Tema	Klokkeslett
Intro om kurset	09:00
Om Normen	09:10
Spørsmål	*09:35*
Pause	09:45
Risikovurdering/ styring	10:00
Kaffepause	10:45
Internkontroll	11:00
Utvalgt personvern	11:30
Lunsj	12:00
Spørsmål	12:45
Utvalg av Normens krav til informasjonssikkerhet, kap. 5	13:00
Spørsmål	13:45
Pause	14:00
Normens krav i anskaffelser	14:15
Veiledningsmateriell	14:45
Spørsmål	
Takk for i dag	15:30

NORMEN

Risiko: risikostyring og risikovurdering

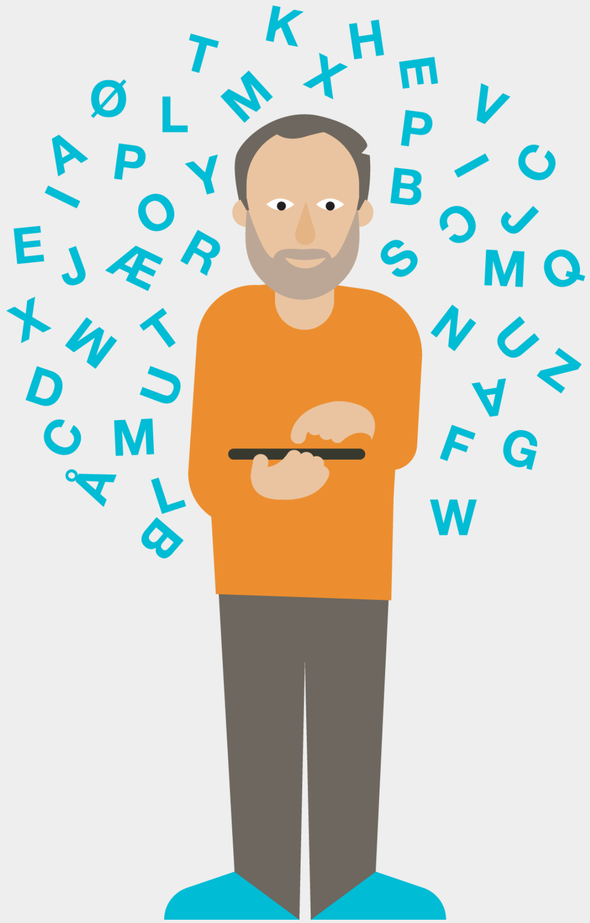
12.05.21

Kurset «Intro om Normen»

Hva er risikostyring?

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

- Få oversikt over informasjon og teknologi i virksomheten
- Identifisere trusler og mulige uønskede hendelser for virksomheten og de registrerte
- Analysere risikoen
- Etablere tiltak for å opprettholde nivå for akseptabel risiko



Hva er risikovurdering?

Risikovurdering er et verktøy for å identifisere uønskede hendelser

- Virksomheten skal vurdere **sannsynligheten** for og mulige **konsekvenser** av at en hendelse inntreffer

- Dersom risikoen er uakseptabel, skal virksomheten gjennomføre **tiltak** for å redusere risikoen

Når skal vi risikovurdere?

Risikovurderinger skal som minimum gjennomføres før:

- 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

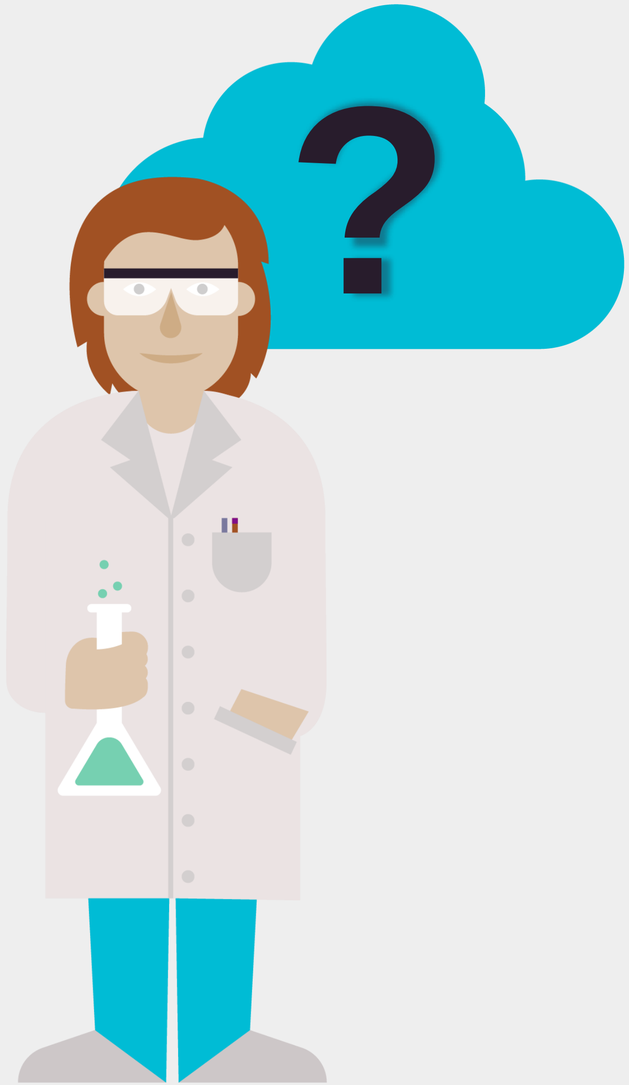
Risikovurdering bør oppdateres ved endring i trusselbildet

Hvordan risikovurderer vi?

