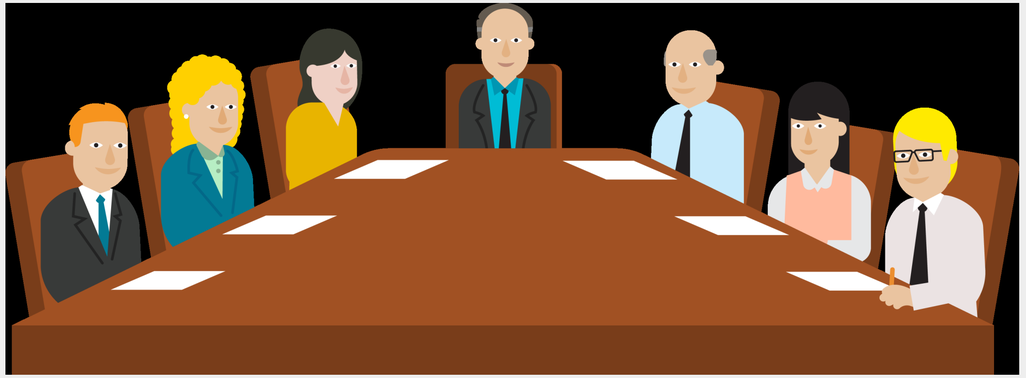
# Ledelse og ansvar – styringssystem for personvern og informasjonssikkerhet (internkontroll)

Introkurs til Normen
08.10.20

# Normens krav til ledelse og ansvar

- Virksomhetenes øverste ledelse har ansvaret for at virksomheten følger gjeldende krav etter Normen og lovgivning
  - Velfungerende styring og kontroll
  - Dokumentere alle tiltak

- 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

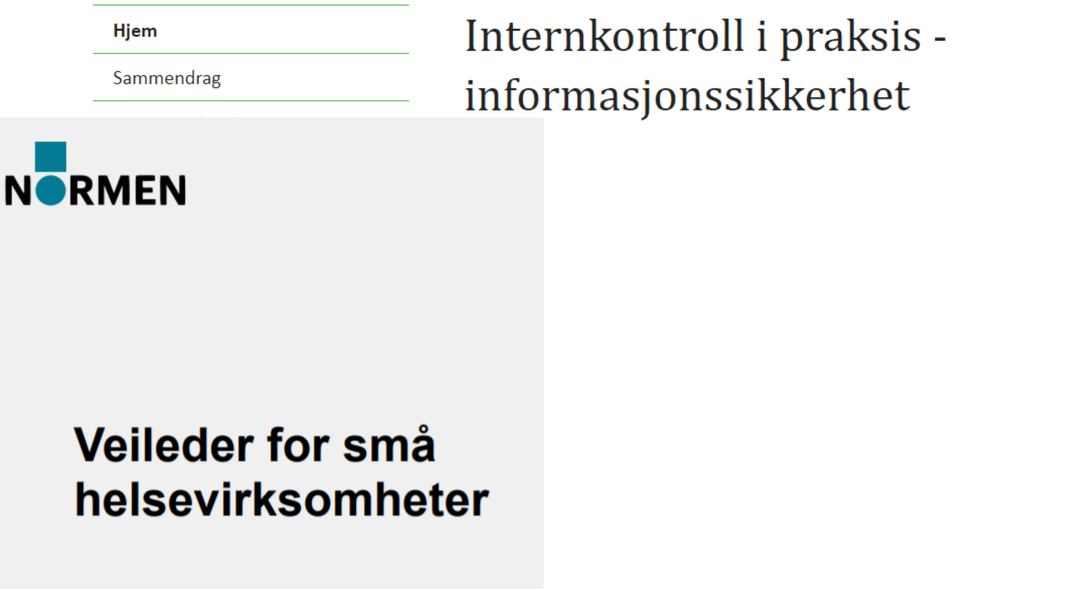
Norm for informasjonssikkerhet
www.normen.no

