Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Helsedirektoratet

Risikovurdering

Støttedokument
Faktaark nr 7
Versjon: 3.0
Dato: 12.2.2015

Formål	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.		
Ansvar	Databehandlingsansvarlig er ansvarlig for at det gjennomføres risikovurdering av behandlingen av helse- og personopplysninger.		
Gjennomføring	Risikovurdering skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandlinger som kan påvirke sikkerheten.		
Omfang	Alle virksomheter i helsesektoren skal gjennomføre risikovurdering. Risikovurdering skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder	☐ Ansatt / medarbeider ☐ Forsker ☒ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☐ Leverandør
Hjemmel	• Personopplysningsforskriften § 2-4. • Forskrift om tilgang til helseopplysninger mellom virksomheter § 5		
Referanser	• Risikovurdering av informasjonssystem Datatilsynet, Oppdatert: 15.02.02, Opptrykk: 06.03.09 • Norm for informasjonssikkerhet, kap 6. 2 Risikovurdering • Faktaark 5 – Nivå for akseptabel risiko • www.difi.no med modell for risikovurdering		

Nr.	Aktivitet/Beskrivelse
1	**Planlegging** a) Ledelsen skal utarbeide og vedta en plan for risikovurdering av behandlingen av helse- og personopplysninger 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
2	**Forberede risikovurdering** a) Innhente oversikt over behandlinger av helse- og personopplysninger b) Velg ut området som skal vurderes (behandlinger, tilgang til helseopplysninger mellom virksomheter, IT-system, teknisk løsning, osv) c) Utarbeide og eventuelt oppdater grunnlaget for risikovurdering slik at alle deltagere har samme forståelse for området som skal vurderes: - Informasjonsflyt for å synliggjøre hvordan helse- og personopplysninger behandles - Konfigurasjonskart for teknisk løsning 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 nivå for akseptabel risiko
3	**Gjennomføre risikovurdering** 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. Det anbefales å følge et enhetlig regime for skalaer i virksomheten. Bl.a. på den måten blir

Nr.	Aktivitet/Beskrivelse
	styringssystemet for informasjonssikkerhet en integrert del av virksomhetens øvrige internkontroll. 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! Vurdere én uønsket hendelse av gangen) (se skjema for risikovurdering nedenfor). Indikere om hendelsen vil påvirke konfidensialitet, integritet og tilgjengelighet slik at sammenligning med nivå for akseptabel risiko forenkles.
4	**Vurdering og anbefaling av nye tiltak** a) Vurdere risiko ift fastsatt nivå for akseptabel risiko 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 det første eksempelet på neste side er fastsatt til 8 (sannsynlighet multiplisert med konsekvens). Matrisen under er hentet fra *Faktaark 5 – Nivå for akseptabel risiko* og viser sammenhengen mellom nivå for akseptabel risiko og vurdert risiko. Nivå for akseptabel risiko for konfidensialitet ved behandling av helse- og personopplysninger fastsatt til 6. Den beregnede risikoen på 8 er dermed høyere enn nivå for akseptabel risiko og det må gjennomføres tiltak for å bringe risikoen ned på et akseptabelt nivå (forslag til tiltak er vist i tabellen på neste side).

Sannsynlighet					
	4 Sannsynlig				
	3 Mulig				
	2 Mindre Sannsynlig			6[1]	8[2]
	1 Usannsynlig				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

[1] Nivå for akseptabel risiko
[2] Brudd på nivå for akseptabel risiko: "Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger" fra Faktaark 5 - Nivå for akseptabel risiko.

Eksepler på skjema for risikovurdering

Eksempel 1

RISIKOVURDERING

Virksomhet: Tannlege Gliset	
Vurdert av: Peder Aas	**Dato: 12.2.2015**
Formålet med risikovurderingen:	Tilgjengelighet og konfidensialitet

Forhold som er vurdert (uønsket hendelse / scenario)		**Sannsynlighet**				**Konsekvens**				**Risikonivå** Sannsynlighet x konsekvens
		1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk	Lav risiko, f.eks. risiko < 5 Tiltak ikke nødvendig. / Middels risiko, f.eks. mellom 6 og 8 Tiltak må vurderes gjennomført / Høy risiko, f.eks. risiko > =9 Tiltak skal gjennomføres
1.	Server med journalsystemet inklusive sikkerhetskopi er stjålet fra tannlegekontoret	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☐ 2	☐ 3	☒ 4	☐Lav risiko ☒Middels risiko ☐Høy risiko
2.	Ny versjon av journalsystemet installeres uten at det er tatt sikkerhetskopi av alle data først	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☐ 3	☒ 4	☐Lav risiko ☐Middels risiko ☒Høy risiko
3.	E-post benyttes til å sende 11-siffret fødselsnummer og helseopplysninger	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lav risiko ☐Middels risiko ☒Høy risiko

