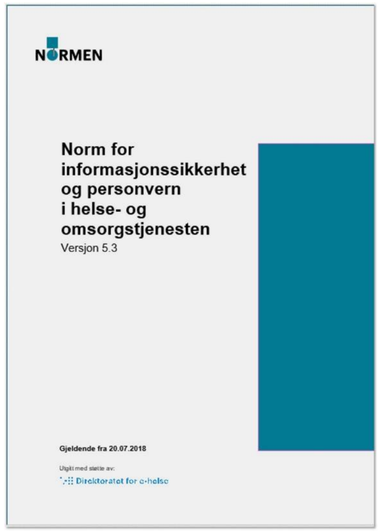
Hva skal til for å kunne benytte skytjenester til høsting av data fra utstyr som benyttes utenfor sykehus

Nasjonalt seminar BHM, Olavsgård

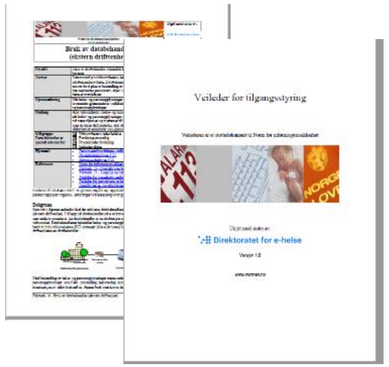
13.11.2019

Bakgrunn | Om Normen

Normen



Faktaark og veiledere



Utadrettet virksomhet

Normkonferansen

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

Normen er åpent tilgjengelig via **www.normen.no**

Andre aktiviteter i regi av Normen

Normkonferansen

(25.) 26.-27. november 2019
The Qube" - Clarion hotell og kongress Oslo airport

Nyhetsbrev

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

Q&A epost

sikkerhetsnormen@ehelse.no

Kurs og foredrag

- Kurs
- Konferanser
- Foredrag

www.normen.no

- Alle dokumentene
- Nyheter
- Om Normen

Sosiale medier

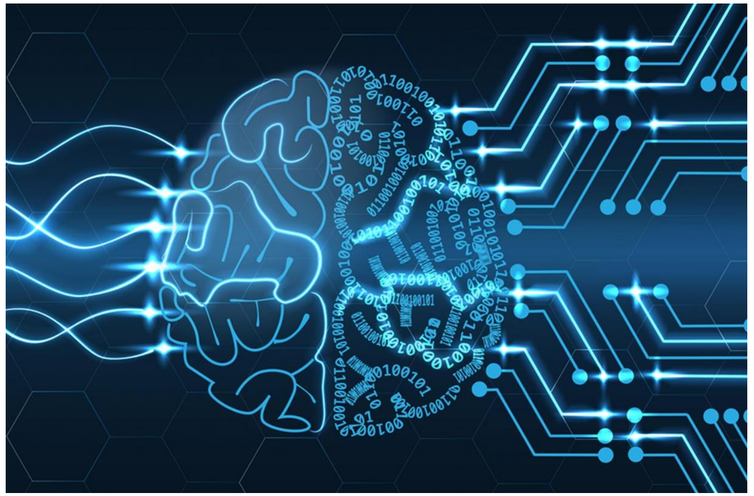
Normen på FB

NORMEN

Skyteknologi i Helsesektoren

I 2020 vil det genereres i gjennomsnitt **1 GB** helserelaterte data per person **daglig**
Kilde: Microsoft

Noen drivere for skyteknologi i helse



Kunstig intelligens

Genteknologi/ persontilpasset medisin

Sensorteknologi IoT

Hvor er data lagret?

Hvordan kan vi utføre kontroll med leverandør?

Kan vi etablere god nok avtale med leverandør?

Har leverandør innsyn i våre data?

Hvordan skal vi trygt nå tjenestene for drift?

Hvilke underleverandører benytter skyleverandøren?

Kan vi slette data på leverandørens delte infrastruktur?

Har vi kontroll når leverandør patcher?

Hvordan sikrer vi admintilgang?

