Webinar: Normens velferdsteknologiveileder

14.10.20

Petter Ludvig Andersen
Sekretariatet for Normen

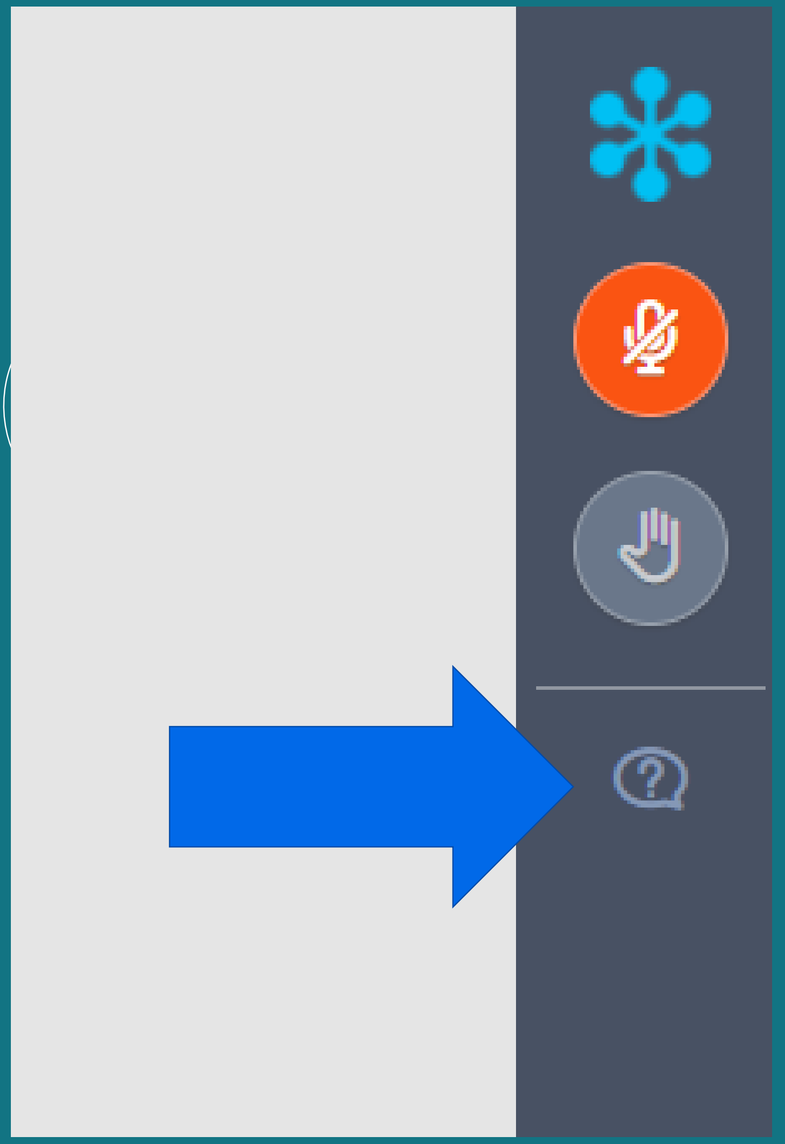
Kjøreregler

- Møteleder styrer ordet
- Deltagernes mikrofoner er mutet som standardinnstilling
- Det foretas ikke opptak av dette webinaret
- Deaktiver fullskjermsmodus dersom du har problemer med å svare på poll
- Presentasjonene legges ut på kurssiden på normen.no