Risikovurderingen bør være en strukturert prosess

- Planlegging
- Forberede risikovurderingen
- Gjennomføre risikovurderingen
- Vurdering og anbefaling av nye tiltak

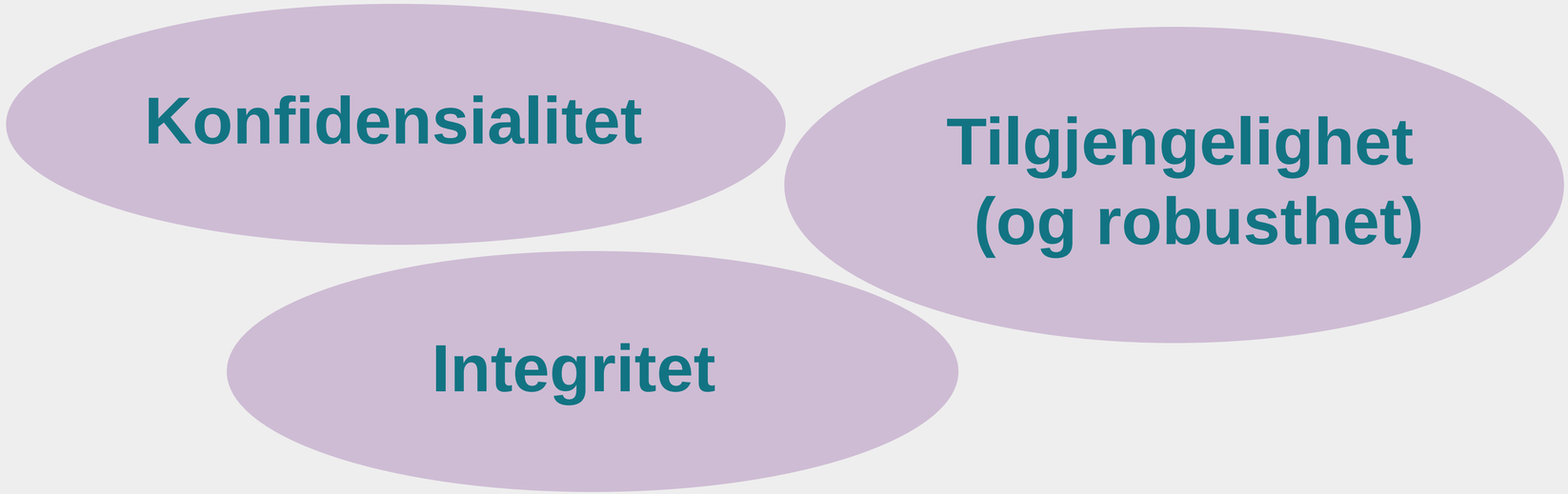
De riktige nøkkelpersonene må være involvert!



POLL

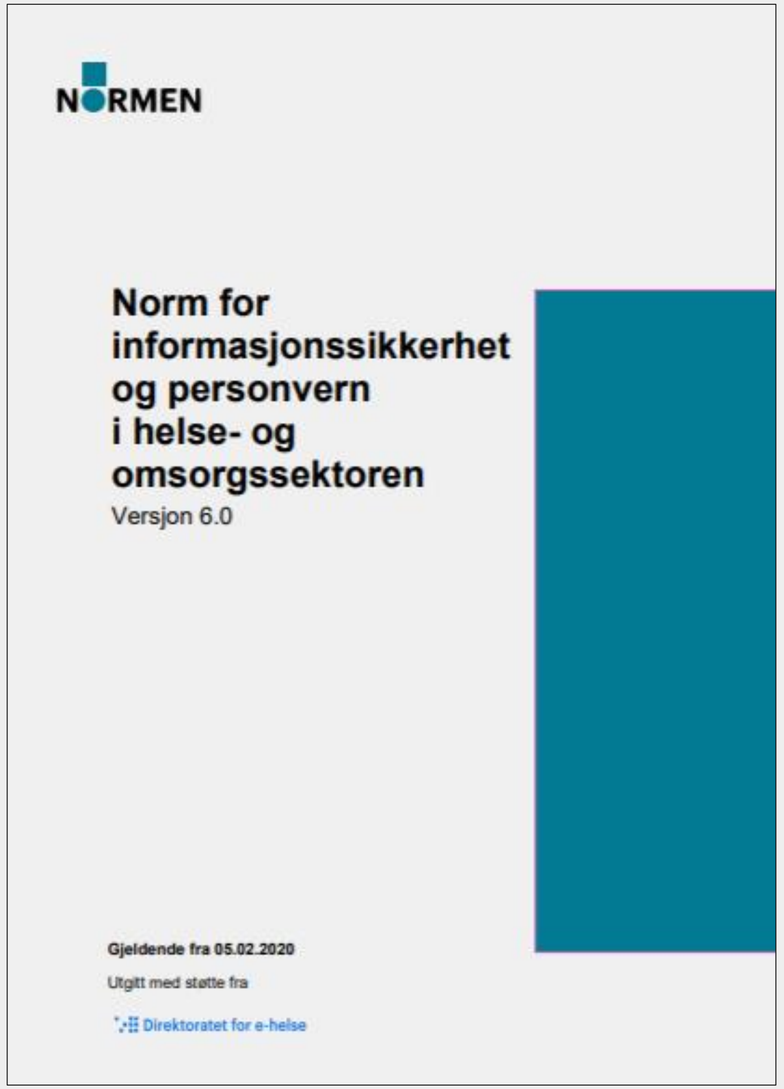
Hva skal vi beskytte?