Kan vi hindre ondsinnet kode i løsningen?

Hvordan sikrer vi tilgang til loggene?

Er sikkerheten i valgte tjenester/komponenter ivaretatt?

Har vi kontroll på tilgangene som gis?

Er sertifikater og tokens godt nok sikret?

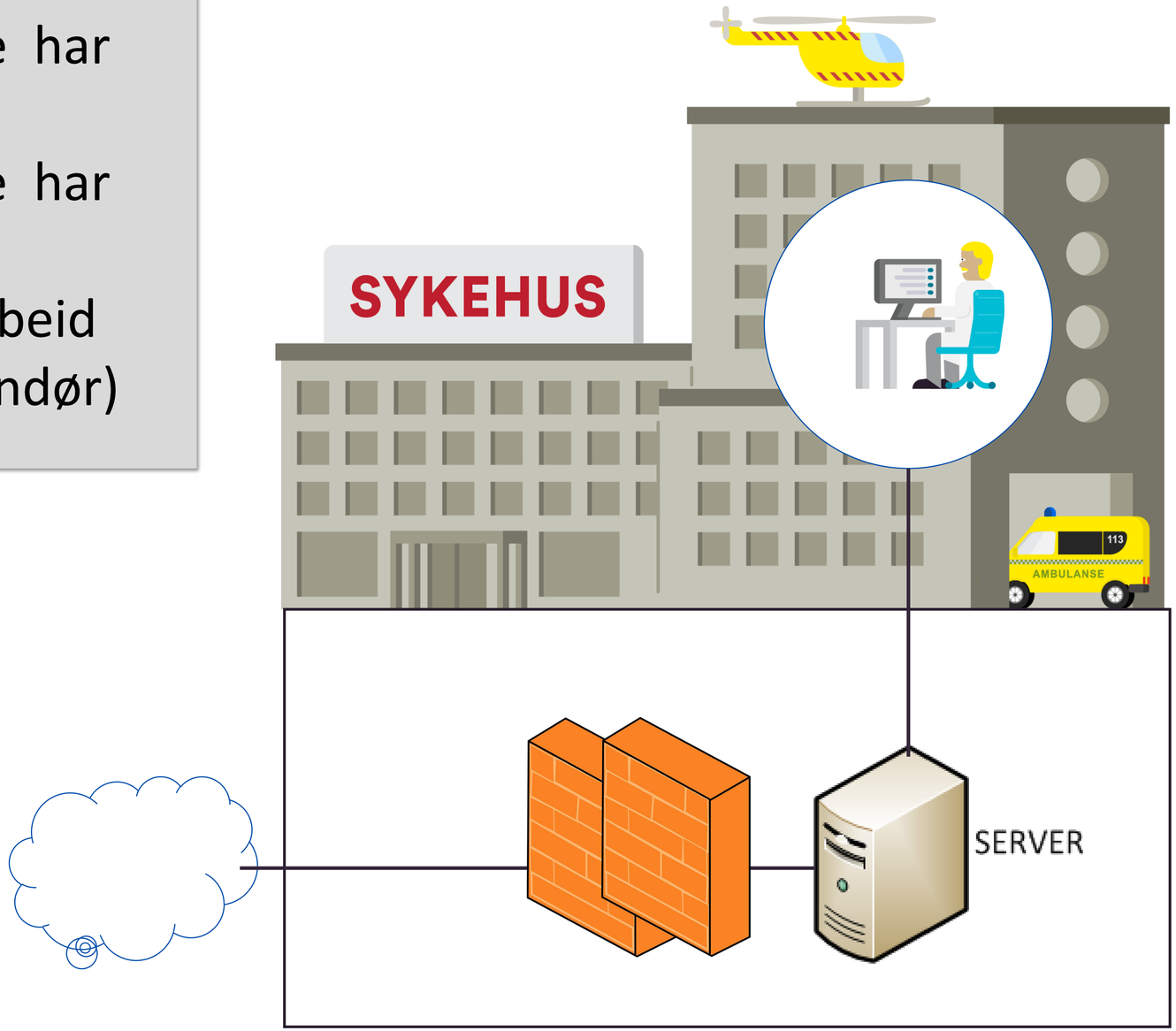
Beskyttes tjenesten mot eksterne angrep?

