

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h1>Risikovurdering</h1>	<b>Støttedokument</b> <b>Faktaark nr 7</b> Versjon: 2.1 Dato: 15.12.2010

<b>Målgruppe</b> 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 / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens ledelse er ansvarlig for å gjennomføre risikovurdering av behandlingen av helse- og personopplysninger.		
<b>Gjennomføring</b>	Risikovurdering skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandlinger som kan påvirke sikkerheten.		
<b>Formål</b>	Dokumentere at databehandlingsansvarlig har iverksatt tilstrekkelige tiltak og at behandlingene utføres innefor nivå for akseptabel risiko. Virksomhetene er pålagt å vurdere sannsynlighet for og konsekvens av sikkerhetsbrudd, og basere sikkerhetsarbeid på resultater fra slike vurderinger målt opp mot nivå for akseptabel risiko.		
<b>Omfang</b>	Alle virksomheter i helsesektoren skal gjennomføre risikovurdering. Risikovurdering skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger.		
<b>Hjemmel</b>	Personopplysningsforskriften § 2-4.		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Risikovurdering av informasjonssystem Datatilsynet, Oppdatert: 15.02.02, Opptrykk: 06.03.09</li> <li>• Norm for informasjonssikkerhet, kap 6. 2 Risikovurdering</li> </ul>		

Nr.	Aktivitet/Beskrivelse
<b>1</b>	<b>Planlegging</b> a) Ledelsen skal utarbeide og vedta en plan for risikovurderinger i virksomheten b) Det anbefales å gjennomføre flere små risikovurderinger fremfor en stor omfattende der dette er mulig. Det gir bedre oversikt og den enkelte risikovurdering kan avsluttes og aktuelle tiltak planlegges og gjennomføres
<b>2</b>	<b>Forberede risikovurdering</b> a) Innhente oversikt over behandlinger av helse- og personopplysninger b) Velg ut området som skal vurderes (behandlinger, IT-system, teknisk løsning, osv) c) Utarbeide og eventuelt oppdatere grunnlaget for risikovurdering slik at alle deltagere har samme forståelse for området som skal vurderes <ul style="list-style-type: none"> <li>- Prosessflyt for å synliggjøre hvordan helse- og personopplysninger behandles</li> <li>- Konfigurasjonskart for teknisk løsning</li> </ul> d) Utarbeide forslag til trusler og uønskede hendelser som arbeidsgruppen skal vurdere ift behandlinger, prosessflyt og konfigurasjonskart e) Etablere arbeidsgruppe som skal gjennomføre risikovurdering. Gruppen bemannes avhengig av hva som skal vurderes. Det er særlig viktig at daglige brukere av IT-systemer deltar når bruken av IT-systemer vurderes f) Tilpasse skala for sannsynlighet og konsekvens ift utarbeidede akseptkriterier (se vedlagte Skjema for risikovurdering)
<b>3</b>	<b>Gjennomføre risikovurdering</b> a) Invitere deltagere til å komme med egne uønskede hendelser som skal vurderes b) Gjennomgå og eventuelt tilpasse prosessflyt eller konfigurasjonskart i gruppen c) Tilpasse skala for sannsynlighet og konsekvens iht gruppens vurdering d) Dokumentere risikovurdering av den enkelte uønskede hendelse med sannsynlighet iht skala, konsekvenser og konsekvensenes størrelse iht benyttet skala, regn ut risiko (sannsynlighet multiplisert med konsekvens), eksisterende tiltak og forslag til nye tiltak (NB! Vurder én uønsket hendelse av gangen) (se vedlagte Skjema for risikovurdering).

Nr.	Aktivitet/Beskrivelse
	Det anbefales å benytte PC-prosjektor slik at alle deltagere ser hva som dokumenteres e) Indikere om hendelsen vil påvirke konfidensialitet, integritet, tilgjengelighet og kvalitet slik at sammenligning med fastlagt nivå for akseptabel risiko forenkles (se vedlagte Skjema for risikovurdering)
<b>4</b>	<b>Vurdering og anbefaling av nye tiltak</b> a) Vurdere risiko ift fastsatt nivå for akseptabel risiko (se Matrise - Vurdering av risiko under) b) Prioriter tiltak hvor risiko er større enn akseptabel risiko c) Utarbeide handlingsplan for hvilke tiltak som skal gjennomføres når og hvem som er ansvarlig. Det er viktig å skille på strakstiltak og mer langsiktige tiltak.

### Eksempel

Eksempelet på neste side viser forslag til skjema for risikovurdering og ikke prosessen beskrevet over.

