



WEBINAR:

Normens skyveileder - Bli med på en skyreise!

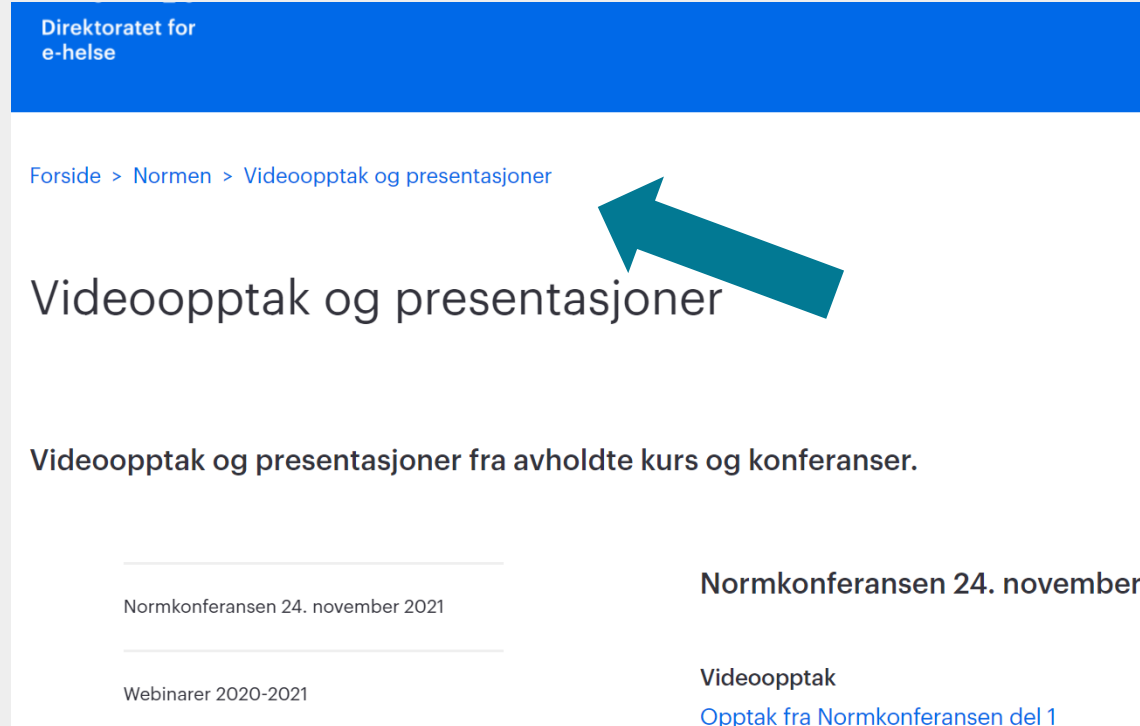
Thea Gulbranson, seniorrådgiver

Knut Herje, seniorrådgiver

14.02.2024

# Praktisk informasjon

- Vi setter mikrofonene deres på «mute» fra start
- Det foretas opptak av dette webinarret
- Vi legger ut opptak og presentasjoner på normen.no



Direktoratet for e-helse

[Forside](#) > [Normen](#) > [Videoopptak og presentasjoner](#)

## Videoopptak og presentasjoner

Videoopptak og presentasjoner fra avholdte kurs og konferanser.