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

Internkontroll i praksis - informasjonssikkerhet

NORMEN

**Veileder for små helsevirksomheter**

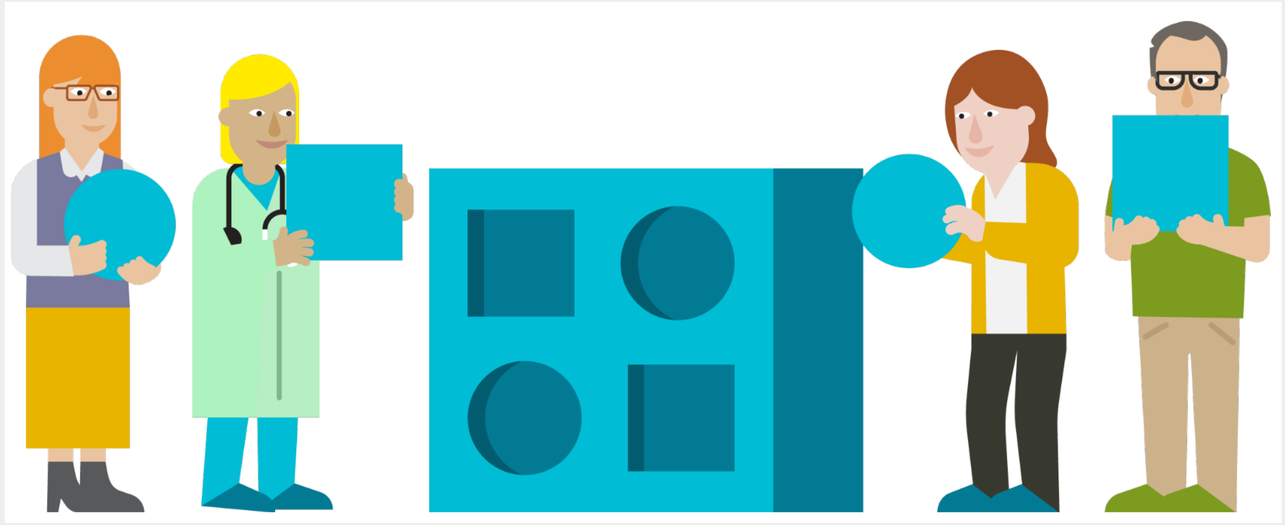
Direktoratet for e-helse

Ledelsessystem for informasjonssikkerhet

*Ledelsessystem for informasjonssikkerhet i direktoratet for e-helse*

# Hvordan ha velfungerende styring og kontroll?

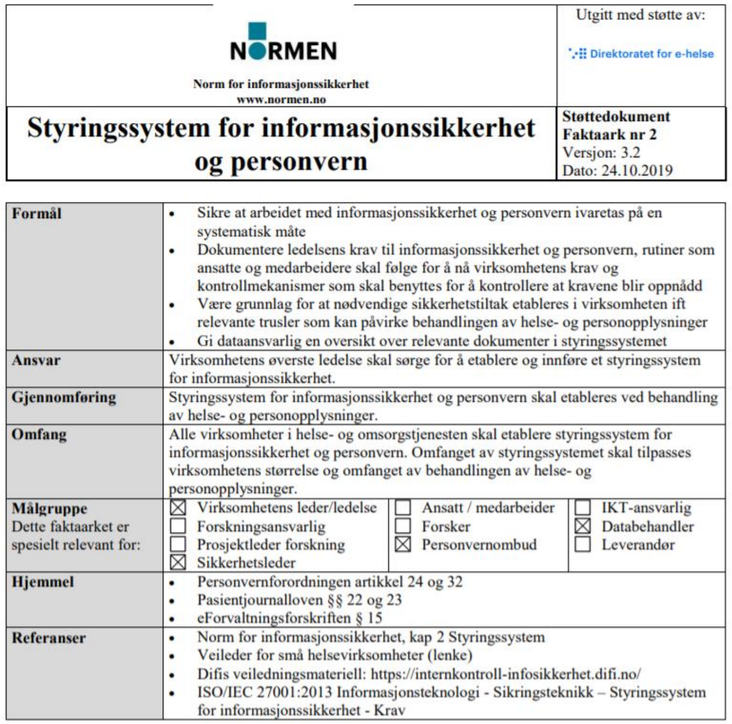
- Etablere et styringssystem/ internkontroll for informasjonssikkerhet og personvern
  - Tilpasses virksomhetenes størrelse, risiko, egenart, aktiviteter og de behandlinger din virksomhet gjennomfører
  - Ledelsen har ansvaret for styringssystemet og skal sørge for å gjøre dette kjent for alle ansatte
  - 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



