Webinar:
Ny veileder om internkontroll for informasjonssikkerhet og personvern

12.01.22

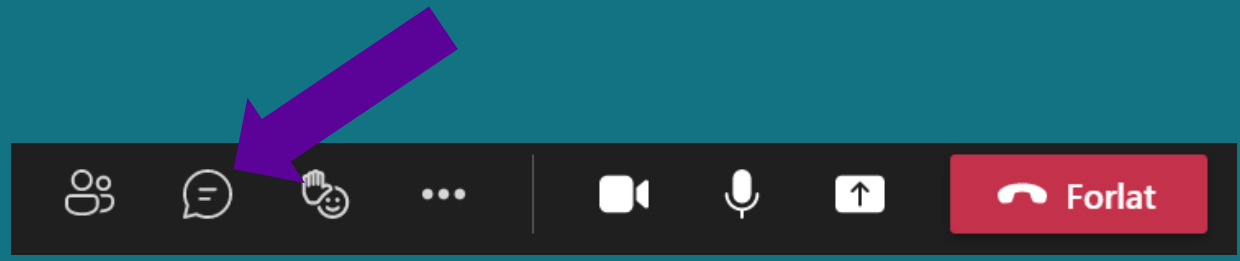
Kjøreregler

- Møteleder styrer ordet
- Vi setter mikrofonene deres på «mute» fra start
- Det foretas opptak av dette webinaret
- Vi legger ut opptak og presentasjoner på normen.no (se også opptak fra Normkonferansen!)

NORMEN

Spørsmål og kommentarer underveis

- Bruk chatfunksjonen når som helst under webinaret til spørsmål eller kommentarer
- Send spørsmål eller kommentarer direkte til meg om du ikke ønsker å skrive i møtechatten
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Hvis du har spørsmål som ikke blir besvart under webinaret eller innspill du ønsker å komme med i etterkant, send oss en epost til sikkerhetsnormen@ehelse.no



NORMEN

Agenda

- Bakgrunn for oppdatering av veiledningsmateriell innen internkontroll
- Litt om prosessen
- Innhold i veilederen

BAKGRUNN FOR OPPDATERING

Hvorfor oppdatere Normens veiledningsmateriell om internkontroll?

- Endringer i krav som er spesielt viktige for internkontrollen
  - Artikler i personvernforordningen (GDPR) som beskriver dataansvarlig og databehandlers ansvar, samt øvrige endringer som følge av ny personopplysningslov
  - Forskrift for ledelse og kvalitetsforbedring i helse- og omsorgstjenesten som beskriver at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter i tråd med forskriften, og at medarbeiderne i virksomheten medvirker til dette

- Digitaliseringsdirektoratets oppdaterte veiledningsmateriell på internkontrollområdet

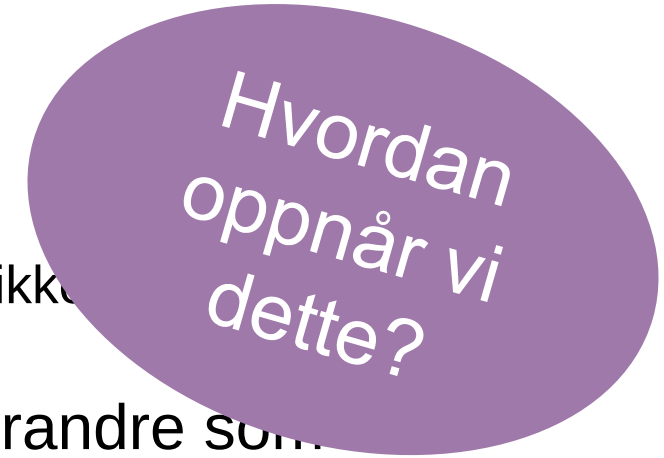
- Behov for generell faglig oppdatering og brukervennlig restrukturering av veiledningen på området

Oppdatering av veiledningsmateriell: Internkontroll og risikostyring

- 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 07 Risikovurdering
- Faktaark 08 Avviksbehandling
- Faktaark 09 Opplæring av ledere og medarbeidere
- Faktaark 27 Retningslinjer for daglig informasjonssikkerhet
- Faktaark (nytt) om personvernkonsekvensvurdering (DPIA)
- Veileder for små helsevirksomheter
- Mal for internkontroll legekontor
- Mal for internkontroll psyk, fysio, manuell, og kiropraktor
- Mal for internkontroll tannhelsetjeneste
- Mal for internkontroll apotek