---

Normkonferansen 24. november 2021

---

Webinarer 2020-2021

Normkonferansen 24. november

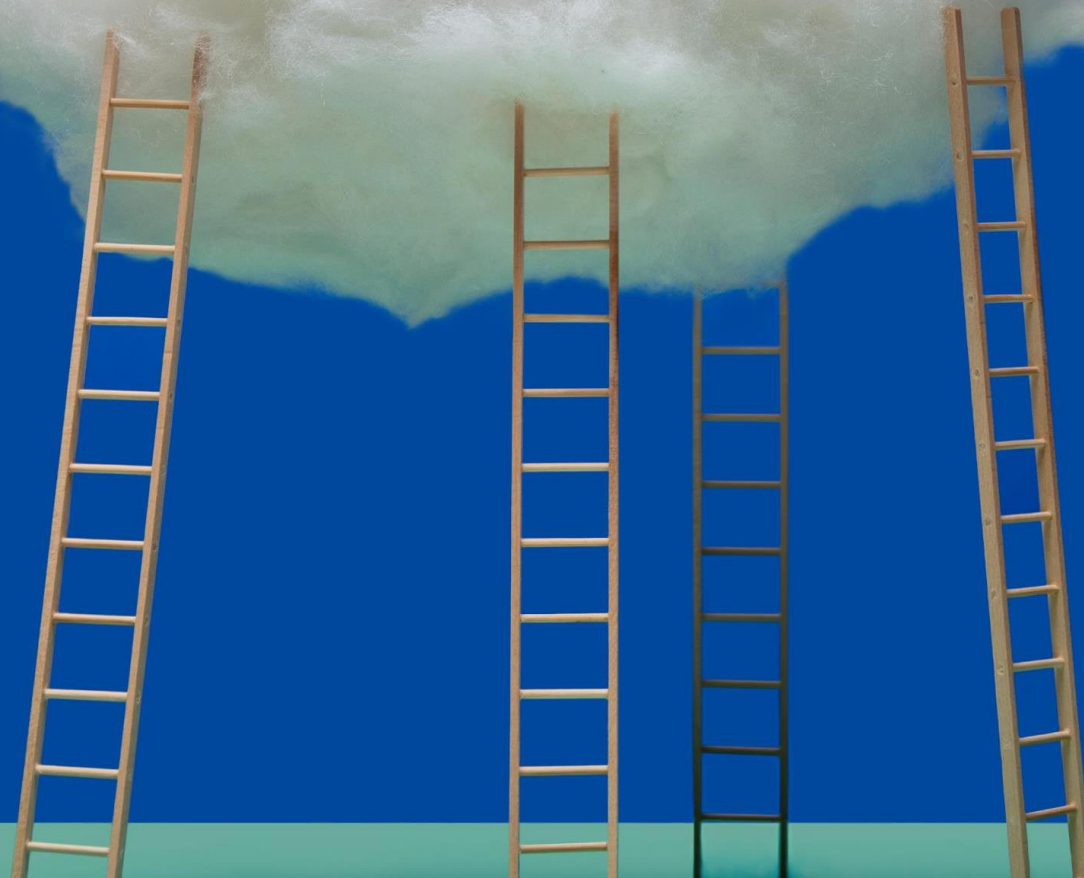
Videoopptak  
[Opptak fra Normkonferansen del 1](#)

# Spørsmål og kommentarer underveis

- Bruk chatfunksjonen når som helst under webinarret til spørsmål eller kommentarer
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Hvis du har spørsmål som ikke blir besvart under webinarret eller innspill du ønsker å komme med i etterkant, send oss en epost til [normen@helsedir.no](mailto:normen@helsedir.no)