Risikovurderingen bør ta utgangspunkt i en kartlegging av **informasjonsverdier** og konsekvensen av hendelser som rammer tilgjengeligheten, integriteten og konfidensialiteten til informasjonsverdiene.



Normens krav – minimumskrav

- Normen har en risikobasert tilnærming
- Det finnes krav til konfidensialitet, integritet, tilgjengelighet og robusthet gjennomgående i hele bransjenormen
- Vi har likevel utledet noen såkalte minimumskrav på disse områdene, der alle er formulert som skal-krav

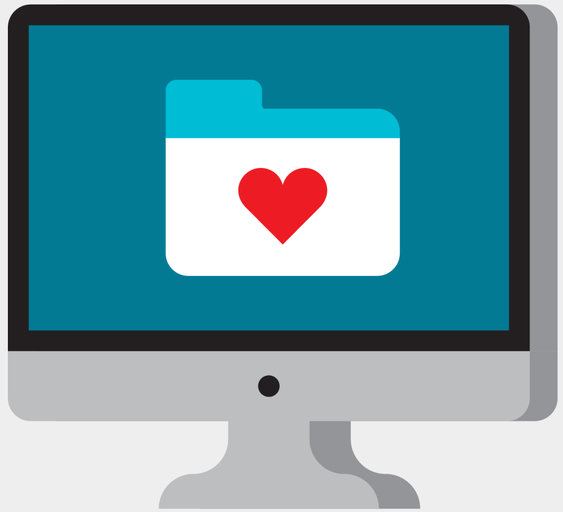


Normens krav for å sikre konfidensialitet

Minimums-krav

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

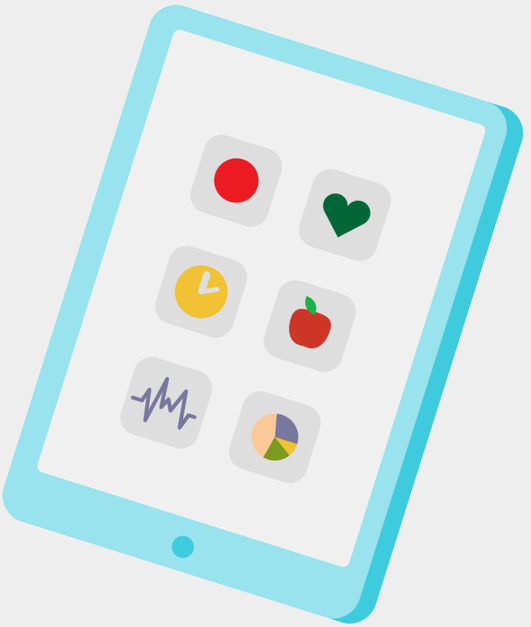


NORMEN

Normens krav for å sikre integritet

Minimums-krav

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

Normens krav til tilgjengelighet og robusthet

Minimums-krav

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

Eksempel – vår egen risikovurdering av GoToWebinar

		Risikoscenario		Eksisterende/planlagte tiltak	Årsak/Sårbarhet	Sannsynlighet		Konsekvens		R
2	#	Beskrivelse av sikkerhetshendelse	Brudd (K-I-T)	Tiltaksbeskrivelse	Sårbarhetsbeskrivelse	Sannsynlighets-beskrivelse	S	Konsekvens-beskrivelse	K	S*K
3		**Risikovurdering av GoToWebinar**								
4	**Scenarioer**									
5	A1	Presentatør deler mer informasjon enn ønsket gjennom skjermdelingsfunksjonen		Opplæring av presentatører i forkant Opplærning av webinarverter	Kan være vanskelig å forstå, særlig ved første gangs bruk	Opplæringstiltak gjør mindre sannsynlig	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
6	A2	Presentatør misforstår funksjonalitet og ender opp med å gjøre noe annet enn planlagt		Opplæring av presentatører i forkant Opplæring av webinarverter	Kan være vanskelig å forstå, særlig ved første gangs bruk	Opplæringstiltak gjør mindre sannsynlig	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
7	A3	Personer som ikke skal ha tilgang til webinaret oppnår tilgang gjennom annens lenke		Informasjon til de påmeldte Kun bruke webinarform til "åpen informasjon"	Ikke sperret tilgang for andre enn de som får tildelt lenke	Mulig ettersom det bare er å videresende lenken på tross av informasjon om at lenken er personlig	3	Webinar skal kun benyttes for åpen informasjon, ubetydelig konsekvens	1	3
