Introkurs Normen – Risikostyring

Oslo 12. februar 2020

André Meldal
Norsk Helsenett, Sekretariatet for Normen

Risikostyring

«Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko»

NORMEN

Hva skal vi beskytte?

Konfidensialitet

Med «konfidensialitet» menes i Normen at helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene. Konfidensialitet bidrar til ivaretakelse av taushetsplikt og personvern, noe som er viktig for innbyggernes tillit til helse- og omsorgstjenesten.

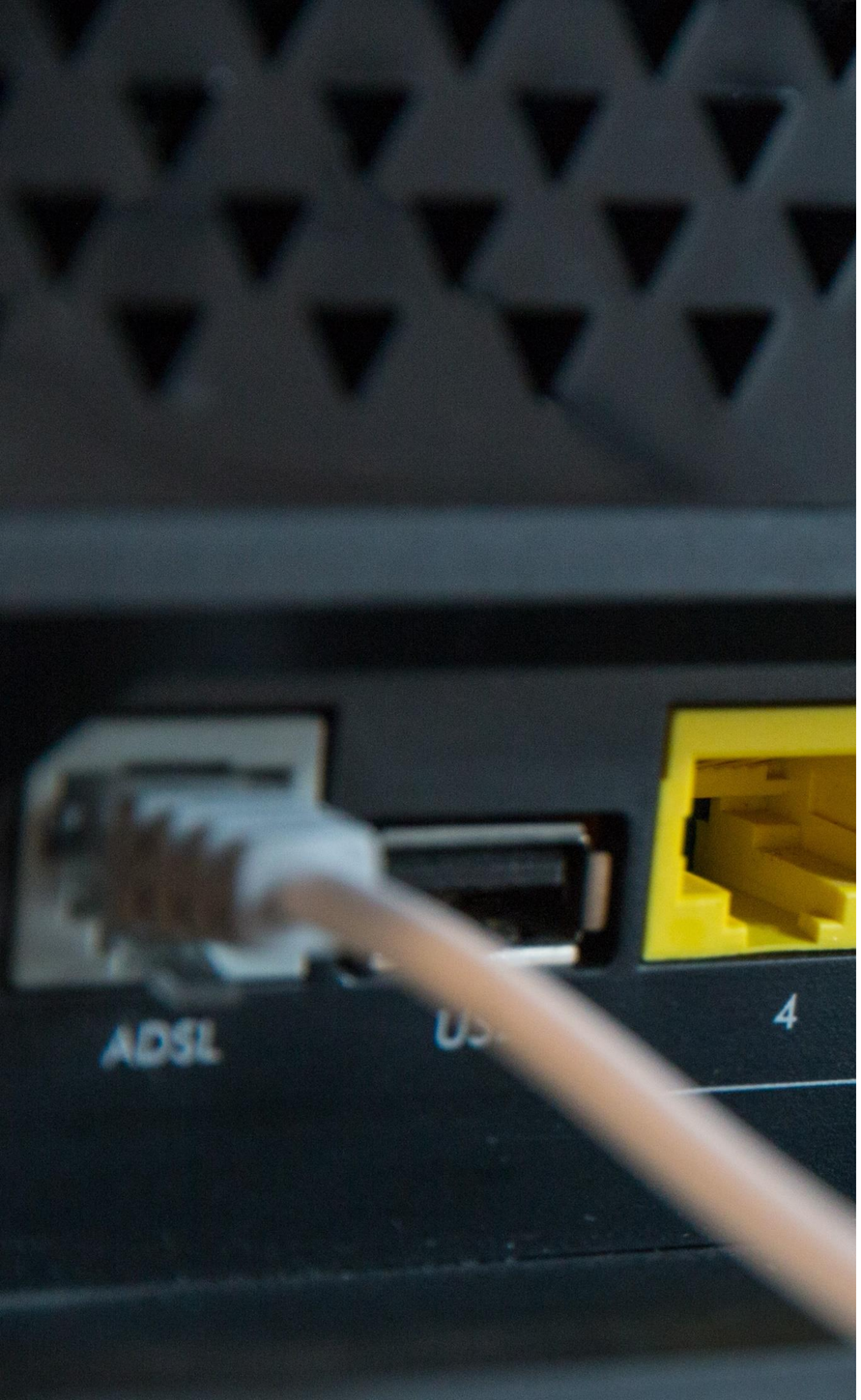
Integritet

Med «integritet» menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting. Integritet er en forutsetning for god og forsvarlig helsehjelp.

Tilgjengelighet og robusthet

Med «tilgjengelighet» menes i Normen at helse- og personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene. Tilgjengelig informasjon for helsepersonell er en forutsetning for god og forsvarlig helsehjelp.

Med «robusthet» menes i Normen organisasjonens og informasjonssystemenes evne til å gjenopprette normaltilstand etter for eksempel en fysisk eller teknisk hendelse



Normens minimumskrav

Krav for å sikre konfidensialitet

Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger.

- Hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- Avgrense tilgang for autorisert personell iht. tjenstlig behov
- Ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten

Krav for å sikre integritet

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting.

- Integritet er en forutsetning for god og forsvarlig helsehjelp
- Logge hvem som har rettet, registrert, endret og slettet
- Hindre utilsiktet eller uautorisert endring eller sletting
- Sikre at helse- og personopplysninger registreres på rett person
- Sikre at helse- og personopplysninger føres i henhold til relevant kodeverk og terminologi
- Sikre at helse- og personopplysninger er korrekte og om nødvendig oppdaterte
- Hindre at kopier av data blir en kilde til utdatert informasjon

Krav for å sikre tilgjengelighet og robusthet

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid.

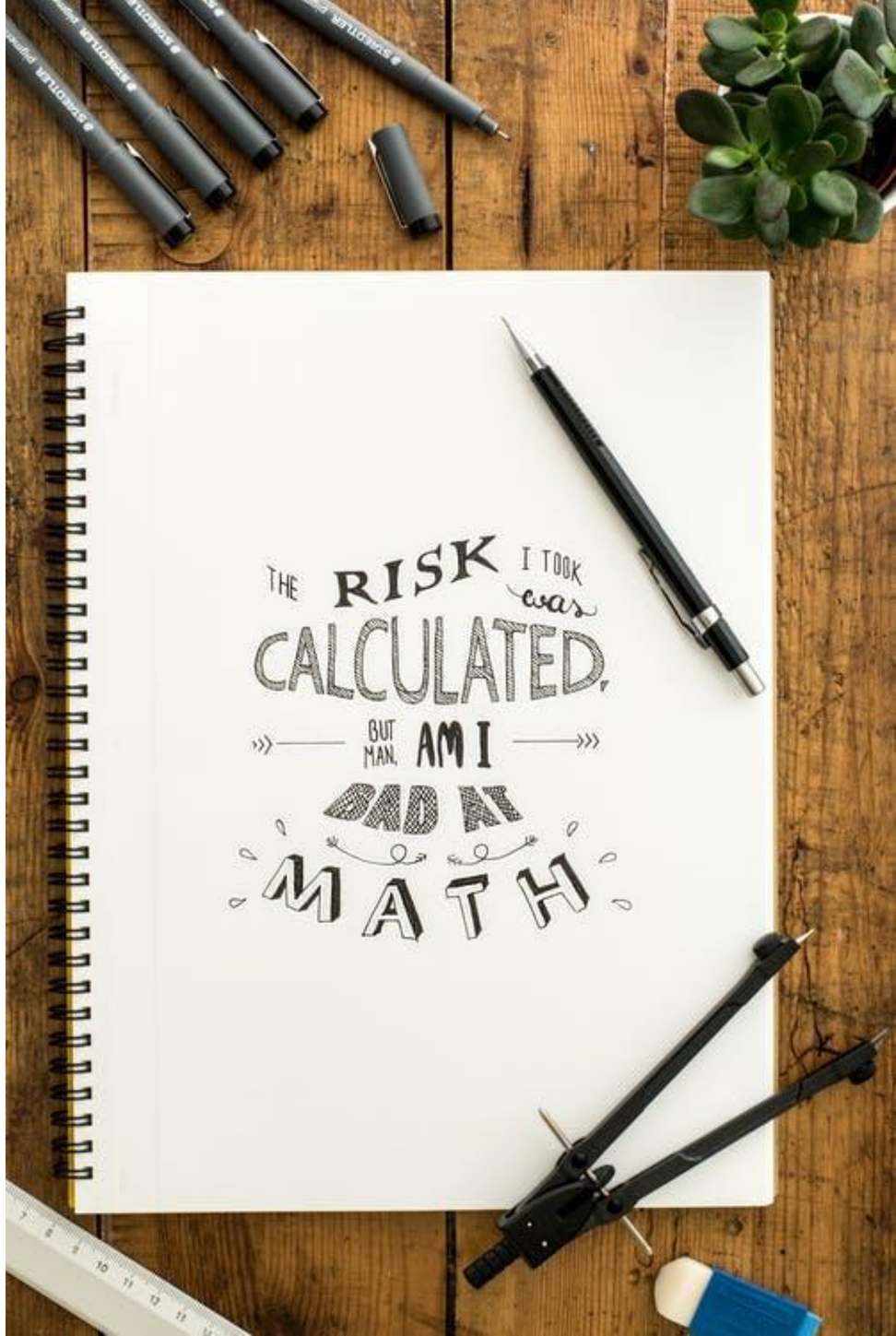
- Sikre at helse- og personopplysninger er tilgjengelig iht. tjenstlig behov
- Sikre forsvarlig og stabil drift av informasjonssystemene
- Sikre at det finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting
- Sikre at informasjonssystemene er tilgjengelig iht. virksomhetens tilgjengelighetskrav