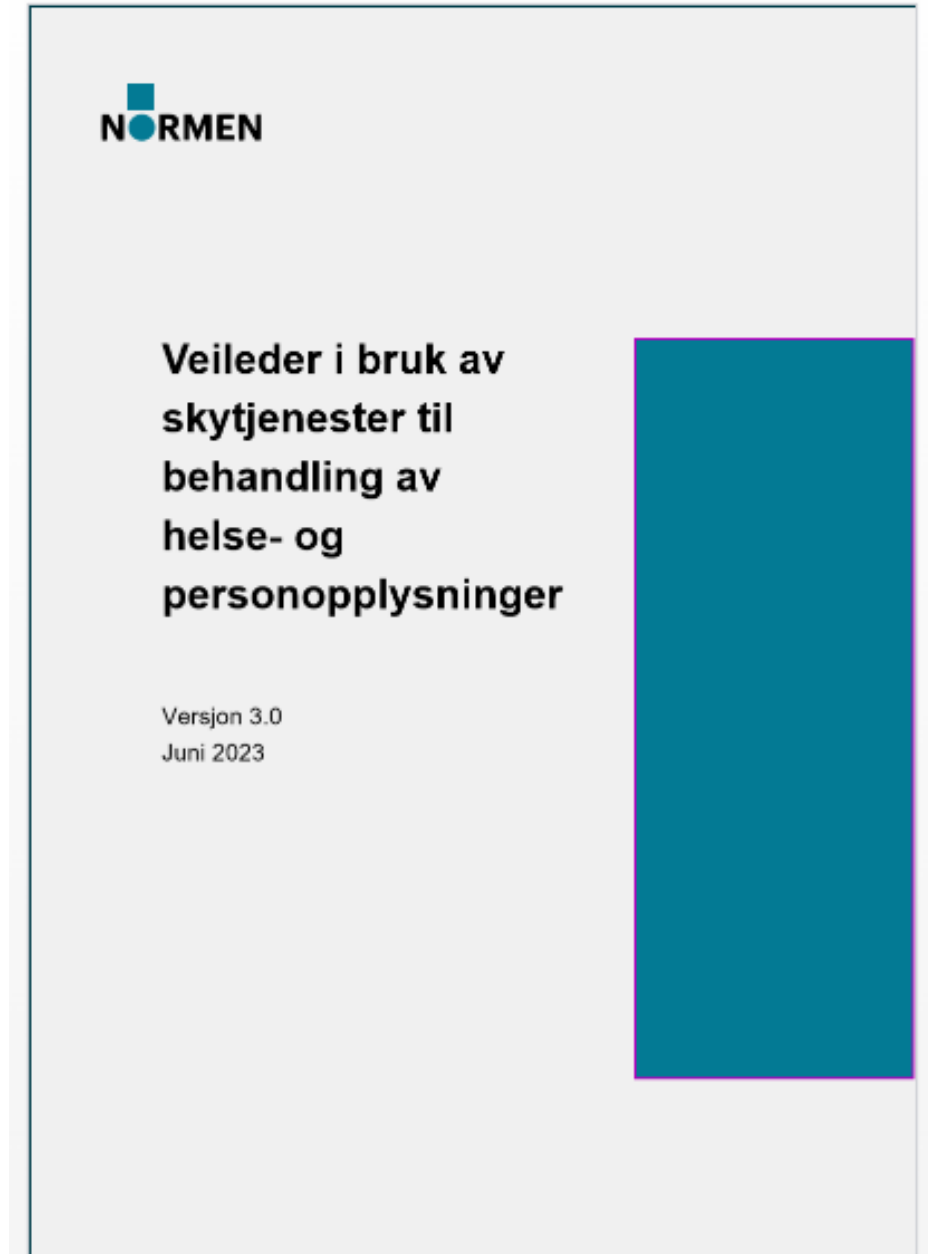
**«Vi skal i skyen»**

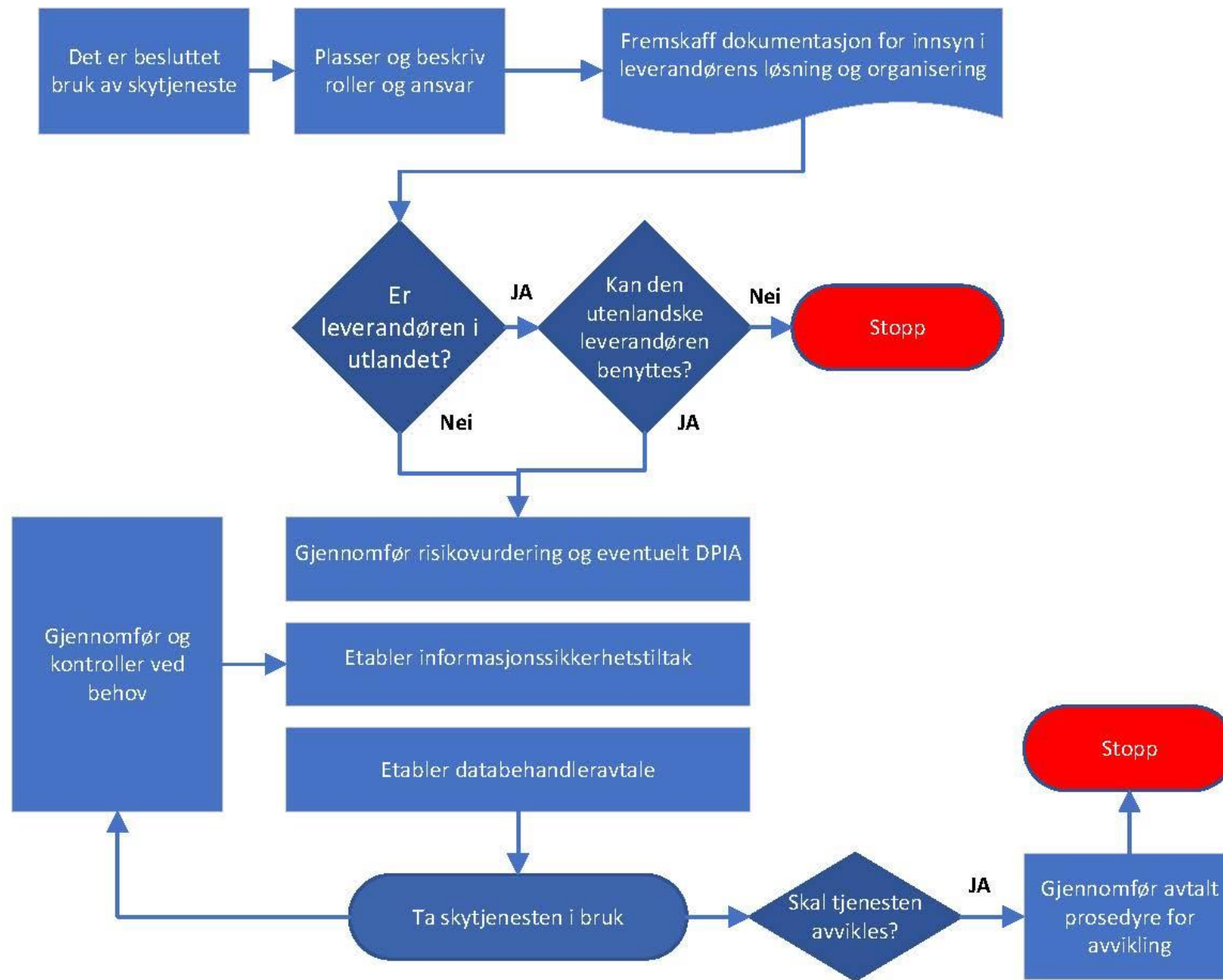


# Veileder for bruk av skytjenester

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
- Behandling av helse- og personopplysninger under Normens virkeområde