8	A4	Personer deler helseopplysninger gjennom spørsmålsfunksjonen		Gjennomgang av kjøreregler i begynnelsen av webinar Rutine for at webinarvert "skriver om" informasjon før det deles i plenum	Ingen sperrer på hva personer kan skrive i spørsmålsfunksjonen	Gjennomgang av kjøreregler gjør mindre sannsynlig, samt at fokus for webinar er tilbydere av helsetjenester og/eller profesjonelle organisasjoner heller enn enkelt-pasienter/-brukere	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
9	A5	Spørsmål/dialog lagres lengre enn nødvendig/slettes ikke (raskt nok)		Etablere rutiner for å slette evt anonymisere	Slettes trolig ikke hos leverandør, men kan trolig anonymiseres	Kjent med at det lagres lengre enn nødvendig, men kan trolig anonymiseres	4	Regelverksbrudd som kan medføre advarsel eller vedtak	2	8
	A6	Vi samler inn mer informasjon om deltagernes oppførsel		Etablere rutiner for at man ikke skal nyttiggjøre seg	Mulighet for analyse av data på personnivå	Kjent med at det samles inn mer enn	4	Regelverksbrudd som kan medføre	2	8

Leserveiledning | Metodebeskrivelse | Planlegging og forberedelse | Omfang | System og kritikalitet | Skala | Skjema | Oppsummering og handling ...

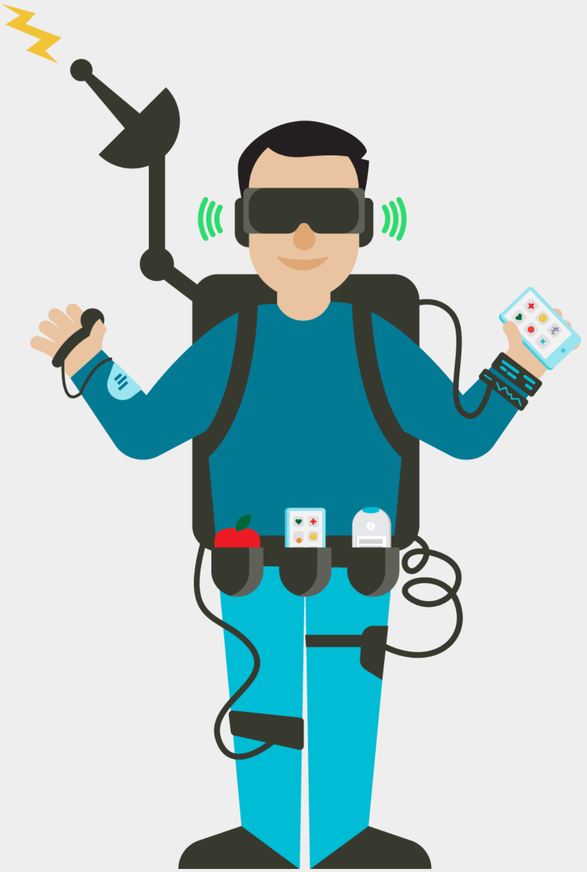
La oss jobbe litt praktisk!

SCENARIO – uønsket hendelse

- Uvedkommende får tilgang til spørsmålene som stilles i GoToWebinar-verktøyet

Informasjonsverdier

- Personopplysninger (navn og virksomhetstilhørighet) til spørsmålsstiller
- Potensielt sensitiv informasjon som deles med webinarets organisator
- …



Sannsynlighet – eksempel på hvordan det kan vurderes

	Tiltaksstyrke	Frekvens
4 – Sannsynlig	Det er ikke iverksatt sikkerhetstiltak. Det er kjente kjente/sårbarheter, og det er identifisert ytterligere tiltak.	>365/1 Daglig eller oftere
3 – Mulig	Sikkerhetstiltak er iverksatt, men de er ikke effektive nok. Det er kjente svakheter/sårbarheter, og det er identifisert ytterligere tiltak.	12/1 En gang hver måned
2 – Mindre sannsynlig	Ett eller flere effektive sikkerhetstiltak er iverksatt, men tiltakene kan omgås av aktører med store ressurser eller med god kjennskap til sikkerhetstiltakene. Det er kjente svakheter/sårbarheter, men det er ikke identifisert ytterligere tiltak.	1/1 En gang hvert år
1 – Usannsynlig	Flere effektive sikkerhetstiltak er iverksatt. Ingen kjente svakheter/sårbarheter som medfører ytterligere tiltak.	1/5 En gang hvert 5. år eller sjeldnere