Oversikt over teknologi og behandling av helse- og personopplysninger

NORMEN

Valg av tiltak

Risikovurdering



NORMEN

Om risikovurdering generelt

Verktøy for å stille seg kritiske spørsmål om risiko

Ledet gruppearbeid

Heller flere små enn en stor risikovurdering

Gjennomføres ved konkrete behov:

- Etablering av eller endring i behandling av helse- og personopplysninger
- Etablering av nye systemer eller registre som inneholder eller benytter helse- og personopplysninger
- Det etableres organisatoriske, tekniske eller andre endringer med betydning for informasjonssikkerheten •
- Det etableres eller endres tilgang til helseopplysninger mellom virksomheter

NORMEN

Akseptkriterier for risiko

- Dokumentere målbare størrelser på sikkerhetsmålene som er fastsatt. Det skal også kunne kontrolleres om sikkerhetsmålene nås ved at resultat for risikovurdering sammenlignes med nivå for akseptabel risiko

- Akseptkriterier er mål på akseptabel risiko for K, I og T:
  - Se eksempler i Faktaark 5

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: Tilgjengelighet, Konfidensialitet, Integritet og Kvalitet)	1 **Ubetydelig** -	2 **Moderat**	3 **Alvorlig**	4 **Kritisk**

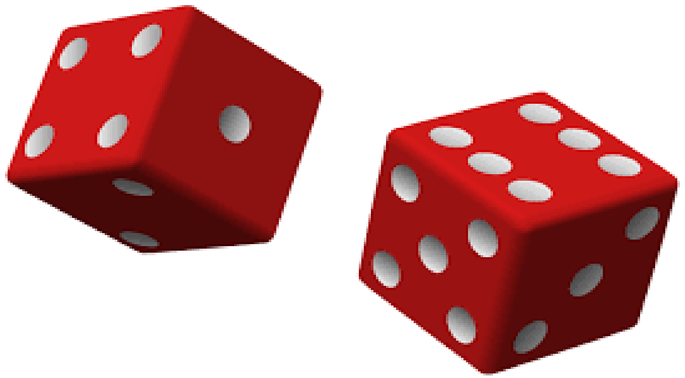
Metode for gjennomføring av risikovurdering

1. Velg ut et eller få konkrete områder
2. Start med å utarbeide konkrete forslag til trusler og uønskede hendelser i en tabell (senarioliste). F.eks. ut fra:
   - Dokumentasjon
   - Konfigurasjonskart
   - Intervjuer
   - Normen
   - Idedugnad i arbeidsgruppe
   - Annet
3. Etabler en arbeidsgruppe og involver folk

NORMEN

4. Drøft scenariolisten og prioriter i 1 eller 2
5. Overfør prioritert 1 til mal for risikovurdering og vurder hvert scenario for:
    - mulige konsekvenser
    - eksisterende og nye tiltak
    - tallfest sannsynlighet og konsekvens
    - beregn risikonivå

Trussel=sannsynlighet x konsekvens



NORMEN

Rapportering

- Utarbeid sammendrag
  - Prosa og tabell

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

  - Tabell med tiltak og ansvar
- Presenter bakgrunn (ta med underlag)
- Presenter metode, framdrift og deltagere
- Utarbeid tiltaksliste
- Skjematikk som vedlegg

NORMEN

Plenumsoppgaver

Er du kjent med om det finnes definerte akseptkriterier i din virksomhet?

Virksomheten skal etablere en ny tjeneste, og i tjenesten skal det behandles helseopplysninger. For å betrygge kundene har leverandøren gjort en risikovurdering av tjenesten.

Må virksomheten gjøre en egen risikovurdering?

Kan virksomheten basere seg på leverandørens vurdering?

I en pågående risikovurdering har dere vurdert en trussel som følger.

Sannsynlighet 2
Konsekvens 4

Ut i fra i faktaark 5, er man innenfor eller utenfor akseptert risikonivå?

En hendelse har ført til full stopp i journalsystemet, og det viser seg at det ikke finnes en backup som kan benyttes til å gjenopprette systemet.

Hvilke minimumskrav definert av Normen er ikke etterlevd?

Du har laget oversikt over hvilken informasjon som behandles i en av virksomhetens tjenester, men oppdager etter en stund at informasjonen er endret, og at det som nå ligger der er feil.

Har du brudd på K, I eller T/R?

Du jobber i et enkelpersonforetak, benytter et godkjent journalsystem og har nettopp vært på kurs og lært om logging.

En selger ringer deg og sier at for å tilfredsstille kravene i Normen anbefaler de en løsning for automatisk innsamling og kontroll av tilgangslogger. Løsningen koster en god del i innkjøp, og har en årlig lisenskostnad.

Vil det være hensiktsmessig å gå til anskaffelse av produktet?

Hva om dette er et større sykehus?