Temaer som inngikk i arbeidspakken

Målsetninger/prinsipper for veiledningsmateriell i pakken



- Vise sammenhengene mellom ulike delprosesser
  - For eksempel mellom ulike typer risikovurderinger (informasjonssikk
    pasientsikkerhet, DPIA)
- Synliggjøre behovet for å veie ulike hensyn opp mot hverandre som
  del av risikostyringen
- Synliggjøre ledelsens ansvar og behov for beslutningsgrunnlag
- Ikke skrive mye om det samme mange steder
  - Unngå dobbeltarbeid både i arbeidet med veiledningsmateriellet og for virksomhetene som skal benytte materiellet i sine prosesser
- Sektorspesifikt og praktisk rettet
  - Ikke for teoretikerne, men for de som skal gjøre dette i praksis i sektoren

… ved å organisere de faglige temaene på denne måten

Internkontroll

- Faktaark 01 - Ansvar og organisering
- Faktaark 02 - Styringssystem for info.sikkerhet og personvern
- Faktaark 08 - Avviksbehandling
- Faktaark 09 - Opplæring av ledere og medarbeidere
- Faktaark 27 - Retningslinjer for daglig informasjonssikkerhet
- Nytt tema: sikkerhetskultur i helse- og omsorgssektoren
- Maler og eksempler (bl.a. fra maler for internkontroll for små virksomheter)
- Sette de ulike prosessene som er en del av internkontrollen mer i sammenheng
- Beskrive at risikostyring er en del av den totale internkontrollen, henvise til risikoveileder

Risikostyring

- Faktaark 04 - Kartlegge og klassifisere systemer
- Faktaark 05 - Fastsette nivå for akseptabel risiko
- Faktaark 07 - Risikovurdering
- Nytt tema: Vurdering av personvernkonsekvenser (DPIA)
- Maler og eksempler
- Sette de ulike prosessene som er en del av risikostyringen mer i sammenheng

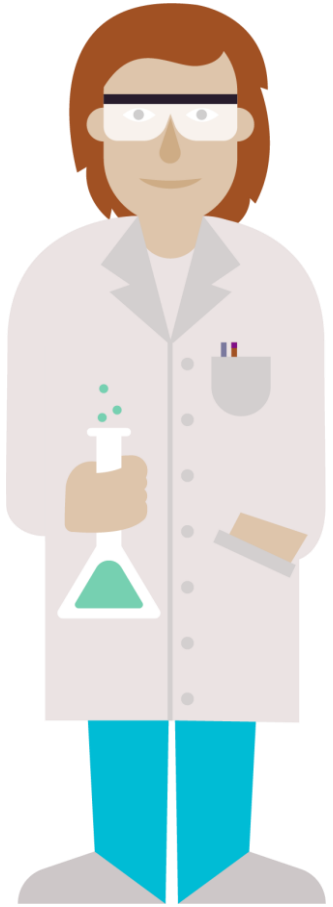
- Oppdatere og tilpasse veileder for små virksomheter ved behov, i tråd med ny veiledning og med riktige henvisninger

NORMEN

LITT OM PROSESSEN

Kort om prosessen – gjennomførte aktiviteter

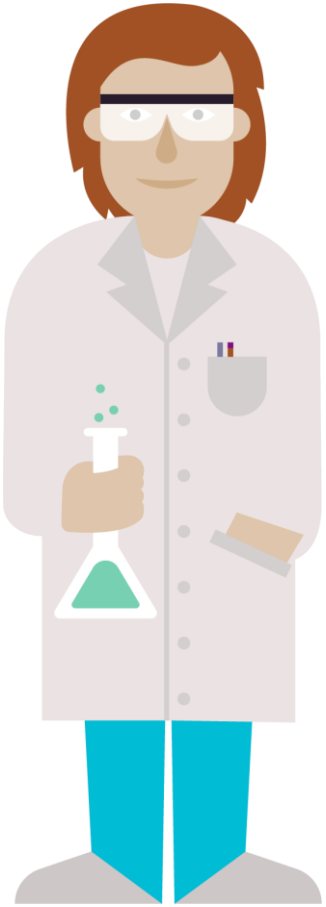
- Oppstart arbeid med oppdatering feb/mars 2021
- Innspillswebinar for veiledning om DPIA ble gjennomført 5. mai
  - Menti for å samle konkrete innspill om utfordringer, behov og eksempler/maler fra sektoren
- Innspill fra styringsgruppen og andre aktører i sektoren
- Etablert referansegruppe med representanter fra sektoren
  - Deltakere fra Sykehuspartner, Hemit, Helse Vest IKT, KiNS, Ikomm, Fürst, HSØ, UNN, Digdir, Bergen, Gamvik og Larvik kommune
  - Fagbakgrunn: IT, informasjonssikkerhet, personvern, helsepersonell
- Overordnet fremleggelse av planlagte endringer for Nettverk for veiledningsaktører styring og kontroll 16. juni
- Sendt ut underlag til referansegruppe
- Referansegruppemøte 22. juni