POLL

Konsekvens – eksempel på hvordan det kan vurderes

	Liv og helse	Personvern	Økonomi	Omdømme
4 – Svært høy	Tap av liv og/eller stor, varig helseskade	Langvarig tap av anseelse eller personlig integritet som er krenkende og som kan medføre tap av liv	Uopprettelig økonomisk konsekvens	Langvarig negativ omtale på riksplan
3 – Høy	Varig helseskade	Tap av anseelse eller personlig integritet som er krenkende og/eller påvirker helse på en alvorlig måte	Alvorlig økonomisk konsekvens	Kortvarig negativ omtale på riksplan
2 – Moderat	Forbigående helseskade	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende og/ eller påvirker helse	Mindre alvorlig økonomisk konsekvens.	Kortvarig negativ omtale lokalt
1 – Lav	Ubetydelig helseskade	Ubetydelig tap av anseelse eller personlig integritet	Ubetydelig økonomisk konsekvens.	Ubetydelig omdømmetap

NORMEN

POLL

POLL

Hvilken risiko har scenarioet vårt?

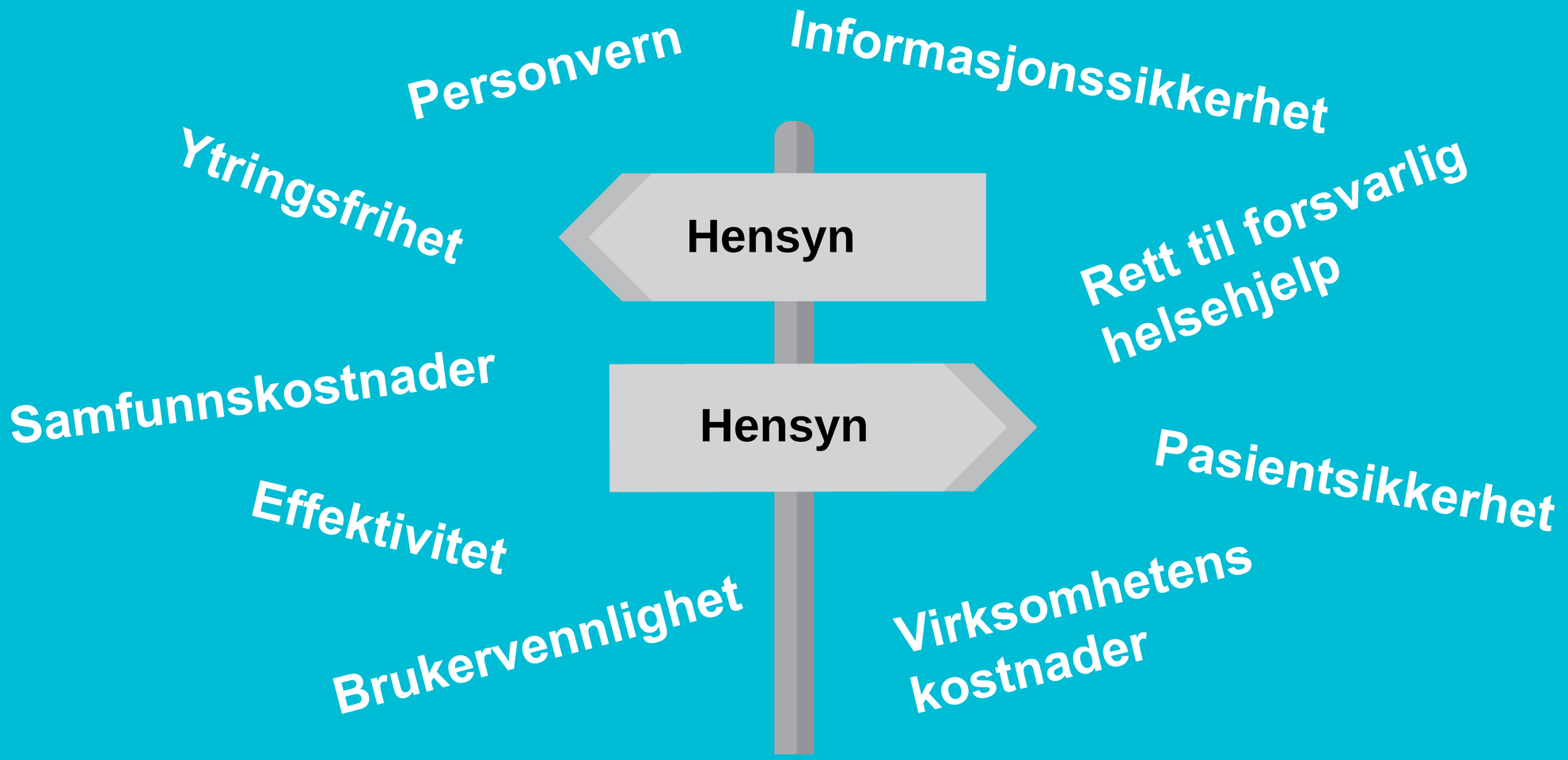
Hva gjør vi nå?

