Velkommen til kurs og intro til Normen

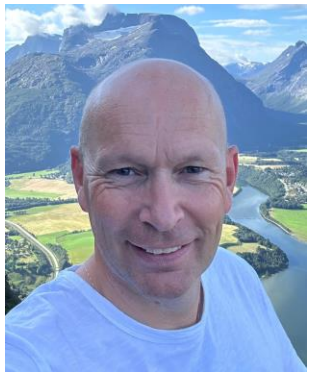
10.01.24

Plan for dagen

09:00 - 09:45	Intro om kurset og om Normen
09:45 - 10:00	Pause
10:00 - 10:30	Internkontroll
10:30 - 10:45	Benstrekk og påfyll av kaffe
10:45 - 11:30	Risikostyring
11:30 - 12:05	Lunsj
12:05 - 12:45	Utvalgt personvern
12:45 - 13:00	Pause
13:00 - 13:45	Krav til informasjonssikkerhet
13:45 - 14:05	Gruppeoppgave - breakout room
14:05 - 14:15	Benstrekk og påfyll av kaffe
14:15 - 14:45	Normens krav i anskaffelser
14:45 - 15:00	Spørsmål og avslutning

Thea Rølsåsen

Andrea Dahl Spone (NHN)



André Meldal (NHN)

Aasta Hetland (Sekretariatsleder)

Jan Gunnar Broch (Seksjonsleder)

John Marius Solli

Knut Herje

Susanne Helland Flatøy

Inger Anne Tøndel

Geir-Erlend Myhre Johansen

Marie Strand Schildmann

Tonje Stegavik

Sekretariatet for Normen

NORMEN

Styringsgruppen for Normen

Helse- og omsorgsdepartementet

Helsedirektoratet

Sekretariatet for Normen

NORMEN

- Sekretariatsfunksjon
- Utvikler veiledning
- Kompetanseheving og utadrettet virksomhet

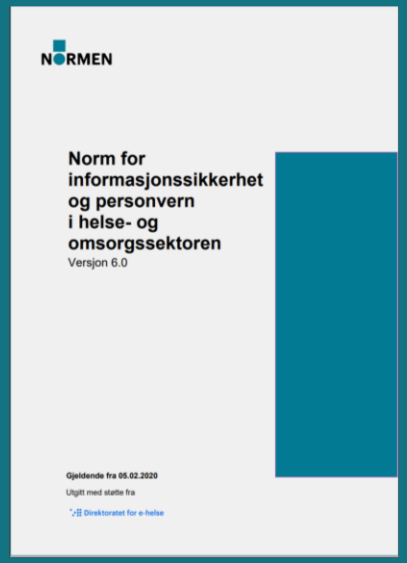
Fagorgan

- Utredninger
- Deltar i prosjekter og fora i/ for direktoratet
- Direktoratsfunksjon

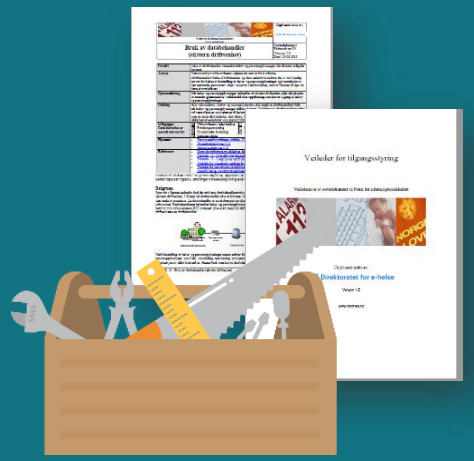
Avdeling informasjonssikkerhet

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren

Bransjenormen



Veiledning



Arena

Norges første og største bransjenorm for informasjonssikkerhet – og fra 2018 også for personvern

NORMEN

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren

Normen er til for..

.. **alle virksomheter** som ved **avtale** har forpliktet seg til å følge **Normen** – i praksis de fleste av sektorens mer enn titusen virksomheter og deres leverandører og databehandlere

Normen godkjennes og forvaltes av..

KS
DEN NORSKE LEGEFORENING
Apotekforeningen
Norges Farmaceutiske Forening
KiNS
Den norske tannlegeforening
folkehelseinstituttet
HELSE MIDT-NORGE
HELSE NORD
HELSE VEST
HELSE SØR-ØST
Direktoratet for e-helse
Helsedirektoratet
norskhelsenett
Den offentlige tannhelsetjeneste
nav
Digdir
FFO
IKT Norge
Melanor
NSM

.. en bredt sammensatt **styringsgruppe** fra sektoren

Normens daglige arbeid koordineres av..