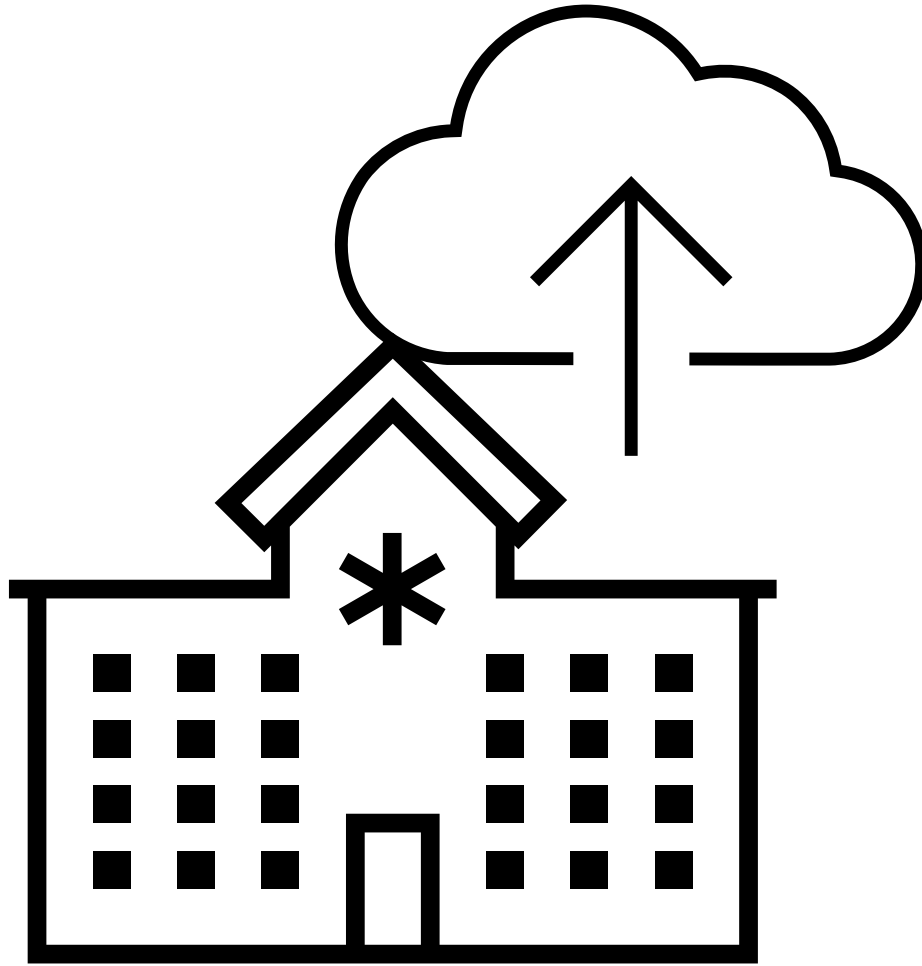




# Temaer i prosessen vi skal gå gjennom

- Vurderinger ved anskaffelse
- Risikovurderinger og personvern vurderinger
- Valg av sikkerhetstiltak
- Leverandøroppfølging og leverandørkontroll

# Dette er Normsykehuset. De skal anskaffe og ta i bruk en ny skytjeneste



- Tjenesten er lagring av pasientjournal i skyen
- Det skal lagres pasientdata i skytjenesten
- Data lagres i Norge
- De er forpliktet til å følge Normen!



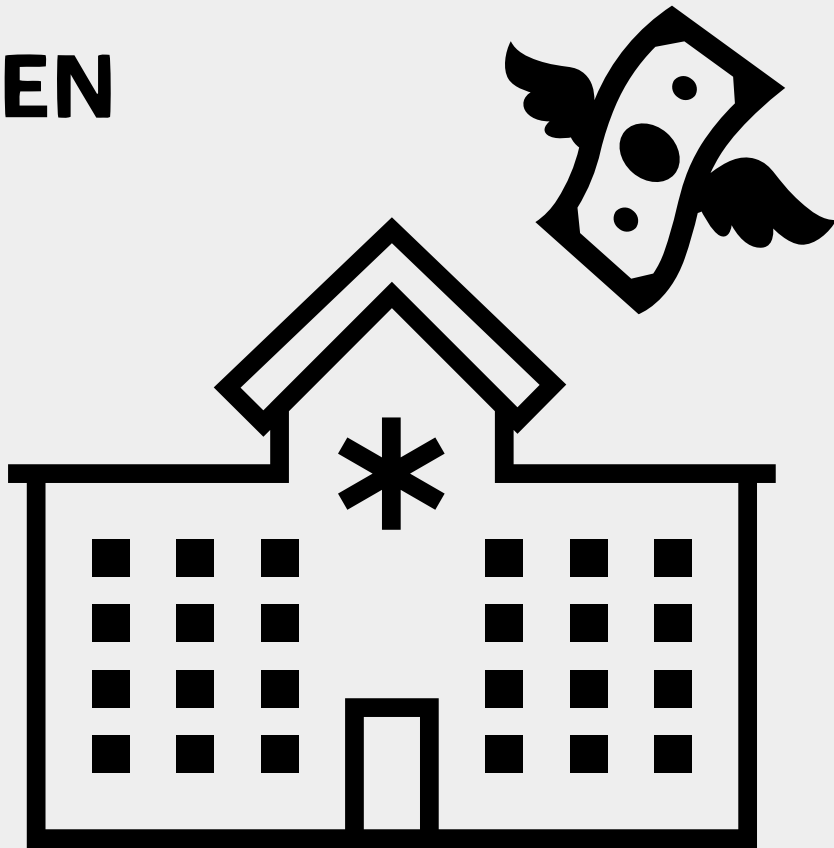
# Normsykehuset vurderer fordeler og ulemper med å ta i bruk skytjeneste