Risiko i eksempelet på neste side er fastsatt til 8 (sannsynlighet X konsekvens). Matrisen under er hentet fra *Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet* og viser sammenhengen mellom nivå for akseptabel risiko og vurdert risiko. Er nivå for akseptabel risiko for konfidensialitet ved behandling av helse- og personopplysninger fastsatt til 4, er resultatet at nivå for akseptabel risiko er overskredet og det må for denne hendelsen (vist på neste side) gjennomføres tiltak for å bringe situasjonen under kontroll.

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

Tabell 1 - Vurdering av risiko

## Eksempel på oppbygging av skjema for risikovurdering

### Forklaring til koder i skjema for risikovurdering

#### Brudd på nivå for akseptabel risiko:

**K** = Konfidensialitet

**I** = Integritet

**T** = Tilgjengelighet

**Kv** = Kvalitet

#### Sannsynlighet:

(Angitt som antall pr år)

1

#### **Usannsynlig** $\leq 1/5$

(En gang hvert 5. år eller sjeldnere)

2

#### **Mindre sannsynlig** 3

1/1 (En gang hvert år)

3

#### **Mulig** $12/1$

(En gang hver måned)

4

#### **Sannsynlig** $\geq 365/1$

(Daglig eller oftere)

#### Sannsynlighet som letthetsbetraktning:

(Alternativ måte å komme frem til sannsynlighet på ved å bedømme hvor enkelt det er å bryte sikkerhetstiltakene)

1

- 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 tiltaken
- Eksternt personell kan ikke omgå/bryte tiltaket

2

- 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

3

- 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.

4

- Sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale ressurser
- Det er ikke nødvendig med kjennskap til tiltakene

**Konsekvens:**

(Angitt for Tilgjengelighet, Konfidensialitet, Integritet og Kvalitet)

1	Ubetydelig	2	Moderat	3	Alvorlig	4	Kritisk
	<ul style="list-style-type: none"><li>- Stans i &lt;system&gt; &lt;= 10 minutter</li><li>- Intet brudd på personvernet</li><li>- Journal er komplett</li><li>- Ikke fare for pasienters helse</li><li>- Ubetydelig økonomisk tap</li><li>- Intet tap av renommé eller rykte</li></ul>		<ul style="list-style-type: none"><li>- Stans i &lt;system&gt; i 30 minutter</li><li>- Brudd på personvernet for et lite antall pasienter</li><li>- Noen mangler i journal</li><li>- Ikke fare for pasienters helse</li><li>- Gjenopprettelig økonomisk tap</li><li>- Moderat tap av renommé eller rykte</li></ul>		<ul style="list-style-type: none"><li>- Stans i &lt;system&gt; 4 timer</li><li>- Brudd på personvernet for et stort antall pasienter</li><li>- Viktig informasjon mangler i journal og brudd på lov</li><li>- Diagnoser blir kodet feil iht. kodeverket der det benyttes kodeverk</li><li>- Medikament, dosering eller behandlingstiltak blir feilregistrert</li><li>- Helse- og personopplysninger blir ikke henført til rett person</li><li>- Fare for pasienters helse og liv ved feilbehandling eller mangelfull behandling</li><li>- Alvorlig økonomisk tap</li><li>- Alvorlig tap av renommé eller rykte</li></ul>		<ul style="list-style-type: none"><li>- Stans i &lt;system&gt; 8 timer eller mere</li><li>- Brudd på personvernet for et stort antall (alle) pasienter</li><li>- Kritisk informasjon mangler i journal og brudd på lov</li><li>- Diagnoser blir kodet feil iht. kodeverket der det benyttes kodeverk</li><li>- Medikament, dosering eller behandlingstiltak blir feilregistrert</li><li>- Helse- og personopplysninger blir ikke henført til rett person</li><li>- Tap av liv på grunn av feilbehandling eller mangelfull behandling</li><li>- Uopprettelig økonomisk tap</li></ul>

Tabell 2

$\text{Risiko} = S \times K_o$

Risiko > 4 krever vurdering av tiltak

Skjema for risikovurdering

Nr	Brudd på	Årsak / Trussel	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Eksisterende tiltak / Forslag til nye tiltak	Ansvarlig / Tidsfrist
1	K <sup>1</sup> , T	Bærbar PC oppbevares usikret i bil eller på reise.  Barbar PC inneholder helse- og personopplysninger.	Tyveri av bærbar PC inneholdende helse- og personopplysninger.	2	4	8	a) Fullt uautorisert innsyn i helse- og personopplysninger b) Stans i behandling av helse- og personopplysninger på bærbart utstyr	<b>Eksisterende tiltak</b> a) Ingen <b>Forslag til tiltak</b> a) Kryptering av lagringsmedium på barbart utstyr b) Sikkerhetskopi av data lagret på bærbart utstyr c) Eventuelt forbud mot å behandle helse- og personopplysninger på bærbart utstyr	

Tabell 3

<sup>1</sup> Brudd på nivå for akseptabel risiko: "Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger" fra Faktaark 29 - Nivå for akseptabel risiko.