Helsedirektoratet

norskhelsenett

.. et **sekretariat** plassert i Helsedirektoratet med fast representasjon fra Norsk Helsenett

NORMEN

Om Normen – selve bransjenormen

- En **bransjenorm** i 18 år!
- Ikke status som atferdsnorm etter reglene i forordningen
- Normen skal bidra til
  - «tilfredsstillende informasjonssikkerhet og personvern»
  - Egnede sikkerhetstiltak
  - Tillit mellom virksomheter
  - Godt personvern
- Normen er
  - Et kravsett
  - Et hjelpemiddel

- Forholdsmessighet og egne vurderinger

Styringsgruppen for Normen

MEDLEMMER

- Apotekforeningen
- Den norske legeforening
- Den norske tannlegeforening
- Norsk farmaceutisk forening
- Norsk fysioterapeutforbund
- Norsk psykologforening
- Norsk sykepleierforbund
- KS
- KiNS
- Helse Midt-Norge RHF
- Helse Nord RHF
- Helse Sør-Øst RHF
- Helse Vest RHF
- *Fûrst (Private helsevirksomheter)*
- Folkehelseinstituttet
- Direktoratet for e-helse
- Helsedirektoratet
- Norsk Helsenett

OBSERVATØRER

- Digitaliseringsdirektoratet
- NAV
- *NSM*
- *IKT Norge (Leverandørorganisasjoner)*
- *Melanor (Leverandørorganisasjoner)*
- *FFO – funksjonshemmedes fellesorganisasjon (Pasientorganisasjoner)*
- *Senior Norge (Pasientorganisasjoner)*
- *We Shall Overcome (Pasientorganisasjoner)*

NORMEN STRATEGI 2023-2025

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten –sektorens felles krav, verktøy og arena for informasjonssikkerhet og personvern

Normen skal

- styrke og forenkle arbeidet med informasjonssikkerhet og personvern
- bidra til at virksomheter som følger Normen har egnede tekniske og organisatoriske tiltak på plass
- fremme samhandling gjennom tillit i helse- og omsorgssektoren
- fremme en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet
- bidra til å understøtte gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og pasientens helsetjeneste

Overordnet strategi

Normen skal opprettholde og forbedre sin relevans og sektorens tillit, gjennom å ha

- relevante og oppdaterte krav
- målrettet og oppdatert veiledning av høy faglig kvalitet
- målrettede og nyttige kompetansehevingsaktiviteter

Helse- og omsorgssektorens behov skal alltid være førende for Normen.

NORMEN STRATEGI 2023-2025

STRATEGISKE FOKUSOMRÅDER OG INITIATIVER

1 Forenkling, nyttige verktøy og kompetanseheving

- Jobbe målrettet med kompetanseheving gjennom blant annet å se veiledningsmateriell og kompetanseheving i sammenheng
- Være tilgjengelig og i tett dialog og samarbeid med sektoren og andre relevante aktører
- Normens veiledningsmateriell skal holdes oppdatert
- Utvikle og forvalte nyttige verktøy på normen.no og ha gode informative nettsider
- Legge til rette for arenaer for erfaringsdeling, samarbeid og deling av maler og vurderinger

2 Prioriterte temaområder

- Tilpasset veiledning til sektorens små virksomheter
- Sette fokus på sikkerhetskultur gjennom alle Normens virkemidler
- IKT-beredskap og hendelseshåndtering
- Være premissleverandør og gi tilpasset veiledning på anskaffelser og leverandøroppfølging
- Legge til rette for og gi veiledning til å understøtte digital samhandling, bruk av ny teknologi og arbeidsformer
- Videreutvikle veiledningsmateriell på forskning
- Følge med på og tilpasse til kommende EU-regelverk, inkludert EHDS

3 Sektorens felles kravsett til informasjonssikkerhet og personvern

- Utvikle og forvalte gode verktøy for oppfølging av etterlevelse av Normen
- Bidra til at helse – og personopplysninger behandles slik at det understøtter pasientsikkerhet og forsvarlig pasientbehandling
- Tydeliggjøre og markedsføre hva Normen er
- Samarbeid, koordinering og kobling med andre veiledningsaktører, kontrollinstanser og krav/rammeverk