Sannsynlighet					
	4 – Sannsynlig				
	3 – Mulig				
	2 – Mindre sannsynlig				
	1 – Usannsynlig				
		1 – Lav	2 – Moderat	3 – Høy	4 – Svært høy
	Konsekvens				

Hvor høy risiko kan virksomheten akseptere?

Husk at en enkelt risikovurdering er en del av en helhet!

- Ledelsens ansvar
- Ha et bevisst forhold til egen risikoappetitt
  - Hvor mye risiko kan vi leve med?
- Fastsette nivå for akseptabel risiko – akseptkriterier
- Hvilke tiltak kan få risikoen ned på et akseptabelt nivå?
  - Menneskelige, teknologiske, organisatoriske



Vurderinger

Ledelsen må ha «eierskap» til vurderingene og hvilke tiltak som eventuelt implementeres

NORMEN

Hvordan henger dette sammen med personvernforordningen?

- Risikobasert tilnærming og forholdsmessighet
- Risikovurderinger som underlag for vurdering av personvernkonsekvenser (DPIA)
- Det er en del av den dataansvarliges ansvar å gjennomføre egnede tekniske og organisatoriske tiltak
  - Disse kan finnes på grunnlag av risikovurderinger

Hvor finner jeg mer om risiko?

- Normens kapittel 3 – Risikostyring
- Faktaark 04 – Kartlegge og klassifisere systemer
- Faktaark 05 – Fastsette nivå for akseptabel risiko
- Faktaark 07 – Risikovurdering
- Informasjon om relevante risikoscenarioer i spesifikke faktaark og veiledere på ulike temaer (som for eksempel i faktaark 54 om videokonsultasjon, MU-veilederen, skyveilederen)

normen.no

NORMEN

Kaffepause
15 min

Tema	Klokkeslett
Intro om kurset	09:00
Om Normen	09:10
Spørsmål	*09:35*
Pause	09:45
Risikovurdering/ styring	10:00
Kaffepause	10:45
Internkontroll	11:00
Utvalgt personvern	11:30
Lunsj	12:00
Spørsmål	12:45
Utvalg av Normens krav til informasjonssikkerhet, kap. 5	13:00
Spørsmål	13:45
Pause	14:00
Normens krav i anskaffelser	14:15
Veiledningsmateriell	14:45
Spørsmål	
Takk for i dag	15:30

Internkontroll

12.05.21

Kurset «Intro om Normen»

Normens krav til ledelse og ansvar

- Virksomhetenes øverste ledelse har ansvar for at virksomheten følger gjeldende krav etter Normen og lovgivning

- Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver

  - Virksomheten beslutter hvilke roller og funksjoner for informasjonssikkerhet og personvern som er nødvendig

Kjært barn har mange navn

NORMEN

Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

Styringssystem for informasjonssikkerhet og personvern

Støttedokument
Faktaark nr 2
Versjon: 3.2
Dato: 24.10.2019

Digitaliseringsdirektoratet
Internkontroll/styringssystem
(Versjon 1.5)

Hjem
Sammendrag
Systematiske aktiviteter

Internkontroll i praksis - informasjonssikkerhet

NORMEN

Veileder for små helsevirksomheter

Målgruppe

Små virksomheter og enkeltpersonforetak i helse og omsorgssektoren.

Den er primært rettet mot personell med ansvar, oppgaver og roller i forbindelse med personvern og informasjonssikkerhet

Formål

Bidra til tydeligere og mer tjenestetilpassede krav for små virksomheter i helse og omsorgssektoren

Veilederen skal gi den som har det overordnede ansvaret for virksomheten, et godt verktøy for:

- å kunne ha god systematisk styring og ledelse
- å få hjelp til å prioritere
- å aktivt jobbe kontinuerlig med forbedring
- at krav i helse- og omsorgslovgivningen etterleves.