Beskrivelse av tiltak *(Nr. 1 har høyest prioritet)*		**Betydning/ Kommentar**	**Referanse til linjenr ovenfor**
1.	Utarbeide prosedyre for bruk av e-post og lære opp alle ansatte i reglene: det er ikke tillatt å sende 11-siffret fødselsnummer og helseopplysninger i intern eller ekstern ordinær e-post	Dette er en risiko som forekommer veldig ofte og tiltaket vil ha god effekt	3
2.	Utarbeide prosedyre som sikrer at det tas sikkerhetskopi av alle data i journalsystemet for ny versjon av journalsystemet installeres.		2
3.	Plasseres server i avlåst rom.		1

Eksempel 2

Brudd på nivå for akseptabel risiko: **K** = Konfidensialitet **I** = Integritet **T** = Tilgjengelighet

Nr	Brudd på	Årsak / Trussel	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Eksisterende tiltak / Forslag til nye tiltak	Ansvarlig / Tidsfrist
1	K, T	Bærbar PC oppbevares usikret i bil eller på reise. Barbar PC inneholder helse- og personopplysninger.	Tyveri av bærbar PC som inneholder 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	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Kryptering av lagringsmedium på mobilt utstyr b) Sikkerhetskopi av data lagret på mobilt utstyr c) Eventuelt forbud mot å behandle helse- og personopplysninger på mobilt utstyr	
2	K	Manglende opplæring av bruker	Bruker sender SMS til pasient at legemiddel som angir en diagnose er ankommet apoteket	2	3	6	a) Brudd på taushetsplikten	**Eksisterende tiltak** a) Prosedyre for opplæring av nytilsatte **Forslag til tiltak** a) Innskjerpe gjennomføring av opplæring b) Endre prosedyre slik at den enkelte må kvittere for at opplæringen er gjennomført	
3	I	Innbrudd ved legekontoret Server er ikke sikret	Server med elektronisk pasientjournal er stjålet (inklusive sikkerhets-kopi som satt i maskinen)	1	4	4	a) Fullt uautorisert innsyn i helse- og personopplysninger b) Stans i pasientbehandlingen	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Sikre server i avlåst rom b) Etablere prosedyre for sikkerhetskopiering med krav til oppbevaring av sikkerhetskopi brannsikkert, adskilt fra server og innelåst	

Nr	Brudd på	Årsak / Trussel	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Eksisterende tiltak / Forslag til nye tiltak	Ansvarlig / Tidsfrist
4	I, T	Ingen test av innhold i sikkerhetskopi	Sikkerhetskopi er blank (inneholder ikke noe) når pasientjournalen skal tilbakekopieres	1	4	4	a) Stans i pasientbehandlingen b) Feil i pasientjournalene	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Etablere prosedyre med kontroll av innhold på sikkerhetskopi b) Etablere prosedyre med periodisk test av tilbakelegging av sikkerhetskopi	
5	K	Skriver er plassert i publikumsområde	Besøkende (pasient eller andre) tar med seg utskrift direkte fra skriver	2	3	6	a) Uautorisert innsyn i helse- og personopplysninger	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Plassere skriver i sikkert område b) Anskaffe teknisk løsning som krever at bruker må autentisere seg for å få utskrift	
6	T	Konfigurasjons-endringer gjennomføres uten konfigurasjonskontroll Uerfarne gjennomfører programoppdatering	Ny versjon av den elektroniske pasientjournalen installeres, men systemet virker ikke	1	4	4	a) Stans i pasientbehandlingen	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Etablere prosedyre for konfigurasjonsendringer med krav til bl.a. løsning for å gjenopprette eksisterende versjon av programvare	
7	K	Utrangert utstyr oppbevares ikke sikkert Uautorisert personell har tilgang til datautstyr som inneholder helse- og personopplysninger	Datautstyr med helse- og personopplysninger kastes på søppelfyllingen	1	4	4	a) Fullt uautorisert innsyn i helse- og personopplysninger	**Eksisterende tiltak** a) Ingen **Forslag til tiltak** a) Etablere prosedyre for utrangering av datautstyr b) Etablere fysisk sikring av datautstyr som skal utrangeres	