NORMEN

# 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<br>Norm for informasjonssikkerhet<br>www.normen.no | Utgitt med støtte av:<br>Direktoratet for e-helse |
|---|---|
| **Styringssystem for informasjonssikkerhet og personvern** | **Støttedokument**<br>**Faktaark nr 2**<br>Versjon: 3.2<br>Dato: 24.10.2019 |

| | | | |
|---|---|---|---|
| **Formål** | • Sikre at arbeidet med informasjonssikkerhet og personvern ivaretas på en systematisk måte<br>• 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<br>• Være grunnlag for at nødvendige sikkerhetstiltak etableres i virksomheten ift relevante trusler som kan påvirke behandlingen av helse- og personopplysninger<br>• 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**<br>Dette faktaarket er spesielt relevant for: | ☒ Virksomhetens leder/ledelse<br>☐ Forskningsansvarlig<br>☐ Prosjektleder forskning<br>☒ Sikkerhetsleder | ☐ Ansatt / medarbeider<br>☐ Forsker<br>☒ Personvernombud | ☐ IKT-ansvarlig<br>☒ Databehandler<br>☐ Leverandør |
| **Hjemmel** | • Personvernforordningen artikkel 24 og 32<br>• Pasientjournalloven §§ 22 og 23<br>• eForvaltningsforskriften § 15 | | |
| **Referanser** | • Norm for informasjonssikkerhet, kap 2 Styringssystem<br>• Veileder for små helsevirksomheter (lenke)<br>• Difis veiledningsmateriell: https://internkontroll-infosikkerhet.difi.no/<br>• ISO/IEC 27001:2013 Informasjonsteknologi - Sikringsteknikk – Styringssystem for informasjonssikkerhet - Krav | | |

# POLL

**Har din virksomhet et styringssystem?**

# POLL

**Hvis ja, bruker du din virksomhets styringssystem?**

# Normens krav til ledelse og ansvar – Dataansvar

**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

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

# Artikkel 24 – den behandlingsansvarliges (dataansvarliges) ansvar

1. 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.**

**= Styringssystem**

# 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

# Styringssystem

01 - Ansvar og organisering

02 - Styringssystem for informasjonssikkerhet og personvern

04 - Kartlegge og klassifisere systemer

05 - Fastsette nivå for akseptabel risiko

06 - Sikkerhetsrevisjon

07 - Risikovurdering

08 - Avviksbehandling

13 - Oversikt over behandling av helse- og personopplysninger i virksomheten

37 - Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter

55 – Sperret adresse i folkeregistret

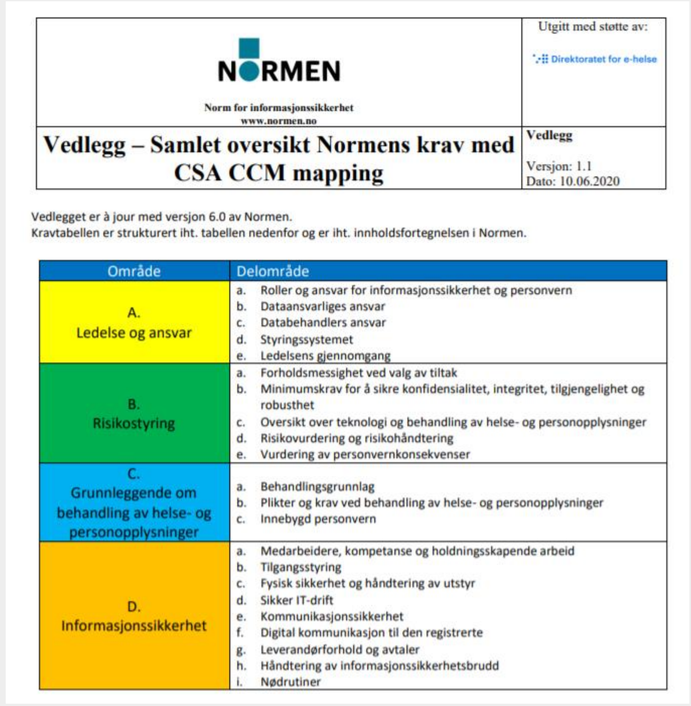
NORMEN

# Kort om utvalgte veiledningsmateriell

# Veileder for bruk av skytjenester

Veilederen gir praktisk hjelp innenfor områdene:

- Fastsette ansvar, inngå avtaler, ivareta kontroll og vurdere risiko
- Belyse fordeler ved teknologien
- Synliggjøre trusler og behov for kontroll
- Ivaretakelse av pasientens rettigheter til samtykke, innsyn, retting sletting mv.
- Eksempler på risikoområder som det er naturlig å belyse
- Etabler databehandleravtale
- Behandling av helse- og personopplysninger under Normens virkeområde



NORMEN

Norm for informasjonssikkerhet
www.normen.no

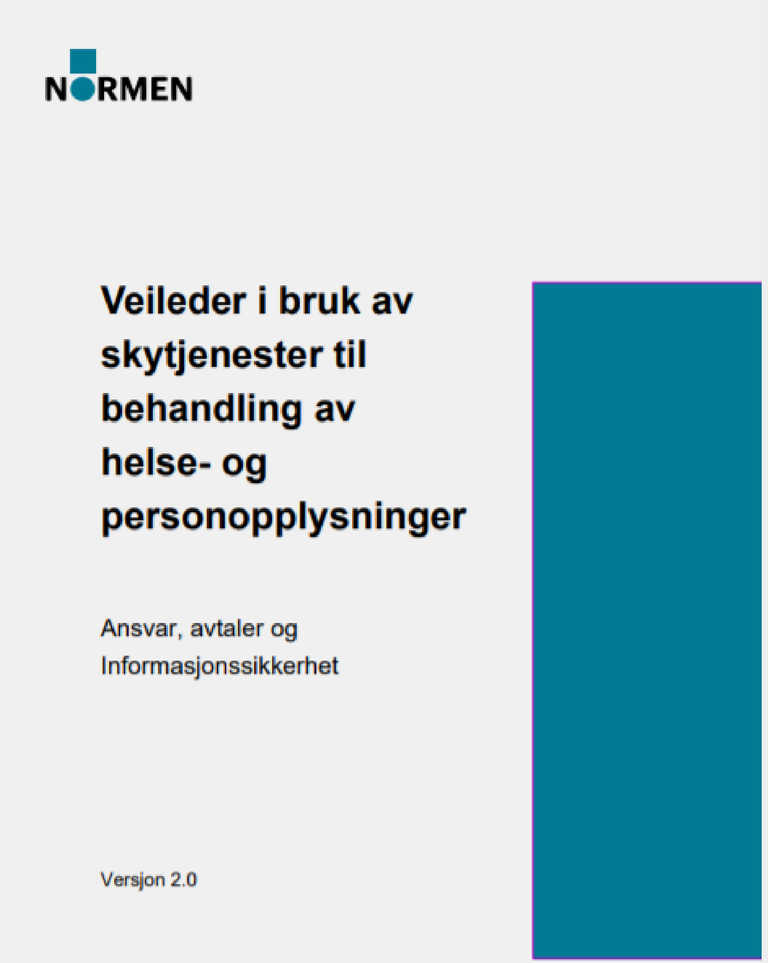
Utgitt med støtte av:
Direktoratet for e-helse

**Vedlegg – Samlet oversikt Normens krav med CSA CCM mapping**

**Vedlegg**
Versjon: 1.1
Dato: 10.06.2020

Vedlegget er à jour med versjon 6.0 av Normen.
Kravtabellen er strukturert iht. tabellen nedenfor og er iht. innholdsfortegnelsen i Normen.