Versjon 1.1

Utgitt med støtte av:
Direktoratet for e-helse

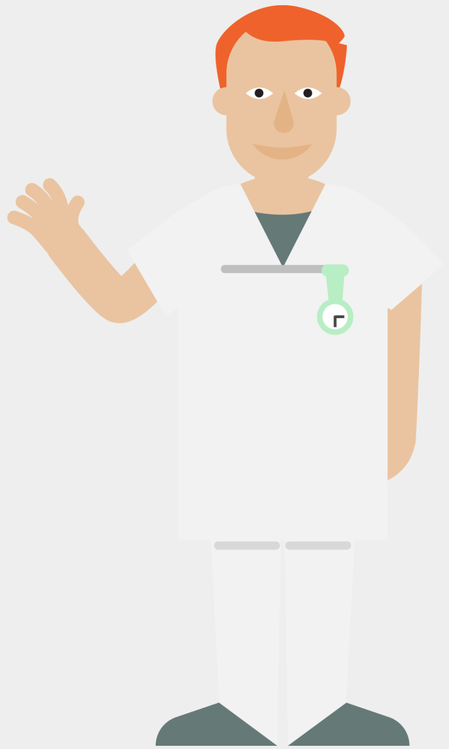
Direktoratet for e-helse

Ledelsessystem for informasjonssikkerhet

Ledelsessystem for informasjonssikkerhet i direktoratet for e-helse

Hvordan ha velfungerende styring og kontroll?

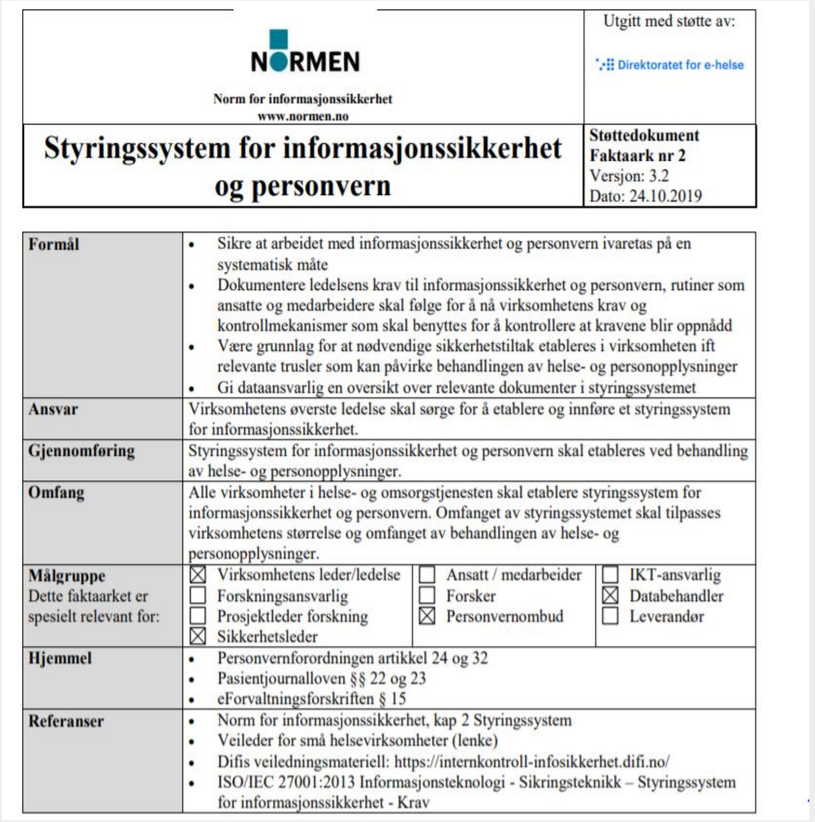
- Etablere et styringssystem / internkontroll for informasjonssikkerhet og personvern
  - Tilpasses virksomhetenes størrelse, risiko, egenart, aktiviteter og de behandlinger din virksomhet gjennomfører
  - Ledelsen har ansvaret for styringssystemet og skal sørge for å gjøre dette kjent for alle ansatte
  - Styringssystemet skal dokumenteres, angitt med løpende oppdatering og arkiveres når det erstattes



- Virksomhetens øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året – Ledelsens gjennomgang
  - Ledelsens gjennomgang skal dokumenteres

Hvordan operasjonalisere et styringssystem?

- Oversikt over behandlinger av helse- og personopplysninger
- Systemoversikt og klassifisering av systemer
- Rutine for opplæring
- Rutiner for plan, gjennomføring og oppfølging av risikovurderinger
- Oversikt over databehandlere og leverandører
- Rutine for oppretting og vedlikehold av autorisasjonsregister
- Rutine for sikkerhetskopiering
- Fysisk sikring av lokaler og områder
- Rutine for innsyn, informasjon, retting og sletting
- Rutine for tilgang til helseopplysninger
- Rutine for utlevering av helseopplysninger til kvalitetssikring
- Autentisering ved tilgang til helseopplysninger
- Avvikshåndtering



NORMEN
Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av: Direktoratet for e-helse