Handlingsplan Normen 2024

Normens krav	Lov om digital sikkerhet/ NIS 1
Veiledningsmateriell	FA Integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen FA 20 a,b,c (Sikkerhets- og samhandlingsarkitektur) Ny helseteknologi, f.eks. KI (må konkretiseres) Revisjon veileder MU og VFT Videreutvikle veiledning og verktøy om Normens krav i anskaffelser Fullføre kartlegging Små virksomheter og arbeide med tiltak avdekket i kartleggingen
Kompetanseheving, samarbeid og nettverk	Skrive fagartikler til www.normen.no Hold minst ett møte i PVO- og CISO-nettverk Vurdere om det skal etableres faste referansegrupper Holde kurs og webinar Evaluere Normkonferansen, veivalg videre

NORMEN

Normens innholdsfortegnelse

Andre aktiviteter i regi av Normen

Normkonferansen

Nyhetsbrev

- Ca. en gang i måneden
- Påmelding www.ehelse.no

Q&A epost

sikkerhetsnormen@ehelse.no

Kurs og webinar

- Kurs
- Webinarer
- Konferanser
- Foredrag

www.normen.no

- Alle dokumentene
- Nyheter
- Om Normen
- Påmelding til kurs og webinar

Sosiale medier

Følg oss på FB og LinkedIn!

NORMEN

Normens faktaark

Normens faktaark

- Målgrupper i faktaark (faktaark 0)
- Sikkerhetsrevisjon (faktaark 06)
- Bruk av databehandler (faktaark 10)
- Nødprosedyrer ved bortfall av IKT (faktaark 11)
- Tilbakerapportering av resultater fra IKT-driften (faktaark 12)
- Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)
- Tilgangsstyring (faktaark 14)
- Logging og innsyn i logg (faktaark 15)
- Fysisk sikring av områder og utstyr (faktaark 17)
- Sikring av bærbart utstyr (faktaark 18)
- Tiltak for å hindre skadelig programvare (faktaark 19)
- Sikkerhets- og samhandlingsarkitektur ved meldingsformidling (faktaark 20a)
- Sikkerhets- og samhandlingsarkitektur ved intern samhandling (faktaark 20b)
- Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter (faktaark 20c)
- Kommunikasjon over åpne nett (faktaark 24)

Normens faktaark (forts.)

- Lagringstid og sletting (faktaark 25)
- Hjemmekontor og annet fjernarbeid (faktaark 29)
- Sikring av mobilt utstyr utenfor virksomheten (faktaark 30)
- Passord og passordhåndtering (faktaark 31)
- Håndtering av lagringsmedia (faktaark 34)
- Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter (faktaark 37)
- Testing og testdata (faktaark 43)
- Tjenesteutsetting av kommunale helse- og omsorgstjenester (faktaark 46)
- Krav ved bruk av PKI ved ekstern kommunikasjon (faktaark 49)
- Tiltak ved konvertering og bytte av EPJ (faktaark 53)
- Videokonsultasjon (faktaark 54)
- Sperret adresse i Folkeregisteret (faktaark 55)
- Formål og behandlingsgrunnlag (faktaark 56)
- Personvernprinsippene (faktaark 57)

Normens veiledere

Normens veiledere

- Veileder for fjernaksess
- Veileder for personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter
- Veileder for små virksomheter
- Veileder om internkontroll for informasjonssikkerhet og personvern
- Veileder om risikostyring i informasjonssikkerhet og personvern
- Veileder i personvern og informasjonssikkerhet - medisinsk utstyr
- Veileder i digital pasientkommunikasjon
- Veileder i personvern og informasjonssikkerhet ved bruk av velferdsteknologi
- Veileder med avtaleeksempler ved samarbeid om felles journal
- Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger
- Veileder video-, lyd og bildeopptak i helse- og omsorgssektoren
- Veileder i bruk av skytjenester til behandling av helse- og personopplysninger
- Veileder om de registrertes rettigheter
- Veileder om informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