| Område | Delområde |
|---|---|
| A. Ledelse og ansvar | a. Roller og ansvar for informasjonssikkerhet og personvern<br>b. Dataansvarliges ansvar<br>c. Databehandlers ansvar<br>d. Styringssystemet<br>e. Ledelsens gjennomgang |
| B. Risikostyring | a. Forholdsmessighet ved valg av tiltak<br>b. Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet<br>c. Oversikt over teknologi og behandling av helse- og personopplysninger<br>d. Risikovurdering og risikohåndtering<br>e. Vurdering av personvernkonsekvenser |
| C. Grunnleggende om behandling av helse- og personopplysninger | a. Behandlingsgrunnlag<br>b. Plikter og krav ved behandling av helse- og personopplysninger<br>c. Innebygd personvern |
| D. Informasjonssikkerhet | a. Medarbeidere, kompetanse og holdningsskapende arbeid<br>b. Tilgangsstyring<br>c. Fysisk sikkerhet og håndtering av utstyr<br>d. Sikker IT-drift<br>e. Kommunikasjonssikkerhet<br>f. Digital kommunikasjon til den registrerte<br>g. Leverandørforhold og avtaler<br>h. Håndtering av informasjonssikkerhetsbrudd<br>i. Nødrutiner |



NORMEN

**Veileder i bruk av skytjenester til behandling av helse- og personopplysninger**

Ansvar, avtaler og Informasjonssikkerhet

Versjon 2.0

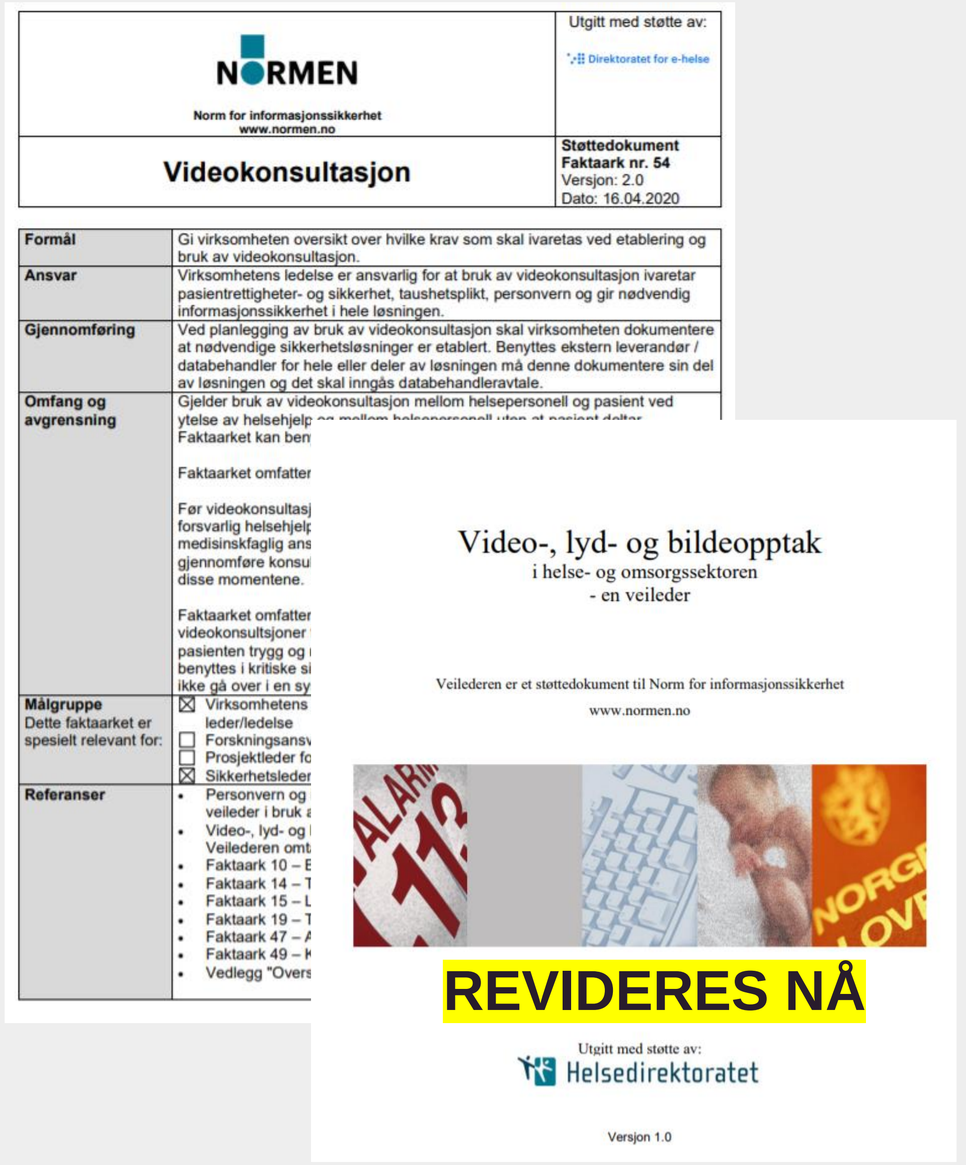
NORMEN

# Veiledere i medisinsk utstyr og velferdsteknologi

- Behandling av helse- og personopplysninger i tråd med regelverk
- Hvordan medisinsk utstyr og velferdsteknologi kan beskyttes mot angrep og sårbarheter
- Brukerscenarier
- VFT veilederen publiseres i ny versjon i neste uke!
- MU veilederen oppdateres nå med snarlig publisering
- Normen arrangerer eget kurs for med.tek personell og andre som jobber med medisinsk utstyr og velferdsteknologi – NESTE nyåret 2021

# Videokonsultasjon

- Ny versjon av FA 54 – pga. Covid-19 stort behov for oppdatert veiledning
  - Normens krav til informasjonssikkerhet ve bruk av videokonsultasjon bl.a.:
    - Sikre lovlig behandling
    - Informasjon til pasient
    - Entydig identifisering av pasient og personell
    - Entydig identifisering av utstyr levert av virksomhet
