Om Normen

Kurset «Intro til Normen»

Hovedtema for kurset «Intro til Normen»

Personvern

Informasjonssikkerhet

- **K**onfidensialitet
- **I**ntegritet
- **T**ilgjengelighet

Normen

Siw
Tynes Johnsen

Thea
Rølsåsen

Aasta
Hetland
(Sekretariatsleder)

Jan Gunnar
Broch
(Seksjonsleder)

Knut Herje

Susanne Helland Flatøy

Marie Strand Schildmann

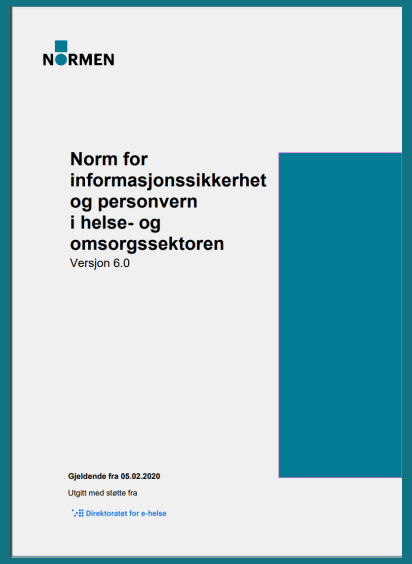
Sekretariatet for Normen

Avdeling juss og informasjonssikkerhet

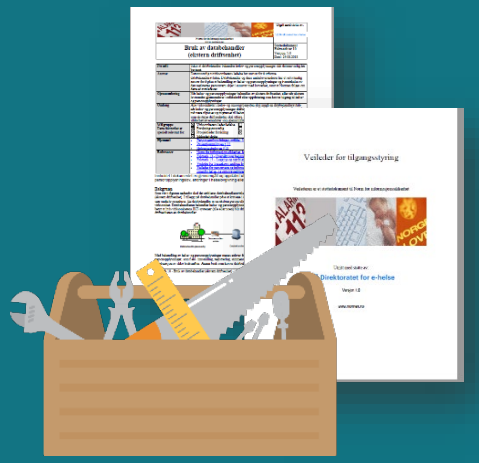
NORMEN

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..

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

Normens daglige arbeid koordineres av..

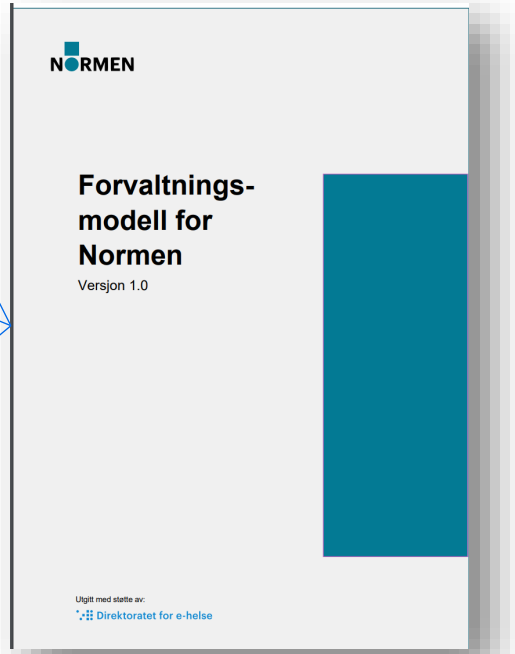
.. et **sekretariat** plassert i Direktoratet for e-helse med fast representasjon fra Norsk Helsenett

Nytt mandat og forvaltningsmodell

Hvordan styres Normen?

Hva er «Normens produkter»?