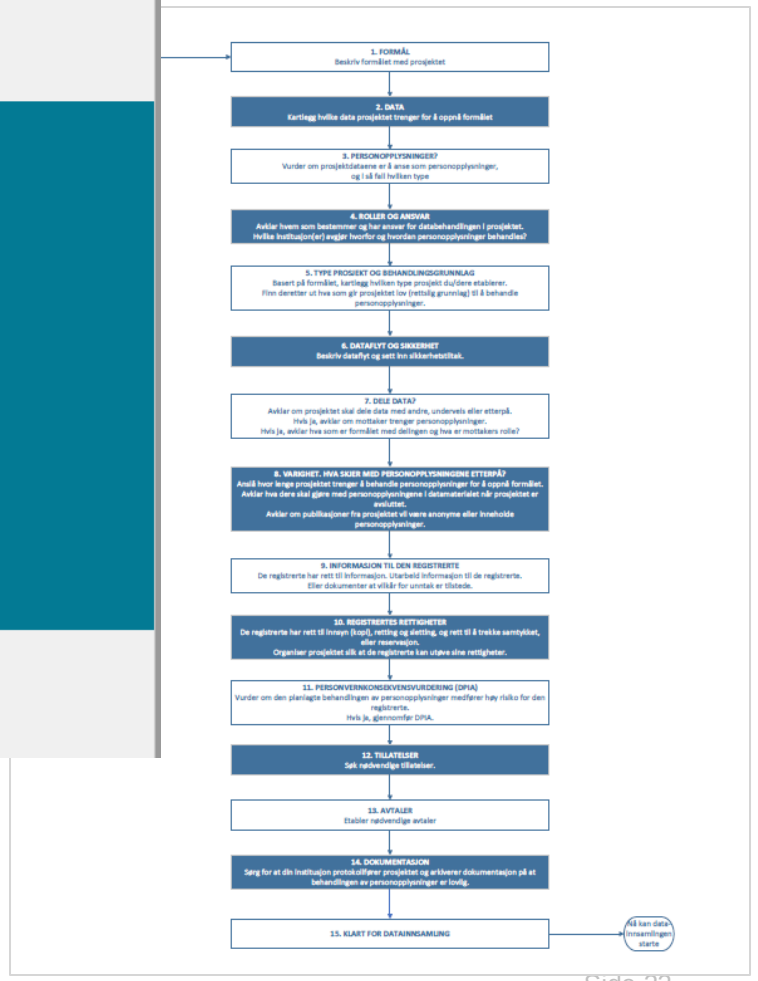
Veileder for fjernaksess mellom virksomhet og leverandør

- Veilederens målgruppe er både virksomheten (databehandlingsansvarlig) og leverandøren.
- Bakgrunnen for veilederen er at:
- Leverandører til helse- og omsorgssektoren forventer fjernaksess for å kunne utføre vedlikehold og oppdatering av leveranser. Det eksisterer ingen gjeldende standard for sikker fjernaksess – så derfor er Normen og veilederen et nyttig grunnlag.
- Det kan være usikkerhet rundt krav til sikkerhet i de eksisterende løsningene for fjernaksess. Ved bruk av Normen og veilederen vil det forhåpentligvis bli tydeligere hvilke tiltak som er nødvendige for å oppnå sikre løsninger.

- Vedlegget har et sett med nyttige sjekklister basert på veilederen.

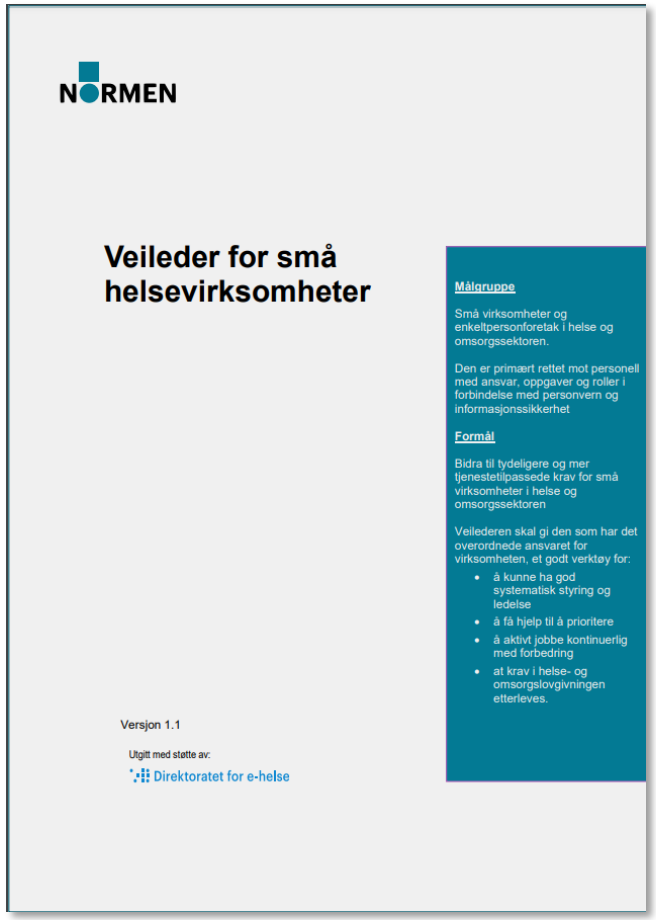
Veileder for personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter

- Veilederen tar for seg all forskning på helse- og personopplysninger, og er ikke begrenset til helseforskningslovens virkeområde.
- Hovedmålgruppen er prosjektledere i forskningsprosjekter, men kan også være nyttig for forskere uten prosjektansvar, forskningssykepleiere, forskerstøttefunksjoner, personvernombud, ledelsen i forskningsinstitusjoner og lignende.
- Veilederen er praktisk innrettet og følger kronologien i et forskningsprosjekt, fordelt på planleggings- gjennomføring- og avslutningsfase.
- Avgrenser mot spørsmål om etikk og etiske spørsmål i forskning.