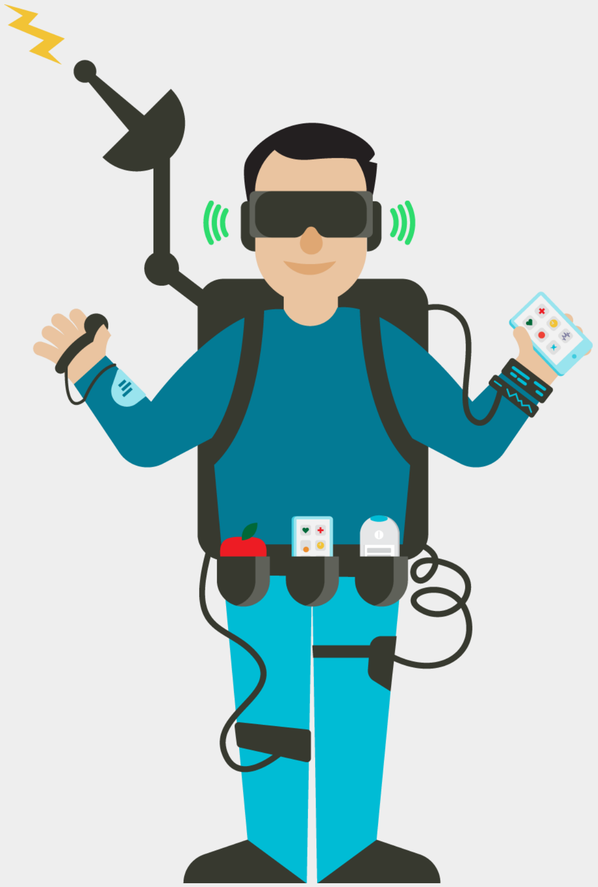
- Vil du vite mer om hvordan vi jobber med GoToWebinar? Se mer på https://ehelse.no/normen/aktuelt-om-normen/digital-kompetanseheving-med-normen

Spørsmål underveis

- Bruk spørsmålsfunksjonen når som helst under foredragene
- Vi samler opp spørsmål og besvarer spørsmålene til slutt
- Vi besvarer spørsmålene som stilles underveis i chat
- Vi lagrer spørsmålet ditt, men ikke hvem det kommer fra.
- Hvis du har spørsmål som ikke blir besvart under kurset, send oss en epost til sikkerhetsnormen@ehelse.no



POLL



NORMEN

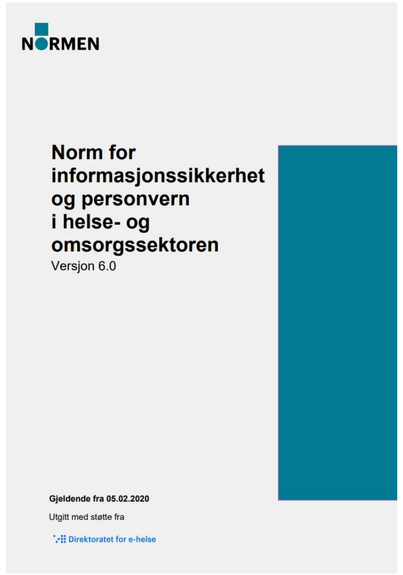
Informasjonssikkerhet og personvern ved bruk av teknologi i kommuner (velferdsteknologi)

Versjon 3.0

Utgitt med støtte av:

Direktoratet for e-helse

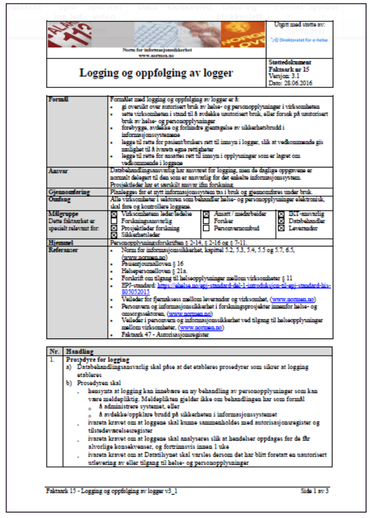
Norm for informasjonssikkerhet

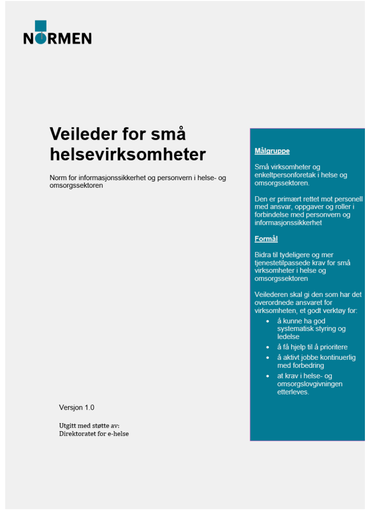


Bindende gjennom medlemsskapet i helsenettet

Veiledere
Faktaark

Ikke bindende





NORMEN

Versjon 3.0

- Versjon 3.0 er endelig publisert!