Hvordan utvikles og vedlikeholdes «produktene»

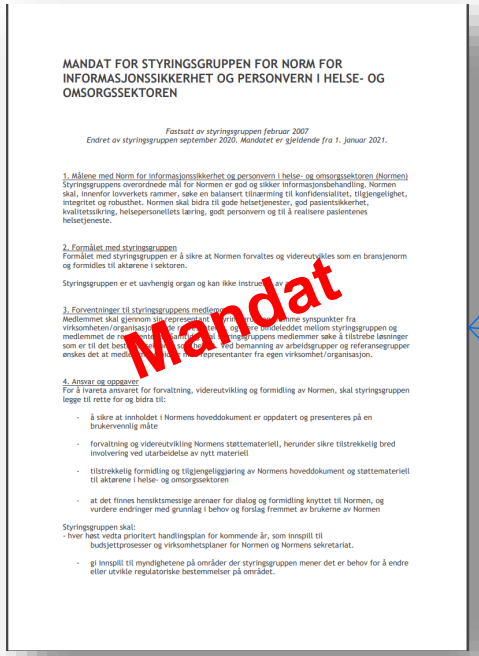

NORMEN

Forvaltnings-modell for Normen

Versjon 1.0

Utgitt med støtte av:

Direktoratet for e-helse


MANDAT FOR STYRINGSGRUPPEN FOR NORM FOR INFORMASJONSSIKKERHET OG PERSONVERN I HELSE- OG OMSORGSSEKTOREN

Fastsatt av styringsgruppen februar 2007
Endret av styringsgruppen september 2020. Mandatet er gjeldende fra 1. januar 2021.

1. Målene med Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)
Styringsgruppens overordnede mål for Normen er god og sikker informasjonsbehandling. Normen skal, innenfor lovverkets rammer, søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet. Normen skal bidra til gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og til å realisere pasientenes helsetjeneste.

2. Formålet med styringsgruppen
Formålet med styringsgruppen er å sikre at Normen forvaltes og videreutvikles som en bransjenorm og formidles til aktørene i sektoren.

Styringsgruppen er et uavhengig organ og kan ikke instrueres av

3. Forventninger til styringsgruppens medlem
Medlemmet skal gjennom sin representant

virksomheten/organisasjon

medlemmet de re

som er til det beste

ønskes det at medl

Mandat

4. Ansvar og oppgaver
For å ivareta ansvaret for forvaltning, videreutvikling og formidling av Normen, skal styringsgruppen legge til rette for og bidra til:

- å sikre at innholdet i Normens hoveddokument er oppdatert og presenteres på en brukervennlig måte
- forvaltning og videreutvikling Normens støttemateriell, herunder sikre tilstrekkelig bred involvering ved utarbeidelse av nytt materiell
- tilstrekkelig formidling og tilgjengeliggjøring av Normens hoveddokument og støttemateriell til aktørene i helse- og omsorgssektoren
- at det finnes hensiktsmessige arenaer for dialog og formidling knyttet til Normen, og vurdere endringer med grunnlag i behov og forslag fremmet av brukerne av Normen

Styringsgruppen skal:
- hver høst vedta prioritert handlingsplan for kommende år, som innspill til budsjettprosesser og virksomhetsplaner for Normen og Normens sekretariat.
- gi innspill til myndighetene på områder der styringsgruppen mener det er behov for å endre eller utvikle regulatoriske bestemmelser på området.

Agenda og referater fra styringsgruppens møter skal offentliggjøres

Nestleder

Ny sammensetning av styringsgruppen

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)*
- *Kreftforeningen (Pasientorganisasjoner)*

Om Normen – selve bransjenormen

- En **bransjenorm** i 16 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
- Normens krav til lovverket

Kap 1 Om Normen

- Normen skal **bidra** til **tilfredsstillende informasjonssikkerhet og personvern** hos den enkelte virksomhet, i felles systemer og infrastruktur, og i sektoren generelt. Normen skal **bidra til å sikre** at en virksomhet som etterlever og innretter seg etter Normen har **egnede tekniske og organisatoriske tiltak** for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

- Videre skal Normen bidra til at virksomhetene kan ha **gjensidig tillit** til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. De som samhandler med en virksomhet som har forpliktet seg til å innrette seg etter Normens krav, skal **kunne stole på** at denne virksomheten har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