NORMEN

Kort om prosessen – gjennomførte aktiviteter

- Innspillswebinar 23. juni og 25. august
  - Tema struktur og overordnet innhold
- Styringsgruppemøte 20. september
  - Innspill fra medlemmene i SG
- Fullstendig utkast delt med referansegruppen 4. oktober
- Innspill mottatt på e-post i forkant og diskutert på møtet
- Referansegruppemøte 15. oktober
- Ferdig utkast sendt til styringsgruppen iht. dokumentfrist
- Godkjent på styringsgruppemøte 2. desember
- Publisert på normen.no desember 2021



INNHOLD I VEILEDEREN

Faktaark som inngår i veilederen

Innhold fra følgende faktaark inngår i veilederen:

- *Faktaark 01 – Ansvar og organisering*
- *Faktaark 02 – Styringssystem for informasjonssikkerhet og personvern*
- *Faktaark 08 – Avviksbehandling*
- *Faktaark 09 – Opplæring av ledere og medarbeidere*
- *Faktaark 27 – Retningslinjer for daglig informasjonssikkerhet*

Disse faktaarkene ble sanert ved publisering av veilederen

Om veilederen

- Denne veilederen skal gi veiledning til, og bidra til etterlevelse av, kravene i Normen knyttet til internkontroll.
- Veilederen er nyttig for alle ledere og medarbeidere i helse- og omsorgssektoren. Ledere er en særlig viktig målgruppe. Også nyttig for systemleverandører og andre samarbeidspartnere til sektoren.
- Internkontroll for informasjonssikkerhet og personvern er en del av virksomhetens helhetlige internkontroll, men ikke fokus på øvrige internkontrollkrav i veilederen. Heller ikke på internkontrollkrav utenfor sektoren. Krav til risikostyring behandles i egen veileder.