## Fordeler

- Høyere grad av sikkerhet for servere og utstyr
- Slipper å kjøpe og installere oppdateringer selv
- Rask håndtering av patching
- Sikkerhetsoppdateringer
- Mulig å skalere opp ved behov
- Systemet er tilgjengelig der hvor brukeren er

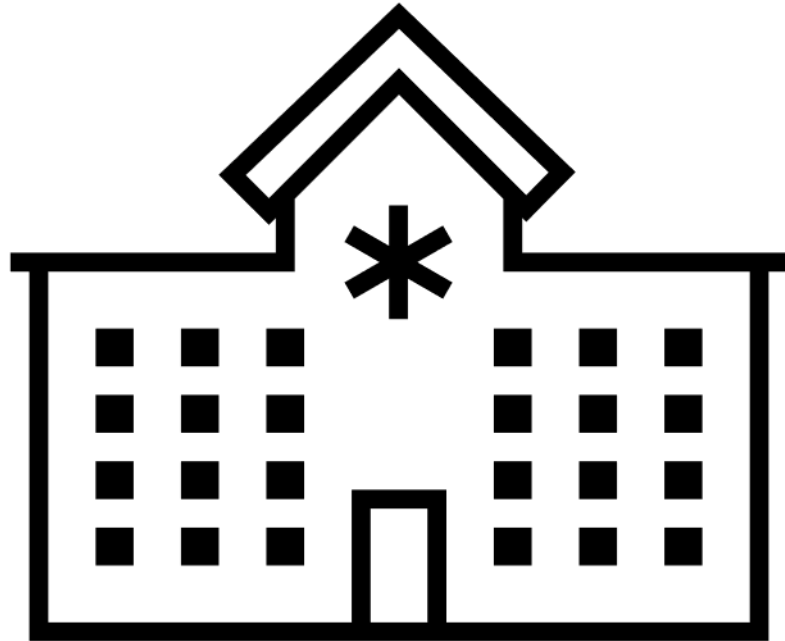
## Ulemper

- Tjenesten krever en annen type forvaltning
- Ansvarslinjene kan være uklare
- De er usikre på hvor opplysningene befinner seg
- Usikker på om leverandøren oppfyller kravene i Normen
- Leverandøren kan ha standardbetingelser som er vanskelige å forstå



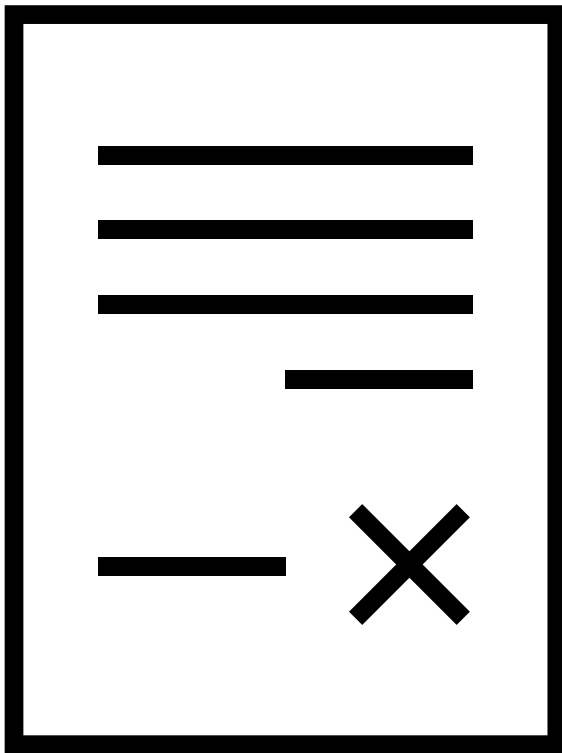
Steg 1: Anskaffelse

# Hvilke krav bør man stille til leverandør?



- Krav som stilles i anskaffelsen legger grunnlaget for god innføring og drift av tjenesten.
- Normen har veiledningsmateriell for hvordan kravene kan brukes i anskaffelser.
- Det kommer også en «oversettelse» av kravene i Normen til bruk i kravspesifikasjoner