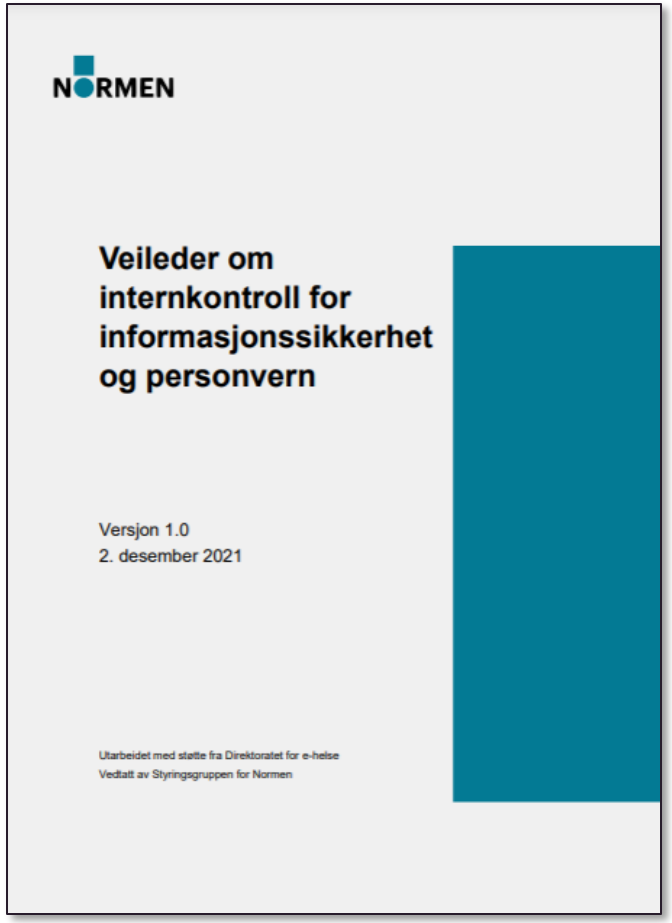
Veileder for små helsevirksomheter

- Formålet med veilederen er å bidra til tydeligere og mer tjenestetilpassede krav for små virksomheter i helse og omsorgssektoren.
- 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.
- Inneholder praktiske eksempler.
- Veilederen samler de viktigste dokumentasjonskravene i en sjekkliste.



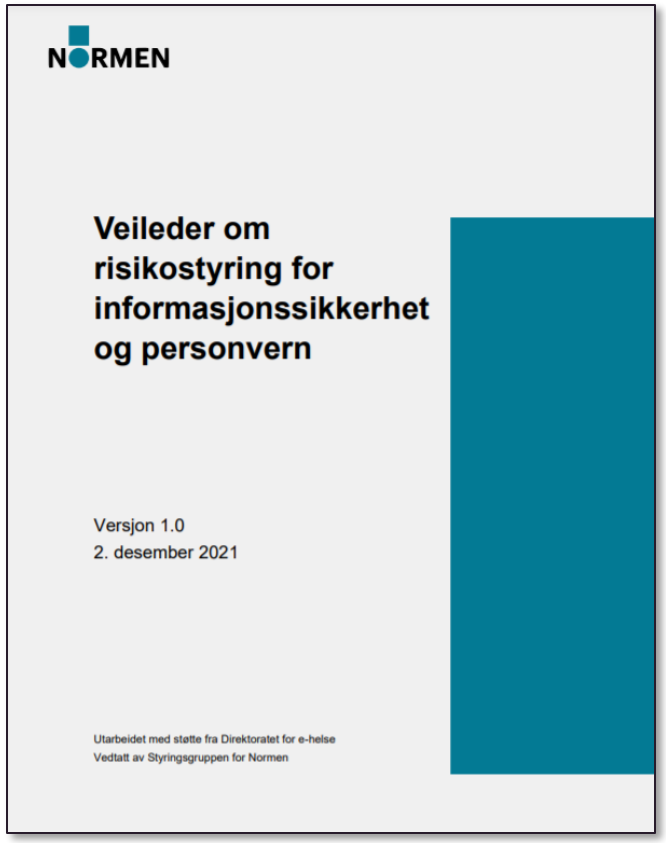
Veileder om internkontroll for informasjonssikkerhet og personvern

- 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.



