resurser - Det er ikke nødvendig med kjennskap til tiltakene

Tabell 1

Eksempel på skala for konsekvens				
Konsekvens:	1 Ubetydelig/Ingen	2 Moderat	3 Alvorlig	4 Kritisk

Eksempler angitt for tilgjengelighet, konfidensialitet og integritet	-Stans i <system> forekommer ikke -Intet uautorisert innsyn i helse- og personopplysninger -Journal er komplett -Ikke fare for pasienters helse -Ikke brudd på personvernet -Ikke økonomisk tap -Ikke tap av renommé eller rykte	-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	-Stans i <system> 2 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 fra 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	-Stans i <system> mer enn 2 timer -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 -Medikament, dosering eller behandlingstiltak blir feilregistrert -Helse- og personopplysninger knyttes til feil person -Tilgang til behandlingsrettet helseregister (inkl. EPJ) og helse- og personopplysninger kommer på avveie -Tap av liv -Uopprettelig økonomisk tap -Omfattende tap av omdømme

Tabell 2

Ved gjennomføring av risikovurderinger (se Faktaark 7 – Risikovurderinger) benytter virksomheten den etablerte skalaen for sannsynlighet og konsekvens. 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 Figur 1 nedenfor er det illustrert et eksempel med en hendelse som gir en risiko på 8. Nivå for akseptabel risiko for denne typen hendelse er fastsatt til 4 og det er sannsynligvis nødvendig å gjennomføre tiltak for å bringe risikoen ned på et akseptabelt nivå.

Sannsynlighet					
	4 Sannsynlig				
	3 Mulig				
	2 Mindre Sannsynlig		Nivå for akseptabel risiko = 4		Hendelse med risiko = 8
	1 Usannsynlig				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

Figur 1 - Risikomatrise

Bruk av farger og hva som er høy, middels og lav risiko må den enkelte virksomhet selv fastsette.

Følgende vil være en norm for vurdering av risiko:

For risikonivå "Høy" skal det alltid planlegges og iverksettes risikoreduserende tiltak.

For risikonivå "Middels" anbefales det å planlegge og iverksette risikoreduserende tiltak.

Risikonivå "Lav" er restrisiko hvor det normalt ikke er nødvendig med risikoreduserende tiltak.

Eksempler på nivå for akseptabel risiko på grunnlag av Tabell 1 og 2 over:

Tilgjengelighet

- Det aksepteres ikke-planlagt stans i tilgang til pasientrettede systemer med mer enn 30 minutters varighet mer enn 1 gang pr år (S = 2 og K = 2 gir nivå for akseptabel risiko på 4)

Konfidensialitet
- Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger mer enn en gang per år (S = 2 og K = 2 gir nivå for akseptabel risiko på 4)

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)