# Hva kan/bør Normsykehuset regulere i databehandleravtalen?



- Segmentering av informasjon slik at det er logisk eller fysisk separasjon mellom ulike virksomheters data.
- Hvordan sikkerhetskopiering gjennomføres og hvordan tilbakekopiering skal skje.
- Hvor og i hvilket land den faktiske lagringen av helse- og personopplysninger skjer
- Innsyn i den tekniske løsningen.
- Innsyn i logger.
- Hvordan pasientens rettigheter ivaretas
- Prosesser for avviksbehandling

# Hvor behandles dataene?



Utgangspunkt: Virksomheter som overfører personopplysninger til utlandet, skal påse at beskyttelsesnivået i personvernforordningen skal opprettholdes ved overføringen.



Risikovurdering og sikkerhetstiltak

# Normsykehuset må gjøre en risikovurdering og DPIA av tjenesten

- For å kunne vurdere om skytjenesten skal tas i bruk, må risikoområdene, som informasjonssikkerhet, personvern og pasientsikkerhet, vurderes opp mot hverandre.
- Riktig kompetanse må være med!
- Når i prosessen skal risikovurderingen gjennomføres?


Hvor sannsynlig er det?

Hvilke konsekvenser kan det få?

Hvor plasserer vi scenarioet i risikomatriksen?

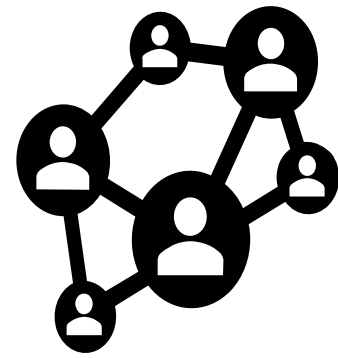
Sannsynlighet	5 Svært sannsynlig	Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
	4 Sannsynlig	Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
	3 Mulig	Mindre sannsynlig	Mindre sannsynlig	Moderat	Alvorlig	Svært alvorlig
	2 Mindre sannsynlig	Mindre sannsynlig	Mindre sannsynlig	Moderat	Alvorlig	Svært alvorlig
	1 Usannsynlig	Mindre sannsynlig	Mindre sannsynlig	Moderat	Alvorlig	Svært alvorlig
Risikomatrikse		Konsekvens				

# Hvilke risikoer og tiltak kan være relevante å vurdere

- Overskuddsinformasjon som benyttes til andre formål?
  - Løsepengevirus, etterretningsoperasjoner, tjenestenekt, og datatyveri og salg av informasjon på det mørke nettet.
  - Leverandør behandler helse- og personopplysningene i strid med databehandleravtalen.
  - Hvor ligger dataene?
  - Hvordan sikres pasient- og personrettigheter
  - Tilbakelevering
- 
- Tilgangsstyring
    - Logging
    - Krypering
    - Opplæring
  - Sikkerhetskopiering