Styringssystem for informasjonssikkerhet og personvern

Støttedokument
Faktaark nr 2
Versjon: 3.2
Dato: 24.10.2019

Formål	• Sikre at arbeidet med informasjonssikkerhet og personvern ivaretas på en systematisk måte • Dokumentere ledelsens krav til informasjonssikkerhet og personvern, rutiner som ansatte og medarbeidere skal følge for å nå virksomhetens krav og kontrollmekanismer som skal benyttes for å kontrollere at kravene blir oppnådd • Være grunnlag for at nødvendige sikkerhetstiltak etableres i virksomheten ift relevante trusler som kan påvirke behandlingen av helse- og personopplysninger • Gi dataansvarlig en oversikt over relevante dokumenter i styringssystemet
Ansvar	Virksomhetens øverste ledelse skal sørge for å etablere og innføre et styringssystem for informasjonssikkerhet.
Gjennomføring	Styringssystem for informasjonssikkerhet og personvern skal etableres ved behandling av helse- og personopplysninger.
Omfang	Alle virksomheter i helse- og omsorgstjenesten skal etablere styringssystem for informasjonssikkerhet og personvern. Omfanget av styringssystemet skal tilpasses virksomhetens størrelse og omfanget av behandlingen 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	• Personvernforordningen artikkel 24 og 32 • Pasientjournalloven §§ 22 og 23 • eForvaltningsforskriften § 15
Referanser	• Norm for informasjonssikkerhet, kap 2 Styringssystem • Veileder for små helsevirksomheter (lenke) • Difis veiledningsmateriell: https://internkontroll-infosikkerhet.difi.no/ • ISO/IEC 27001:2013 Informasjonsteknologi - Sikringsteknikk – Styringssystem for informasjonssikkerhet - Krav

POLL

POLL

Normens krav til ledelse og ansvar – Dataansvar

Normens krav 2.2

2.2 Dataansvarliges ansvar

Dataansvarlig er den som alene eller sammen med andre virksomheter bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes.

I personvernforordningen benyttes begrepet behandlingsansvarlig, som er det samme som dataansvarlig i helsesektoren.

Dataansvarlig skal

- delegere myndighet og oppgaver (jf. kap. 2.1)
- etablere og etterleve styringssystemet (jf. kap. 2.4)
- gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig (jf. kap. 3)
- sikre den registrertes rettigheter (jf. kap. 4)
- etablere og dokumentere tekniske og organisatoriske tiltak (jf. kap. 5)
- inngå og følge opp avtaler (jf. kap. 5.7)
- håndtere avvik (jf. kap. 5.8)

NORMEN

Ansvarlighetsprinsippet etter personvernforordningen

Normens krav 2.2

Dataansvarlig er ansvarlig for å opptre i henhold til personvernprinsippene. Dette innebærer at helse- og personopplysninger skal

- behandles på en lovlig måte (gyldig behandlingsgrunnlag)
- behandles på en rettferdig måte (med respekt for de registrertes interesser og rettigheter)
- behandles på en åpen måte (oversiktlig, forutsigbar og forståelig informasjon) med hensyn til den registrerte (pasienten/brukeren)
- bare registreres for bestemte formål som skal være legitime (som dokumentasjon av helsehjelp)
- være tilgjengelige for helsepersonell når dette er nødvendig for å kunne gi forsvarlig helsehjelp
- bare benyttes til de formål de er registrert for, med mindre det finnes behandlingsgrunnlag for andre formål
- være relevante, adekvate, korrekte og om nødvendig oppdaterte for de formål de er registrert for
- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene
- sikres mot uautorisert tilgang, endring, ødeleggelse og spredning

Dataansvarlig skal dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernforordningen.

NORMEN

Personvernforordningen

«Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige **gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov**.»

Artikkel 24:
Den behandlingsansvarliges (dataansvarliges) ansvar

= **Internkontroll**

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

- Med formål om å bidra til forsvarlige helse- og omsorgstjenester, pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves

- Den med det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter
  - Plikt til å planlegge
  - Plikt til å gjennomføre
  - Plikt til å evaluere
  - Plikt til å korrigere

§ 2.Virkeområde

Forskriften gjelder virksomheter som er pålagt internkontrollplikt etter

a) helsetilsynsloven § 5

b) spesialisthelsetjenesteloven § 2-1a tredje ledd

c) helse- og omsorgstjenesteloven § 3-1 tredje ledd eller

d) tannhelsetjenesteloven § 1-3a.

Forskriften gjelder også virksomheter som er pålagt plikt til å arbeide systematisk for kvalitetsforbedring og pasient- og brukersikkerhet etter

a) spesialisthelsetjenesteloven § 3-4a eller

b) helse- og omsorgstjenesteloven § 4-2.

NORMEN

Hvor finner jeg mer om internkontroll?

- Faktaark 01 – Ansvar og organisering
- Faktaark 02 – Styringssystem for informasjonssikkerhet og personvern
- Faktaark 04 – Kartlegge og klassifisere systemer
- Faktaark 05 – Fastsette nivå for akseptabel risiko
- Faktaark 06 – Sikkerhetsrevisjon
- Faktaark 07 – Risikovurdering
- Faktaark 08 – Avviksbehandling
- Faktaark 13 – Oversikt over behandling av helse- og personopplysninger i virksomheten
- Faktaark 37 – Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter
- Faktaark 55 – Sperret adresse i folkeregisteret
- Veileder for små helsevirksomheter

normen.no