- Basert på flere behovskartlegginger i kommunene
- Innholdet baserer seg i stor grad på det som er meldt inn av veiledningsbehov

- Ikke uttømmende veiledning om personvern, informasjonssikkerhet og helselovgivning

INNHOLD

Behandlingsgrunnlag

- Helse- og personopplysninger kan bare behandles når lovgivningen tillater det.
- Skal dekke alle typer behandlinger av helse- og personopplysninger
  - Innsamling
  - Lagring
  - Sletting
  - Utlevering
  - +++

Samtykke

Helsehjelp

Behandling av helse- og personopplysninger

NORMEN

Hovedregel om samtykke i helse- og omsorgstjenesten

Årsaken er

- at samtykke til helse- og omsorgstjenester – enten den gis med eller uten bruk av teknologi - kan gis implisitt (det er det vanlige)
- at helselovgivningen i seg selv gir rettsgrunnlag for behandling av de opplysningene som er relevant og nødvendig for ytelse av tjenestene

Kun nødvendig med uttrykkelig samtykke

- hvis opplysninger skal behandles for andre formål enn ytelse av helse- og omsorgstjenester til den det gjelder (unntatt intern kvalitetssikring), og det ikke finnes annen hjemmel eller behandlingsgrunnlag
- hvis det skal behandles andre opplysninger enn de som er relevante og nødvendige for å yte tjenester til pasienten/brukeren, og det ikke finnes annen hjemmel eller behandlingsgrunnlag

NORMEN

POLL

Normland kommune skal implementere ny elektronisk medisineringsstøtte.
De lurer på om de trenger samtykke fra tjenestemottakeren?
Kommunen lurer på om hva samtykket skal gjelde?
De vet at å gi medisiner er en del av helsehjelpen, og at rettsgrunnlaget da er implisitt samtykke til å yte helsehjelp.
Men trenger de samtykke til å behandle personopplysninger i tillegg?

Velferdsteknologi som medisinsk utstyr

- Det finnes flere tilfeller hvor velferdsteknologi er klassifisert som medisinsk utstyr. For eksempel kan elektronisk medisineringsstøtte, blodsukkerapparater, blodtrykksmålere, pulsmålere og aktivetsmåler klassifiseres som medisinsk utstyr.

- Når det behandles helse- og personopplysninger i det medisinske utstyret vil personvernforordningen gjelde på samme måte som ved all annen behandling av helse- og personopplysninger = kommunens ansvar

- I forordning om medisinsk utstyr følger det en rekke krav til produsenten skal etterleve.
- Kommunen er selv ansvarlig for å anskaffe medisinsk utstyr som er i samsvar med kravene som stilles produsentene og som er egnet for det tiltenkte brukerområdet.

Kommunens ansvar

- Kommunens øverste ledelse har ansvar for å sørge for at kommunen følger gjeldende krav til informasjonssikkerhet og personvern ved ytelse av helse- og omsorgstjenester

- **Ikke glem velferdsteknologien i dette arbeidet!**

Kommunens ledelse skal sørge for at

- det føres oversikt over behandlinger av helse- og personopplysninger[6]
- det finnes rutiner for å oppfylle de registrertes rettigheter
- medarbeidere gis opplæring og har tilstrekkelig kompetanse[7]
- kommunen har et styringssystem for informasjonssikkerhet(ISMS)[8]
- avvik behandles og håndteres[9]
- kommunen ivaretar sitt behandlingsansvar for ytelse av helsehjelp
- gjennomføre ROS-vurderinger[10] og personvernkonsekvensvurdering[11]
- etablere og dokumentere tekniske og organisatoriske tiltak
- inngå og følge opp avtaler

NORMEN

Sentrale prosesser: Anskaffelse

- Viktig å involvere de riktige ressursene innenfor personvern og informasjonssikkerhet,
- Personvernombud, juristkompetanse, IKT og sikkerhet, samarbeid med fylkesmannen og å bruke eksisterende nettverk som f.eks andre kommuner i regionen eller Nasjonalt velferdsteknologiprogram.