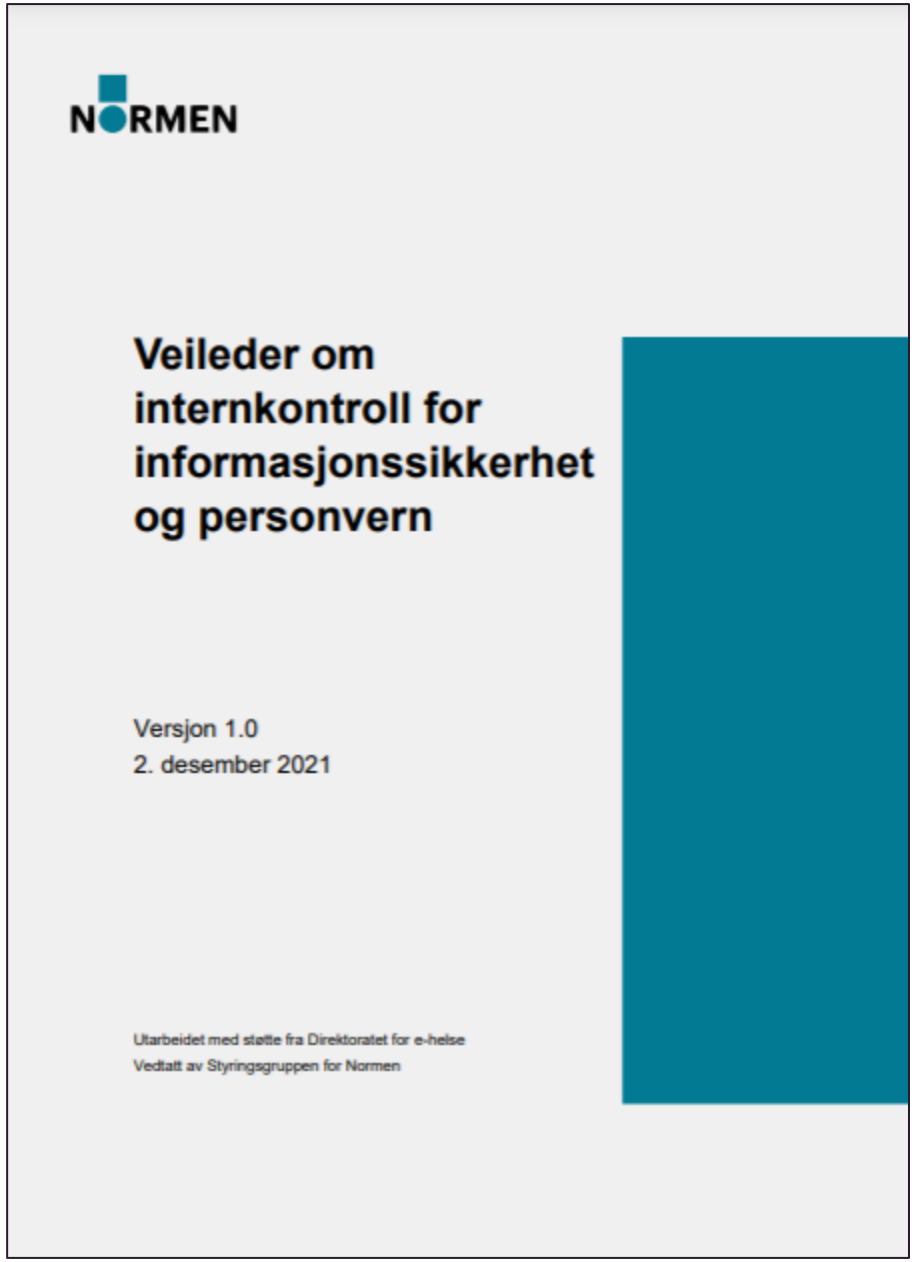
Viktige problemstillinger og løsninger

Problemstilling	Løsning
Krevende for sektoren å forholde seg til en rekke enkeltstående faktaark	Samle innhold fra faktaarkene i en helhetlig veileder om internkontroll
Veilederen ville bli svært omfattende om alle temaer skulle inkluderes i veilederen, kan bli overveldende og lite oversiktlig	Temaer tilknyttet risikostyring skilt ut i en egen veileder
Normen hadde i liten grad veiledning på sikkerhetskultur og kompetanseheving	Nyutvikling av veiledning på dette området med eget kapittel

Hvor finner du veilederen?

normen.no

> Veiledere



Spørsmål?


NORMEN
Veileder om internkontroll for informasjonssikkerhet og personvern
Versjon 1.0
2. desember 2021
Utarbeidet med støtte fra Direktoratet for e-helse
Vedtatt av Styringsgruppen for Normen

Bli med på kurs og webinarer med Normen gjennom året!

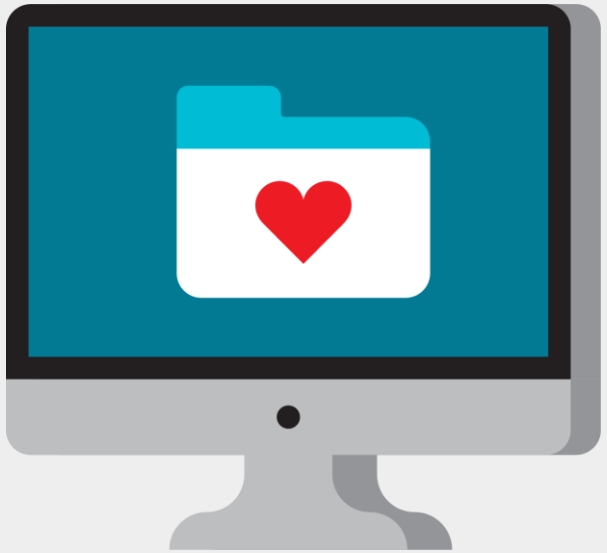
19. januar	Risikostyring – gjennomgang av ny veileder
26. januar	Tilgang til helse- og personopplysninger
02. februar	Om logging
09. februar	Gjesteforedrag fra Helsedirektoratet
16. februar	Informasjonssikkerhet og personvern i forskningsprosjekt
23. februar	Om formål og behandlingsgrunnlag
02. mars	Om lagring og sletting
09. mars	Gjennomgang agenda til styringsgruppemøte 17. mars

Følg med på normen.no, sosiale medier og Normens nyhetsbrev!

NORMEN

Ta gjerne kontakt med oss i Normen!

- Hva vil du høre mer om?
- Hva trenger du veiledning på?
- Hva kan vi bidra med?



sikkerhetsnormen@ehelse.no

NORMEN

Takk for oss!