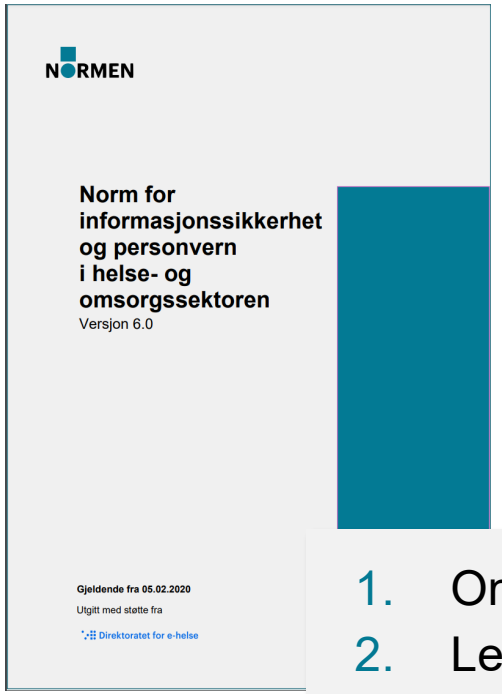
- Normen skal bidra til at pasienter, brukere, ansatte og andre registrerte sikres et **godt personvern**.

- Normen er **et hjelpemiddel** i den enkelte virksomhets arbeid med informasjonssikkerhet og personvern.

- Normen skal bidra til å understøtte gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og pasientens helsetjeneste.

Noen av de viktigste innholdsendringene i Normen v6.0

- Forenkling av både krav og språk
- Rendyrket Normen som kravdokument
  - Som i prinsippet alle typer virksomheter kan velge å følge, eller bli forpliktet til å følge gjennom avtale
- Tilpasninger til personvernforordningen
- Kap 5 Informasjonssikkerhet
  - De fleste sikkerhetskravene gjelder også for behandling av helse- og personopplysninger med **andre formål enn ytelse av helse- og omsorgstjenester**. (Virksomheten må vurdere)
  - NSMs Grunnprinsipper for IKT-sikkerhet
  - Leverandørkapittelet omstrukturert + sky



1. Om Normen
2. Ledelse og ansvar
3. Risikostyring
4. **Grunnleggende om behandling av helse- og personopplysninger**
5. Informasjonssikkerhet
6. Vedlegg

Vedlegg til Normen «Oversikt over Normens krav»

- Alle Normens «skal»-krav
- ISO-mapping (begge veier), lovhjemler, systemkrav, kan ivaretas av databehandler, egenvurdering mm.
- Erstatter faktaark 6b og 38

Nr	Krav (formulert som spørsmål)	Kap. i Normen	Kap. i ISO 27001 og Annex A	Systemkrav i behandlings-rettet helse-register	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivaretatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivaretatt av data-behandler
1.	Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv?	1.5	6.1.1 8.1			☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21 FLK § 6	
2.	Er valgte tiltak basert på risikovurderinger?	1.5	6.1.3 8.3			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐Ja ☐Nei
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	1.5	6.1* 8.1.*			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	

Andre aktiviteter i regi av Normen

Normkonferansen

24. November
Digital konferanse

Nyhetsbrev

- Ca 4 ganger årlig
- Påmelding www.ehelse.no

Q&A epost

sikkerhetsnormen@ehelse.no

Kurs og webinar

- Ukentlige webinarer
- Kurs
- Konferanser
- Foredrag

www.normen.no

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

Sosiale medier

Følg oss på FB og LinkedIn!

NORMEN

Tema	Klokkeslett
Intro om kurset	09:00
Om Normen	09:15
Spørsmål	*09:35*
Pause	09:45
Risikovurdering/ styring	10:00
Pause	10:45
Internkontroll	10.55
Utvalgt temaer om personvern	11:25
Spørsmål	11:45
Lunsj	12.00
Utvalg av Normens krav til informasjonssikkerhet, kap. 5	12:45
Spørsmål	13:30
Pause	13:45
Normens krav i anskaffelser	14:00
Normens handlingsplan 2021 og veiledningsmateriell	14:30
Spørsmål	14:50
Takk for i dag	15:00