    - Kryptering av kommunikasjon
    - Logging
    - Ivaretakelse av taushetsplikt
  - Risikovurdering med eksempler på scenarier
  - Rutiner og opplæring
  - Bruk av databehandler



NORMEN
Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

**Videokonsultasjon**

**Støttedokument**
**Faktaark nr. 54**
Versjon: 2.0
Dato: 16.04.2020

| | |
|---|---|
| **Formål** | Gi virksomheten oversikt over hvilke krav som skal ivaretas ved etablering og bruk av videokonsultasjon. |
| **Ansvar** | Virksomhetens ledelse er ansvarlig for at bruk av videokonsultasjon ivaretar pasientrettigheter- og sikkerhet, taushetsplikt, personvern og gir nødvendig informasjonssikkerhet i hele løsningen. |
| **Gjennomføring** | Ved planlegging av bruk av videokonsultasjon skal virksomheten dokumentere at nødvendige sikkerhetsløsninger er etablert. Benyttes ekstern leverandør / databehandler for hele eller deler av løsningen må denne dokumentere sin del av løsningen og det skal inngås databehandleravtale. |
| **Omfang og avgrensning** | Gjelder bruk av videokonsultasjon mellom helsepersonell og pasient ved ytelse av helsehjelp og mellom helsepersonell uten at pasient deltar<br>Faktaarket kan ben<br><br>Faktaarket omfatter<br><br>Før videokonsultasj<br>forsvarlig helsehjelp<br>medisinskfaglig ans<br>gjennomføre konsu<br>disse momentene.<br><br>Faktaarket omfatter<br>videokonsultsjoner<br>pasienten trygg og<br>benyttes i kritiske si<br>ikke gå over i en sy |
| **Målgruppe**<br>Dette faktaarket er spesielt relevant for: | ☒ Virksomhetens leder/ledelse<br>☐ Forskningsansv<br>☐ Prosjektleder fo<br>☒ Sikkerhetsleder |
| **Referanser** | • Personvern og veileder i bruk<br>• Video-, lyd- og<br>Veilederen omt<br>• Faktaark 10 – E<br>• Faktaark 14 – T<br>• Faktaark 15 – L<br>• Faktaark 19 – T<br>• Faktaark 47 – A<br>• Faktaark 49 – K<br>• Vedlegg "Overs |

Video-, lyd- og bildeopptak
i helse- og omsorgssektoren
- en veileder

Veilederen er et støttedokument til Norm for informasjonssikkerhet

www.normen.no




**REVIDERES NÅ**

Utgitt med støtte av:
Helsedirektoratet

Versjon 1.0