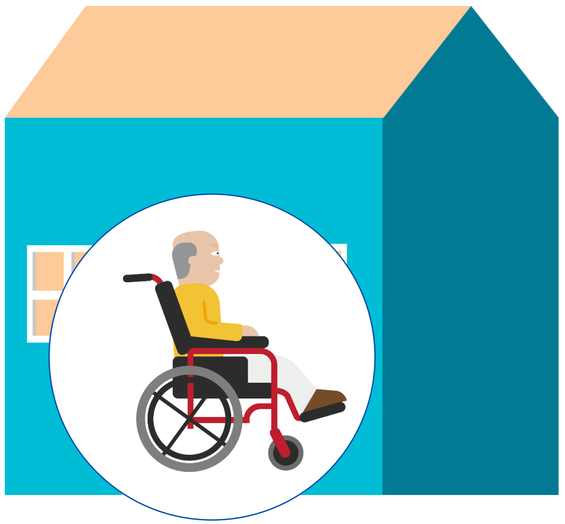
Sletter vi data som ikke lengre er relevante?

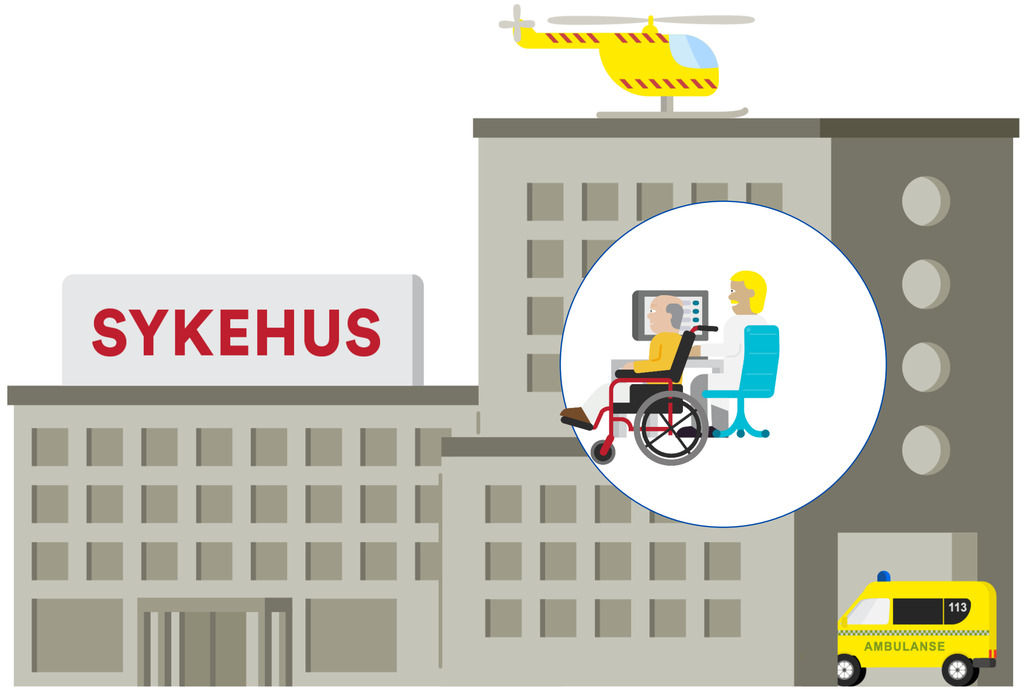
Lysbilde: Andre Meldal, Norsk Helsenett

Case: Avstandsoppfølging av pasient

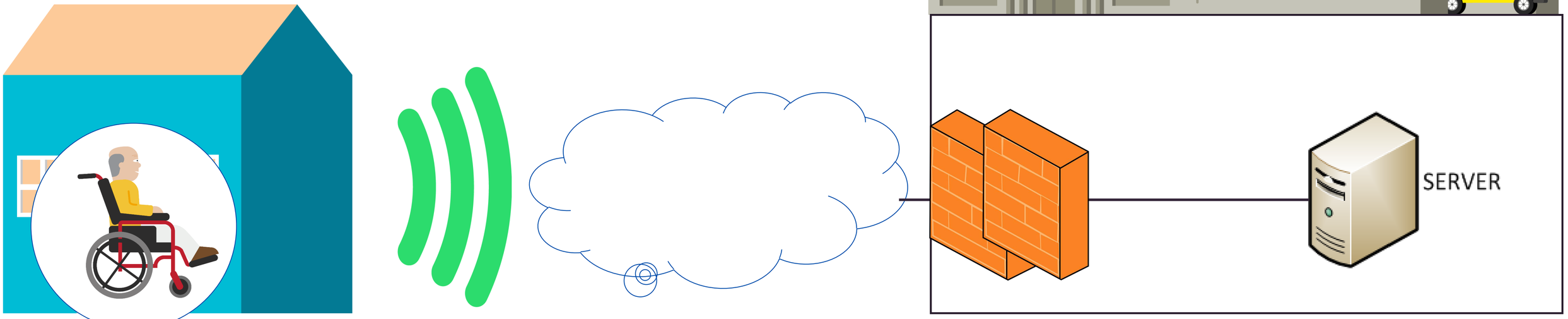
- Den dataansvarlige har **ansvaret**
- Den dataansvarlige har **kontrollen** (i hvert fall i samarbeid med sin IKT-leverandør)