Tabellen nedenfor er et forslag til noen punkter i en sjekkliste i anskaffelsesfasen:

1.	Sikre at relevante roller er med i anskaffelsen (f.eks. personvernombud, juridisk, IT, informasjonssikkerhet, helsefag osv.)	☐ Ja ☐ Nei
2.	Gjennomfør forberedende dialog med leverandør	☐ Ja ☐ Nei
3.	Framskaff underlag ifm. krav til personvern og informasjonssikkerhet	☐ Ja ☐ Nei
4.	Ved kjøp av utstyr eller tjeneste bør kommunen utarbeide kravspesifikasjon med utgangspunkt i Normens krav	☐ Ja ☐ Nei
5.	Still krav til innebygd personvern i produkter og løsninger som anskaffes	☐ Ja ☐ Nei
6.	Gjennomfør risikovurdering og personvernkonsekvensvurdering av tjenesten/ teknologien	☐ Ja ☐ Nei
7.	Etabler databehandleravtale dersom leverandør skal behandle helse- og personopplysninger på vegne av kommunen	☐ Ja ☐ Nei
8.	Fastsette formål med behandlingen og behandlingsgrunnlag	☐ Ja ☐ Nei

Vedlegg til Normens krav

NORMEN Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: Direktoratet for e-helse
Vedlegg – Samlet oversikt Normens krav	**Vedlegg** Versjon: 1.0 Dato: 5. februar 2020

Forside > Normen > Oversikt over Normens krav, og mapping mellom ISO og Normen

Oversikt over Normens krav, og mapping mellom ISO og Normen

Her kan du også laste ned vedlegget "Oversikt over Normens krav" (Word)

CSA har mappet CCM opp mot Normens krav (PDF)

I tillegg til mappingen av Normens krav til ISO som finnes i vedlegget "Oversikt over Normens krav" over, er det også gjort en mapping av ISO27001 til Normens krav (Excel)

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

Sentrale prosesser: utprøving, implementering og drift

- Når kommunen har valgt teknologi er det viktig å ha gode rutiner for implementering og drift av teknologien
- De samme kravene som følger av lov og av Normen gjelder uansett om det er utprøving eller drift. Det er ikke mulig å lempe på tiltakene selv om det er under utprøving av velferdsteknologi.
- Når det behandles helse- og personopplysninger i utprøvingen skal alle tiltak gjennomføres som om det er normal drift.

Tabellen nedenfor er et forslag til noen punkter på en sjekkliste for implementering og drift:

1.	Sikre at relevante roller er med i anskaffelsen (f.eks. personvernombud, juridisk, IT, informasjonssikkerhet, helsefag osv.)	☐ Ja ☐ Nei
2.	Plasser ansvar og etabler roller	☐ Ja ☐ Nei
3.	Oppdater styringssystemet for informasjonssikkerhet	☐ Ja ☐ Nei
4.	Oppdater oversikten over behandling av personopplysninger (protokoll)	☐ Ja ☐ Nei
5.	Gi informasjon om helse- og omsorgshjelpen som tilbys, teknologien som benyttes og behandlingen av helse- og personopplysninger som vil starte	☐ Ja ☐ Nei
6.	Gi opplæring til pasient/brukere, pårørende og helsepersonell	
7.	Etabler / vedlikehold tilgangsstyring	☐ Ja ☐ Nei
8.	Avklar lagringstid for opplysningene og kontinuerlig vurder hva som skal slettes	☐ Ja ☐ Nei
9.	Gjennomfør logging	☐ Ja ☐ Nei
10.	Sikre datakommunikasjon	☐ Ja ☐ Nei
11.	Oppdater konfigurasjonsoversikt ved endringer	☐ Ja ☐ Nei
12.	Gjennomfør avviksbehandling dersom avvik oppstår	☐ Ja ☐ Nei
13.	Rydd opp ifm. avvikling hos bruker	☐ Ja ☐ Nei
14.	Oppdater risikovurdering ved vesentlige endringer, avvik og endringer i risikobilde	☐ Ja ☐ Nei
15.	Etabler rutine for oppfølging av leverandør (revisjon, avtaler mv)	☐ Ja ☐ Nei
16.	Etablere rutine for oversikt og vedlikehold av eventuelle samtykker	☐ Ja ☐ Nei