Veileder om risikostyring for informasjonssikkerhet og personvern

- Veilederen skal gi veiledning til, og bidra til etterlevelse av, kravene i Normen knyttet til risikostyring.
- Nyttig for alle ledere og medarbeidere i sektoren. Ledere er en særlig viktig målgruppe. Også nyttig for systemleverandører og andre samarbeidspartnere til sektoren.
- Veilederen er avgrenset til risikostyring innenfor Normens temaområder i helse- og omsorgssektoren.
- Inneholder praktiske eksempler og eksempel på risikometodikk.



Personvern og informasjonssikkerhet – medisinsk utstyr

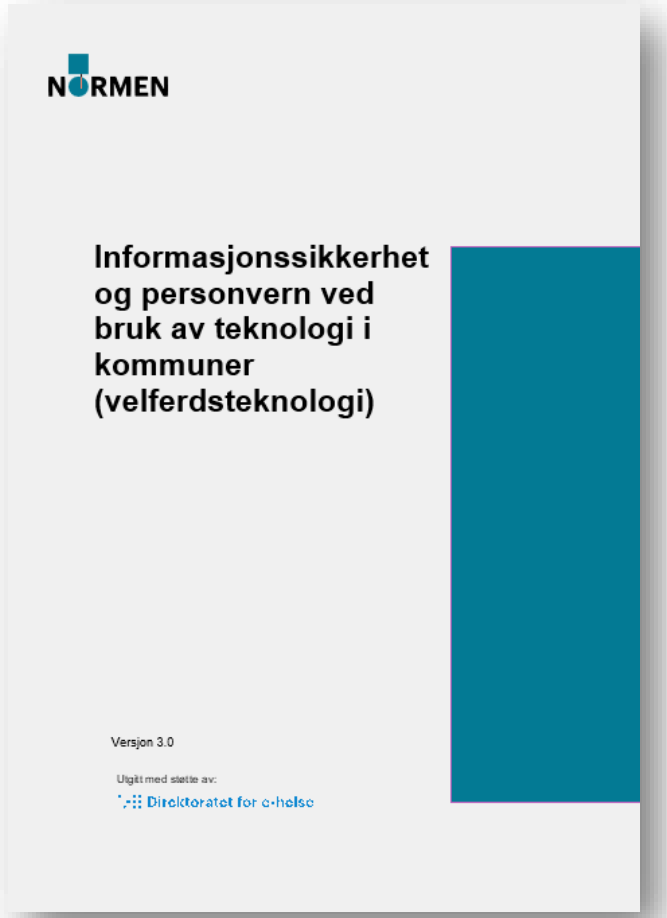
- Veilederen skal bidra til å skape felles forståelse for krav og tilnærming til informasjonssikkerhet hos
  - Virksomheter som benytter MU
  - Databehandlere
  - Leverandører av medisinsk utstyr
- To hovedtemaer i veilederen:
  - Hvordan sikre at behandling av helse- og personopplysninger i tilknytning til medisinsk utstyr skjer i tråd med lovverket
  - Hvordan medisinsk utstyr kan beskyttes mot angrep på digital infrastruktur

Veileder i digital pasientkommunikasjon

- Hensikten med veilederen er å:
  - Bidra til at digital pasientkommunikasjon skjer i samsvar med gjeldende krav til personvern og informasjonssikkerhet
  - Være et praktisk hjelpemiddel når virksomhetene skal kommunisere digitalt med pasient, og være til hjelp i vurderingen når man skal velge og bruke et kommunikasjonsmiddel.
- Målgruppen er helsepersonell og andre i sektoren som trenger å kjenne til hvordan man på en sikker og lovlig måte kan kommunisere digitalt med pasienter.
- Inneholder et eget kapittel om bruk av sosiale medier.

Informasjonssikkerhet og personvern ved bruk av teknologi i kommuner (velferdsteknologi)

- Veilederen inneholder utvalgte juridiske temaer som behandlingsgrunnlag, med et dypdykk i bruk av samtykke, journalføring, og bruk av data til forskning og kvalitetssikring.
- Veilederen er ikke uttømmende om temaer innen velferdsteknologi. Veilederen omfatter i noen grad helselovgivningens alminnelige regler for behandling av helse- og personopplysninger.
- Temaer som taushetsplikt, dokumentasjonsplikt, kommunikasjon av opplysninger og pasient- og brukerrettigheter dekkes ikke av denne veilederen.