SYKEHUS
113
AMBULANSE

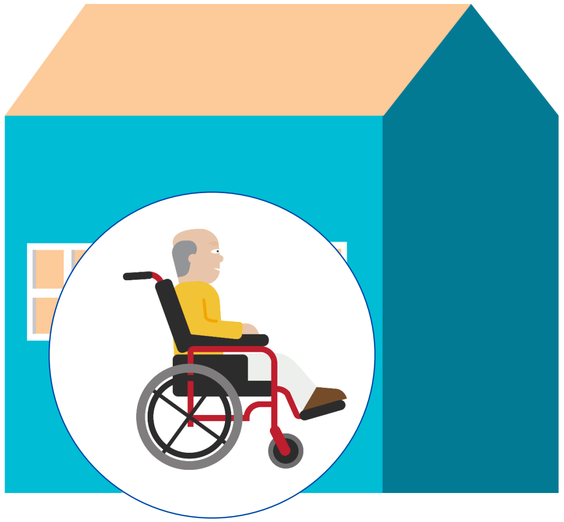
- **Usikker infrastruktur** i pasientens hjem (både konfidensialitet og tilgjengelighet)
- **Sikker autentisering**
  - Av «bokser»
  - Av pasient / bruker (kognitiv svikt?)
- **Overskuddsinformasjon**
  - Dokumentasjonsplikt
  - Sletting
  - Samtykke
- Hva skal **logges**?
- **Medisinsk utstyr** – en sikkerhetsutfordring