Risikovurdering

- **All behandling av helse – og personopplysninger skal risikovurderes. Dette inkluderer også når dette skjer med bruk av velferdsteknologi**
- Det er risikovurderingen som ligger til grunn for alle de videre vurderingene og beslutningene; blant annet om man vil ta i bruk en velferdsteknologisk løsning, for hvordan behandlingen av opplysningene skal foregå og hvilke tiltak som settes i verk

- Eksempler på områder som kan inngå i risikovurderingen av velferdsteknologi:

Tilgjengelighet

- **Ødeleggende programvare (f.eks. om løsningen er tilknyttet Internett)**

Integritet

- **Uautorisert endring av helse- og personopplysninger og konfigurasjon ved tilgang fra eksterne nett (f.eks. Internett, trådløse nett og mobilnett)**

Konfidensialitet

- **Tilgangsstyring hos bruker (f.eks. nettbrettet, rapporteringsløsninger, dørlåser, mv.)**
- **Leverandørs løsning for fjernaksess**

- Personvernkonsekvensvurdering – Personvernforordningen (GDPR)

Personvernkonsekvensvurdering (DPIA)

- **Virksomheten skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte**
- Dokumenter lovligheten av behandlingen, formål, hvordan personvernet til den registrerte blir ivaretatt, og tilstrekkelige tiltak for å håndtere risikoen.

- **Systematisk monitorering: digitalt tilsyn, GPS klokker og annen sporingsteknologi.**
- **Når helseopplysninger behandles i stor skala**
- **Ny teknologi**
- **Barn og andre sårbare grupper**

Kan være aktuelt å vurdere:

- **Omfang av personopplysninger**
- **Personopplysningens art (hvem opplysningene gjelder, sensitivitet)**
- **Kategorier av mottakere (deling, utlevering, innsyn, mv.)**
- **Kategorier av behandlinger (innsamling, sammenstilling og lagring)**

- Løsninger som i utgangspunktet ikke vil være høy risiko for den registrertes rettigheter og friheter:
  - Teknologi som ikke behandler helse- og personopplysninger
  - Forbrukerteknologi som pasienten/ brukeren selv tar i bruk
  - Teknologi som ikke kobles til nettverk
  - Stille sykesignalanlegg

NORMEN

POLL

POLL

Eksempel – elektronisk medisineringsstøtte

Normland kommune skal implementere elektronisk medisineringsstøtte. Medisindispenseren plasseres hjemme hos brukerne hvor et fjernpleiesystem gjør det mulig for ansatte å sjekke om pasienten/brukeren har tatt medisinene som de skal. Normland ønsker å forbedre pasientsikkerheten ved at pasienten/brukeren får rett medisin til rett tid og håper at medisinavvikene går ned.

Normland kommune gjør flere vurderinger (bl.a. risikovurdering, helsefaglige vurderinger) for å sikre at løsningen ivaretar krav til informasjonssikkerhet og personvern. De vurderer konsekvensene for personvernet til pasienten/ brukeren, om de har behandlingsgrunnlag og et klart formål og om det er nødvendig og gjennomføre en DPIA etter personvernforordningen artikkel 35. Kommunen gjennomfører den overordnende vurderingen. De vurderer at:

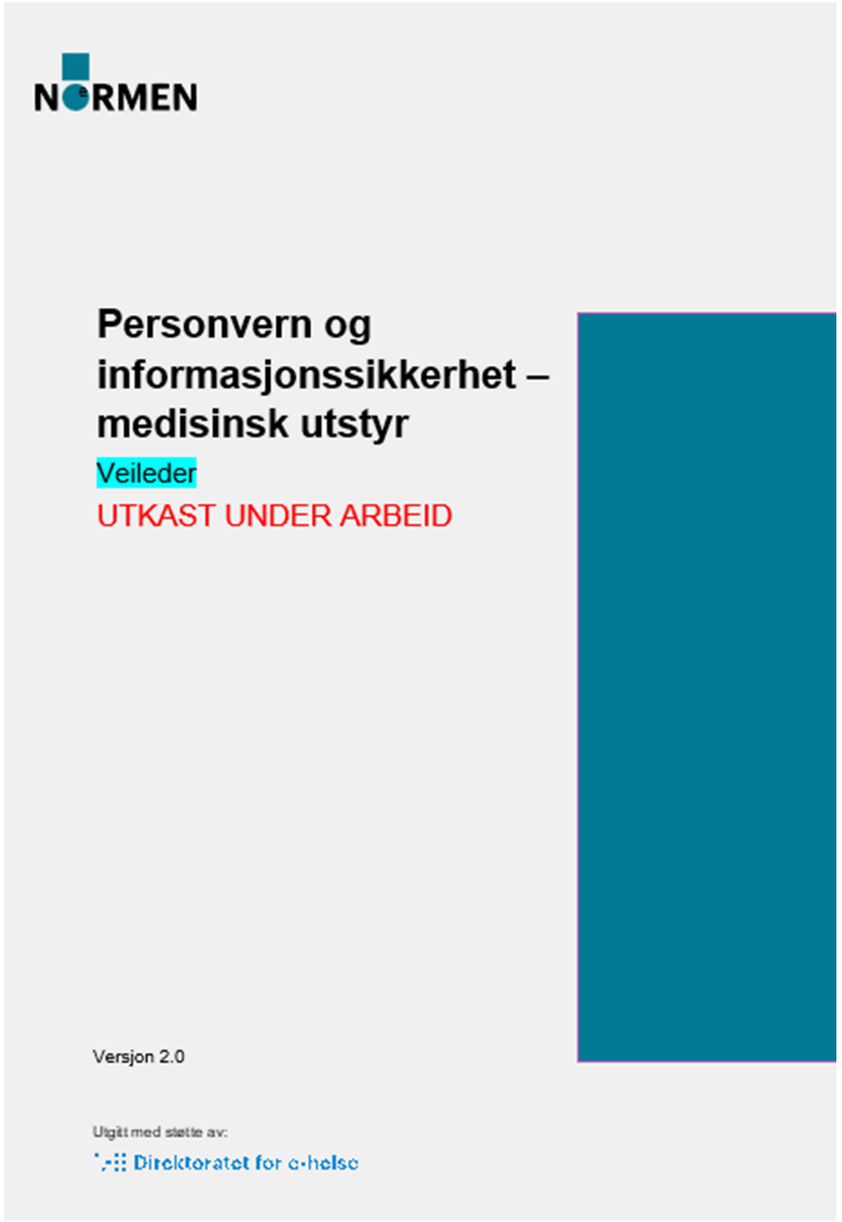
- innføringen av medisindispenserne ikke er en ny prosess da hjemmetjenesten i mange år har jobbet med medisineringsstøtte. Teknologien settes opp med en integrasjon til EPJ. Prosessen inkluderer ikke bruk av forsystem i en skytjeneste
- løsningen ikke samler inn nye personopplysninger om pasientene enn det de allerede gjør
- personopplysningene som behandles ikke er så omfattende.
- teknologien ikke er ny siden dette er blitt brukt i mange andre kommuner
- leverandør får tilgang til opplysningene som registreres i teknologien
- det behandles helseopplysninger i form av type medisiner som kan avsløre et helseforhold.
- det ikke blir inngripende kontakt mellom tjenesten og pasient/bruker. Dersom pasienten/ brukeren ikke tar medisin som planlagt vil dette følges opp av hjemmetjenesten som normalt.

NORMEN

Veien videre

- Brukerscenarier i MU veilederen – liste over scenarier for bruk i ROS arbeid
- Eksempler på kravspesifikasjon i anskaffelse av velferdsteknologi kommer! Utarbeidet av Helseetaten i Oslo kommune basert på Normens krav
- Ønsker oppdateringer fra sektoren på vurderinger om DPIA og ROS

- Velferdsteknologiens ABC



«KVIKKGUIDE»
til behandling av helse- og personopplysninger ved bruk av velferdsteknologi

- et samarbeidsprosjekt!

https://www.ks.no/fagomrader/helse-og-omsorg/velferdsteknologi3/behandling-av-helse--og-personopplysninger-ved-bruk-av-velferdsteknologi/

NORMEN

Spørsmål? Ta gjerne kontakt!

Petter.ludvig.andersen@ehelse.no
sikkerhetsnormen@ehelse.no