NORMEN

Veileder med avtaleeksempler ved samarbeid om felles journal

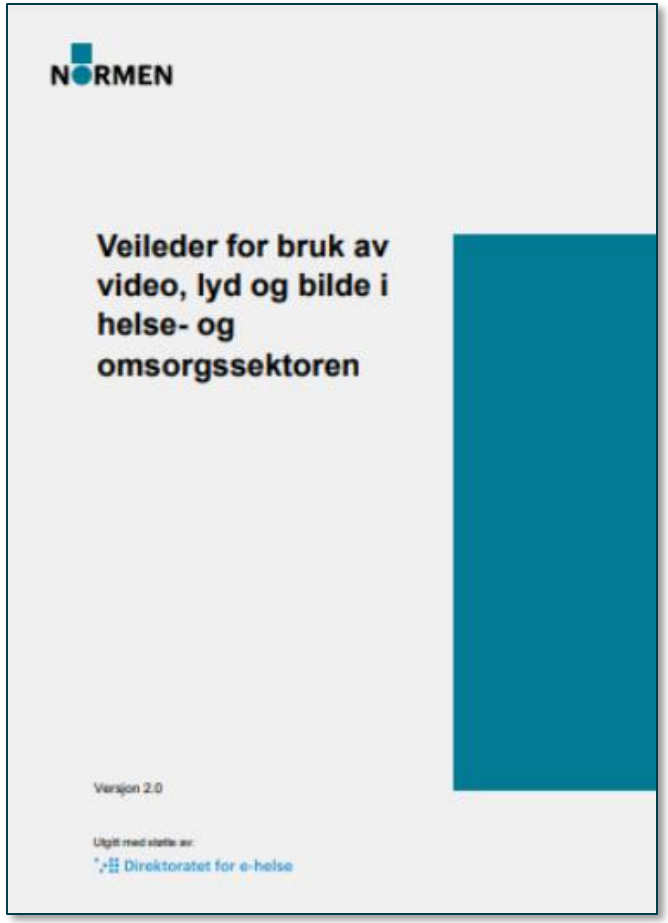
- Veilederen omhandler etterlevelse av kravene i Normen ved etablering av felles journal.
- Veilederen gir hjelp til å bl.a.:
  - Definere ansvar og fastsette oppgaver
  - Fastsette prinsipper for felles journal
  - Foreslå avtaletekster for ulike typer samarbeid om felles journal
- Veilederen gir ikke anvisning på hvordan virksomhetene inngår avtaler om samarbeidet, men vilkårene for etablering av felles journal innenfor samarbeidskonstellasjonene. Det gis også eksempler på hvordan dette kan avtalereguleres.

Veileder for tilgang til helse- og personopplysninger

- Veilederen skal gi veiledning til og bidra til etterlevelse av kravene Normen stiller til etablering av tilfredsstillende tilgangsstyring innad i virksomheten.
- Gjelder tilgangsstyring i behandlingsrettede helseregistre for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte pasient.
- Veilederen omtaler hovedsakelig temaene autorisering, autentisering og kontroll av tilgang til helse- og personopplysninger, men gir også en overordnet innføring i generelle prinsipper for tilgangsstyring.

Veileder for bruk av video, lyd og bilde i helse- og omsorgssektoren

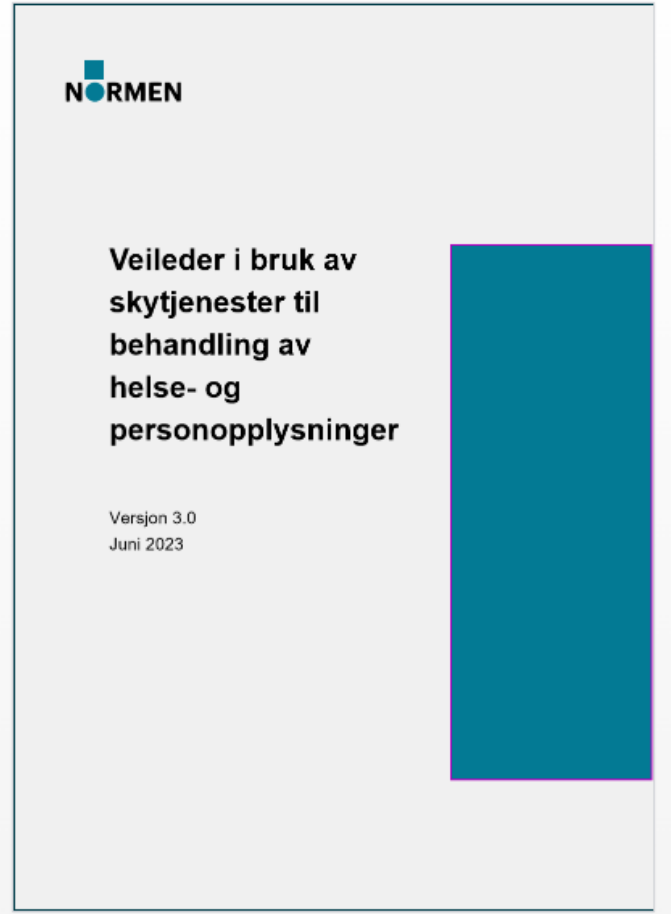
- Hensikten med veilederen er å:
  - Bidra til at bruk av video, lyd og bilde skjer i samsvar med gjeldende krav til personvern og informasjonssikkerhet
  - Være et praktisk hjelpemiddel når virksomhetene benytter video, lyd og bilde
- Målgruppen er helsepersonell og andre i sektoren som trenger å kjenne til hvordan man på en sikker og lovlig måte kan benytte video, lyd og bilde i forbindelse med
  - ytelse av helsehjelp
  - veiledning og opplæring
  - kvalitetssikring