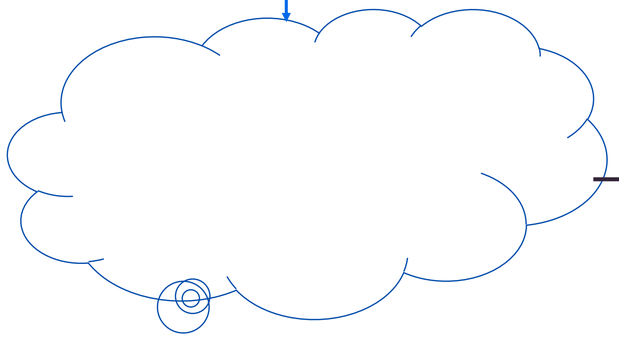


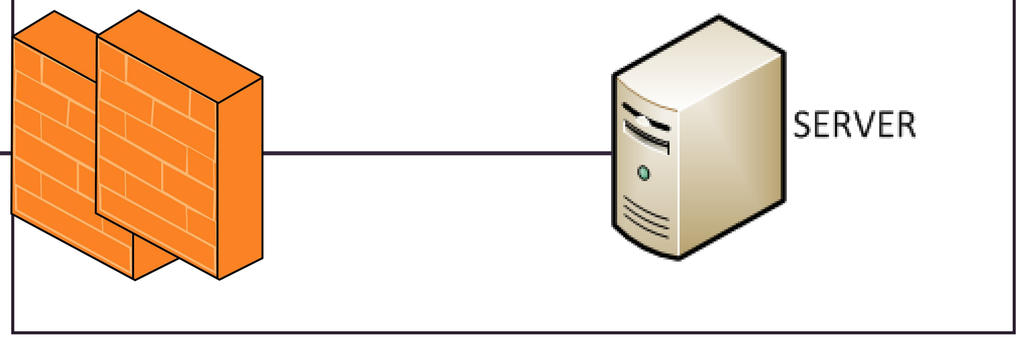
???

Leverandør
(f.eks utstyrsprodusent)

Mellomlagring
Pre-prosessering



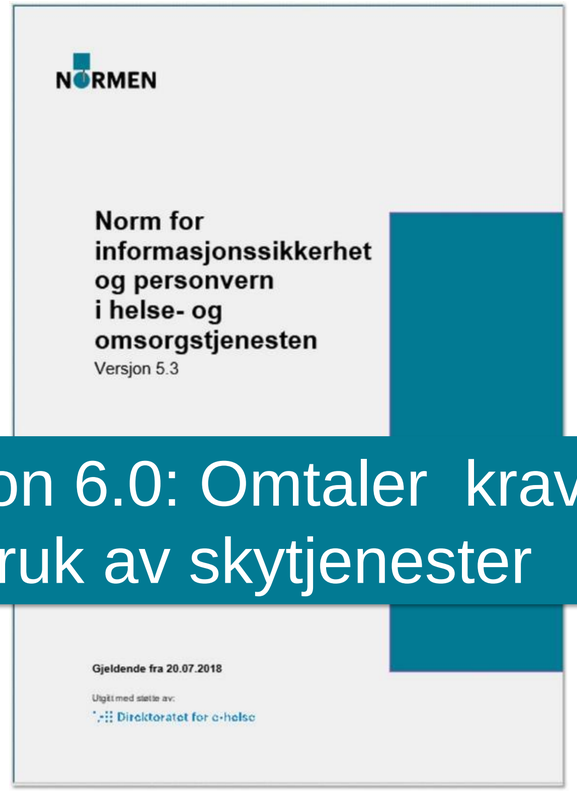




Noen ressurser og verktøy

Noen ressurser og verktøy

Konkrete råd i anskaffelser og leverandøroppfølging



Versjon 6.0: Omtaler krav til bruk av skytjenester

Rapport lansert 30.11.17

«Direktoratet for e-helse mener at det ikke er grunnlag for å konkludere med at noen typer tjenester aldri kan overlates til private leverandører»

Viktige forutsetninger:

- Risikovurdering
- Lav risikoappetitt

Forslag til viktigste tiltak som bør gjennomføres sentralt:

- Avklaring av databehandlingsansvar mellom regionale helseforetak og helseforetak
- Oppdatering av Normen
- Kompetanseheving innen IKT-sikkerhet og risikovurdering på styre og ledelsesnivå