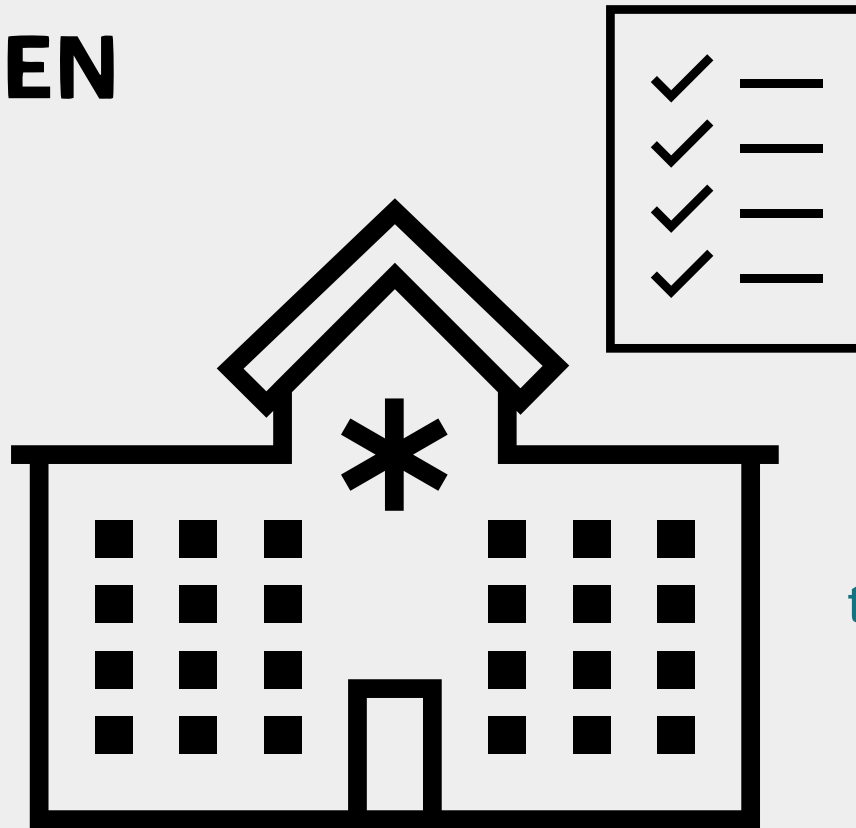
# Migrering til sky



- Normsykehuset flytter tjenester og systemer som tidligere ble driftet lokalt til en skytjeneste.
- Det er noen forhold de bør ha kontroll på før tjenesten flyttes i skyen:
  - Er det tatt hensyn til i kontrakten med leverandøren?
  - Fungerer integrasjoner med andre systemer som de skal etter migrasjon, eller må disse konfigureres på nytt?
  - Beholder løsningen all tidligere funksjonalitet?

# Normsykehuset

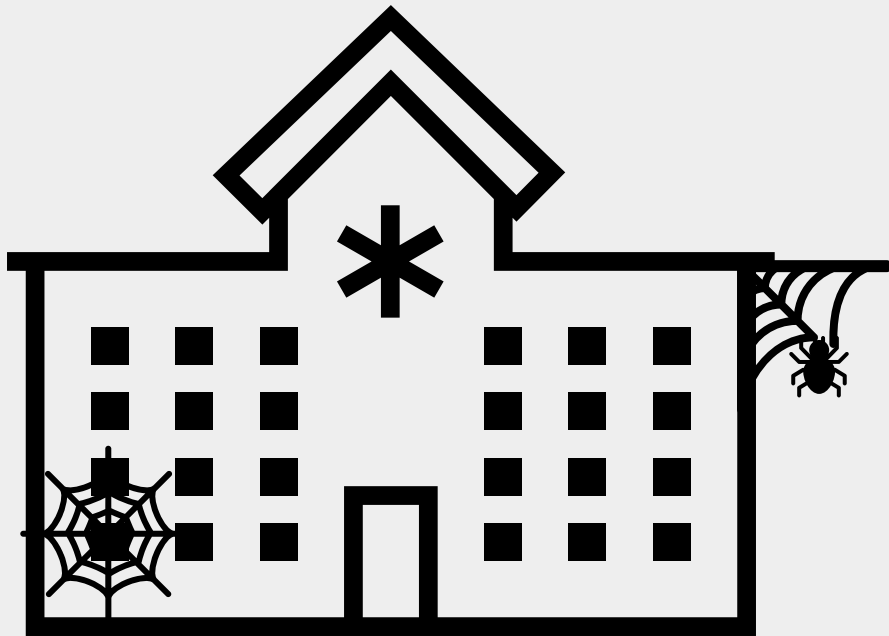




Avtale er signert, Normsykehuset har brukt tjenesten i en stund. Det er på tide å følge opp leverandøren!

# Revisjon underveis i avtaleforholdet

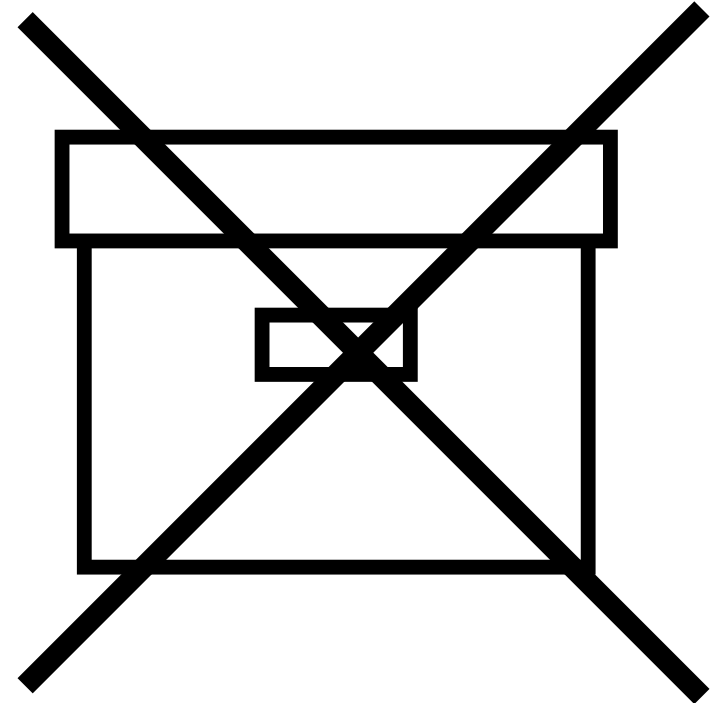
- Normsykehuset har plikt til å kontrollere at skyleverandøren oppfyller kravene som er nedfelt i personvernforordningen og i databehandleravtalen mellom partene.
- Behovet og hyppigheten for revisjon vil bero på hvor høy risiko som er forbundet med behandlingen.
- Revisjon avtales ofte årlig, men kan være nødvendig å gjøre oftere.