Veileder for bruk av skytjenester

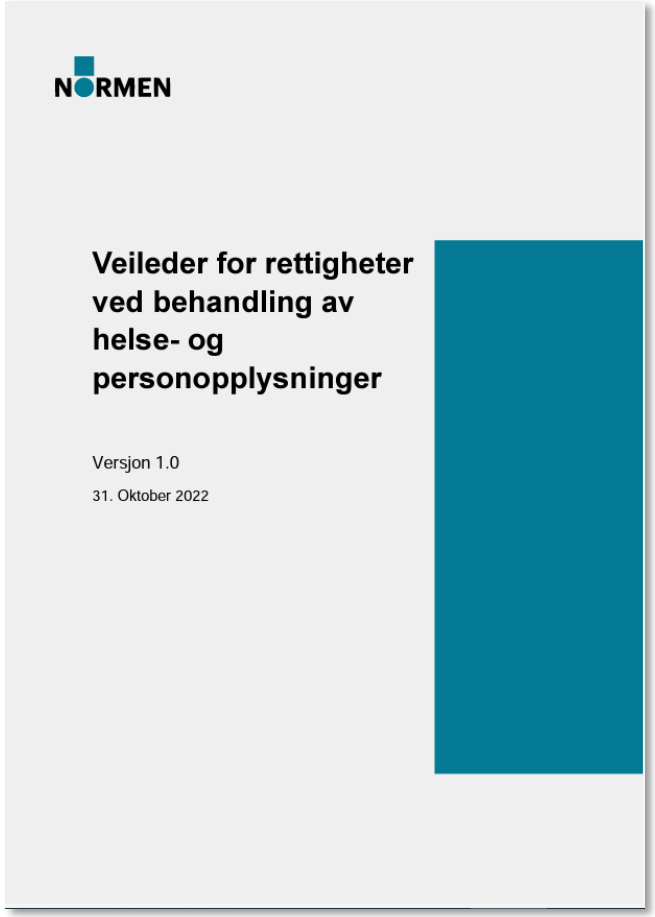
Veilederen gir praktisk hjelp innenfor områdene

- 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



Veileder for rettigheter ved behandling av helse og personopplysninger

- Gir veiledning i hvordan de registrertes rettigheter kan ivaretas, herunder pasienters rettigheter som registrerte. Avgrenser seg til pasienters rettigheter som registrerte.
- Veilederen tar utgangspunkt i kravene som følger av personopplysningsloven, personvernforordningen, helsepersonelloven, pasientjournalloven, helseregisterloven, pasient og brukerrettighetsloven, helseforskningsloven og pasientjournalforskriften.
- Veilederen omhandler først og fremst behandling av personopplysninger i forbindelse med at det ytes helsehjelp. Rettigheter ansatte har som registrerte omtales noe.



Veileder informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

Helsesektoren trenger ikke være en enkel sektor å være leverandør til, det er strenge krav til Informasjonssikkerhet og personvern.

Som leverandør kan det være vanskelig å forså kravene og hva som må til av tiltak for at Informasjonssikkerhet og personvern blir ivaretatt på en god og sikker måte. Denne veilederen er skrevet ut fra hva som er krav og forventninger til leverandører til sektoren. Den inneholder også en guide for hvordan innføre teknologi i sektoren, samt et forslag til en ansvarsmatrise (HUKI).

Veilederen kan med fordel også brukes av de som anskaffer teknologi til sektoren.