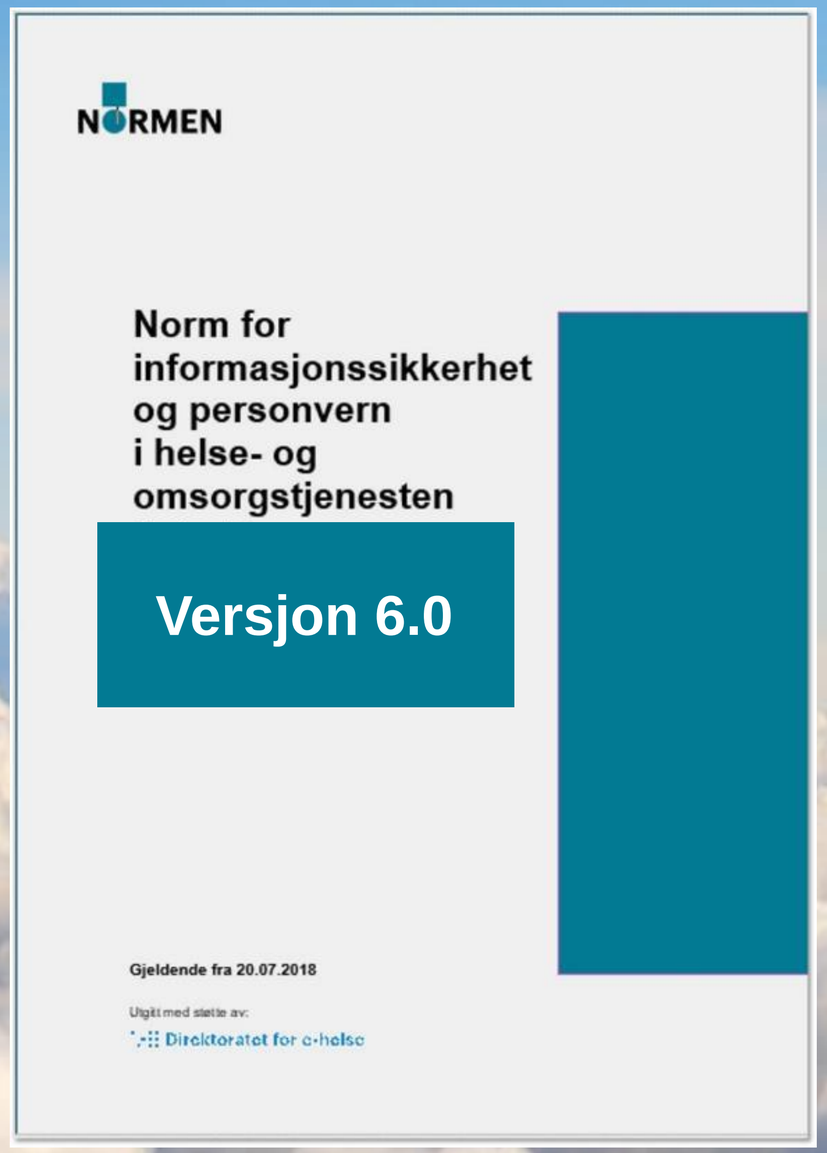
Kriterier og rutiner som bør implementeres i sektoren knyttet til:

- Sikre god og reell ledelsesforankring
- Tilstrekkelig kompetanse

- Helhetlig risikostyring

NORMEN

Om sky i neste versjon av Normen



Viktige begreper

Behandlingsansvarlig

Den som alene eller sammen med andre **bestemmer formålet** med behandlingen av personopplysninger og hvilke midler som skal benyttes

Kan **utpekes** i lov eller forskrift

Er **ansvarlig** for behandlingen av personopplysninger

Dataansvarlig

Begrepet som brukes **om behandlingsansvarlig i helse**

Eget begrep i lovgivningen i vår sektor for å unngå forveksling med ansvar for pasientbehandling

Oslo universitetssykehus

Databehandler

En som behandler personopplysninger **på vegne** av behandlingsansvarlig

SYKEHUSPARTNER

Microsoft

Abbott

Noen grunnkrav

- Taushetserklæringer for leverandørens personell
  - Kan administreres av leverandøren selv

- Personvernforordeningens krav
  - Databehandlers selvstendige ansvar for informasjonssikkerhet
  - Åpenhet om bruk av underleverandører
  - Krav til medvirkning ved avvik
  - **Alltid databehandleravtale**