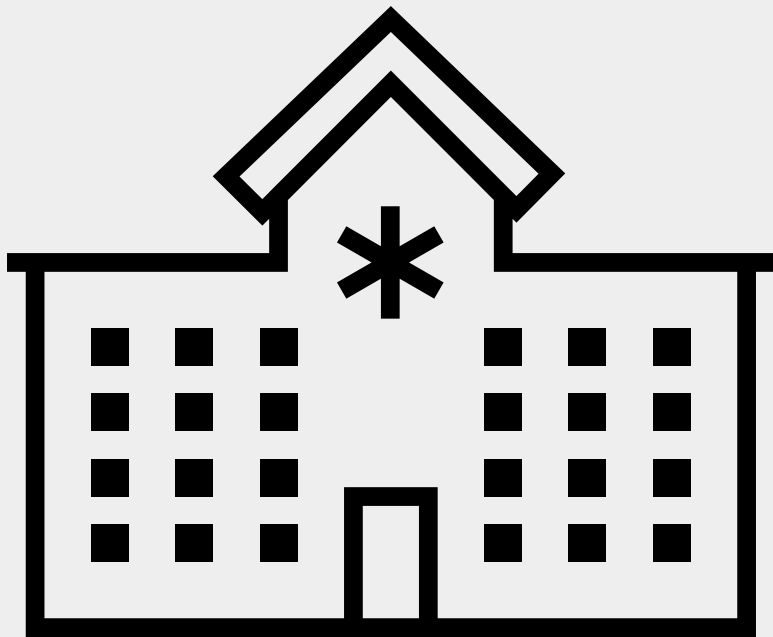


Tiden går.....  
Etter noen år begynner tjenesten å bli litt utdatert,  
og Normsykehuset bestemmer seg for å bytte  
leverandør

# Avvikling av tjenesten

- Leverandøren må levere tilbake alle helse- og personopplysninger, også backup.
- Alle opplysninger må deretter slettes





Normsykehuset er ferdig med denne skyreisen,  
og skal snart i gang med en ny!

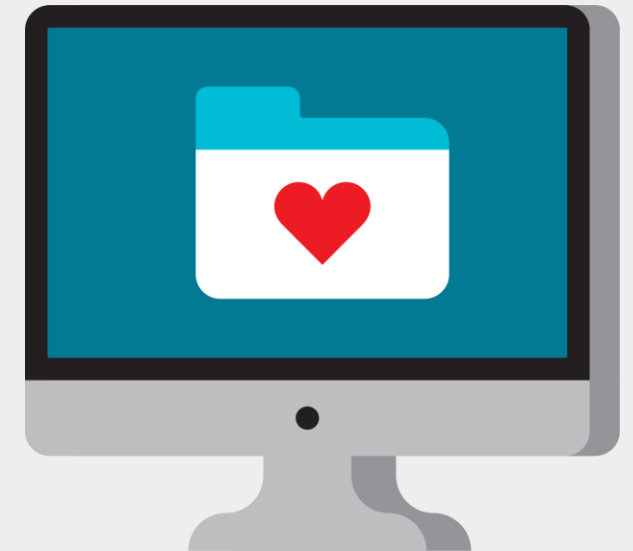


## Spørsmål fra den digitale salen



# Ta gjerne kontakt om du har innspill til Normens veiledningsmateriell!

- Hva trenger du?
- Hva mangler?
- Hva kan oppdatert veiledningsmateriell bidra med?



**[normen@helsedir.no](mailto:normen@helsedir.no)**

# Hvordan holde deg oppdatert på alt som skjer?!?



Direktoratet for e-helse

# Normen.no

Søk

Meny

Forside > Normen

## Normen

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.



Direktoratet for e-helse

## Nyhetsbrev

Velg hvilke interessefelt du ønsker å motta nyhetsbrev fra. Dersom du ikke velger noen interessefelt, får du tilsendt aktuell informasjon fra Direktoratet for e-helse.

Du kan når som helst endre dine innstillinger for nyhetsbrevet.

E-postadresse:

### Interesser

- Aktuell informasjon fra Direktoratet for e-helse
- Arkitekturstyring, standarder og referansekatalog
- Akson: Helhetlig samhandling og felles kommunal journal
- Helsedataprogrammet
- Helsefaglige kodeverk og terminologi
- Norm for informasjonssikkerhet (personvern og informasjonssikkerhet)



# Bli med på våre andre arrangementer!

28. februar	Pen-Testing av Medisinsk utstyr
20. mars	Vil du lære mer om god passordhåndtering?
Datoer kommer	Gjennomgang av de offisielle trusselvurderingene og hvordan kan vi bruke dem
	Workshop om revisjon av veilederne om medisinsk utstyr og velferdsteknologi
	Tilgangsstyring i Helseplattformen
	CISO-samtale fra CISO-nettverksmøte
	HelseID
	Risikostyring

Følg med på [normen.no](https://normen.no), sosiale medier og Normens nyhetsbrev!