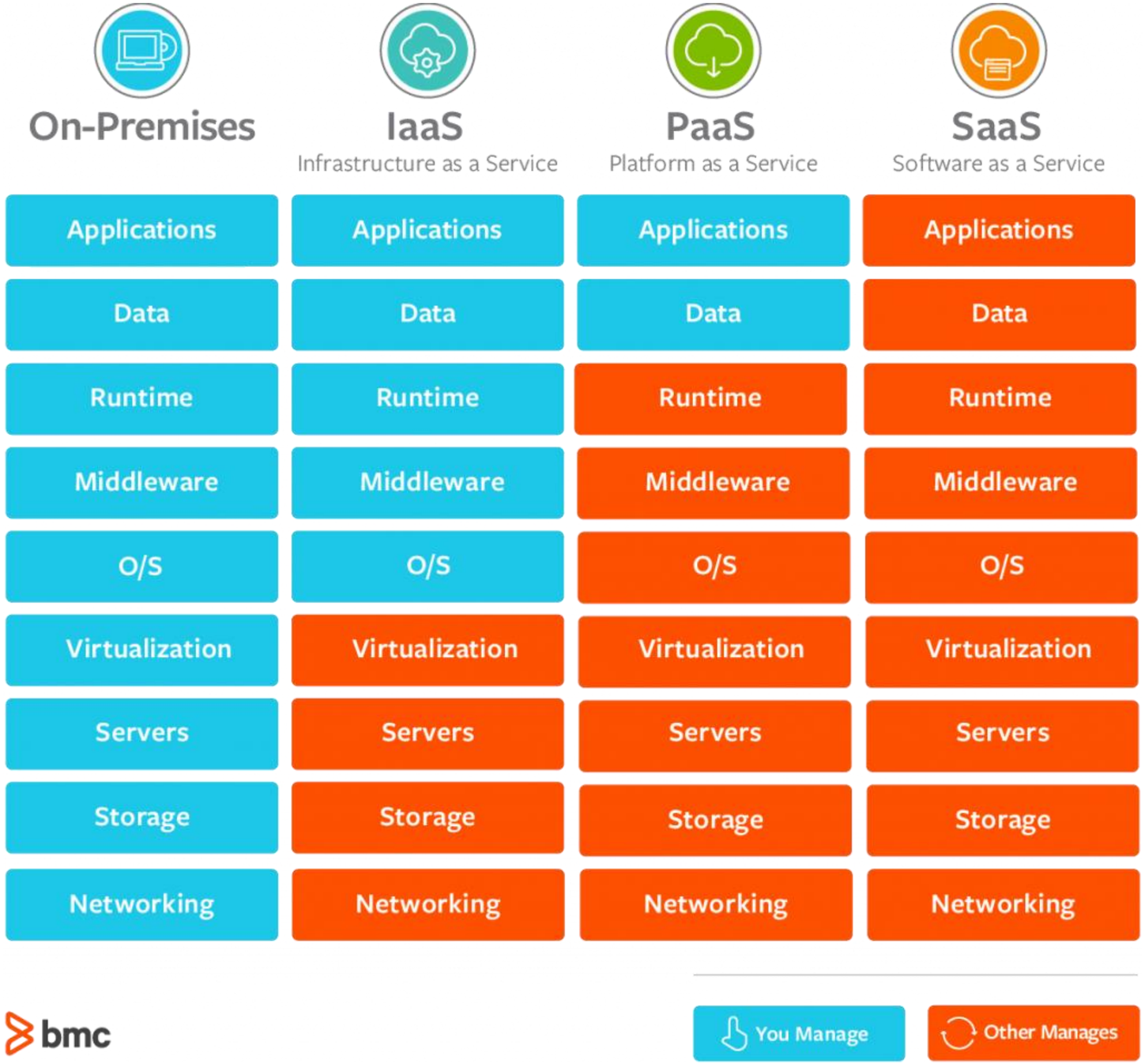
- **Alltid risikovurdering basert på beskrivelse av konfigurasjon og dataflyt**

- Krav til sikkerhetsrevisjoner (kan håndteres av 3. part)

NORMEN

Ansvarsfordeling

Ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset leveransemodellen som benyttes



Hvor data behandles geografisk

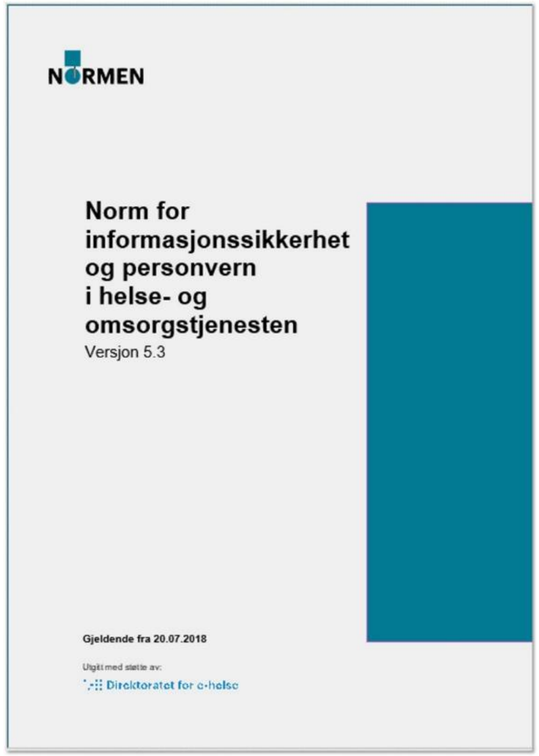
- Innenfor / utenfor EU/EØS
- Godkjent 3. land (liste med 12 navn)
- Andre mekanismer som sikrer «tilstrekkelige garantier»
  - Privacy shield
  - EU standardavtaler

- Landrisikovurdering – også innenfor EU/EØS

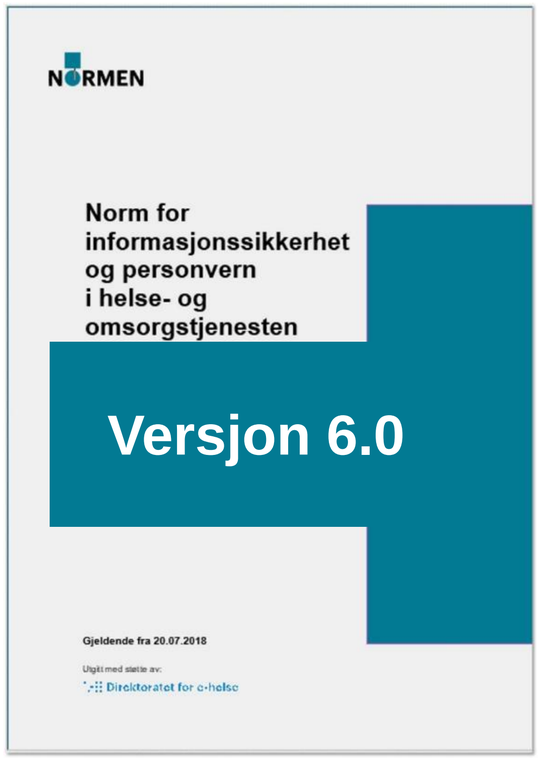
Dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med Normens krav

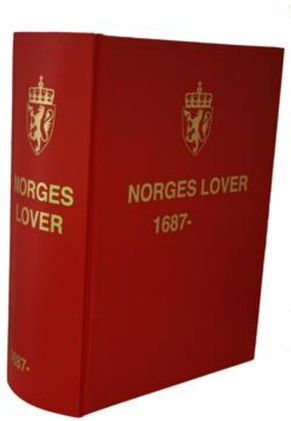
???

Dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med Normens krav



Forenkles ved mapping av Normen





CCM™
Cloud Controls Matrix

EXIT-strategi

- Dataansvarlig skal sørge for å ha en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten

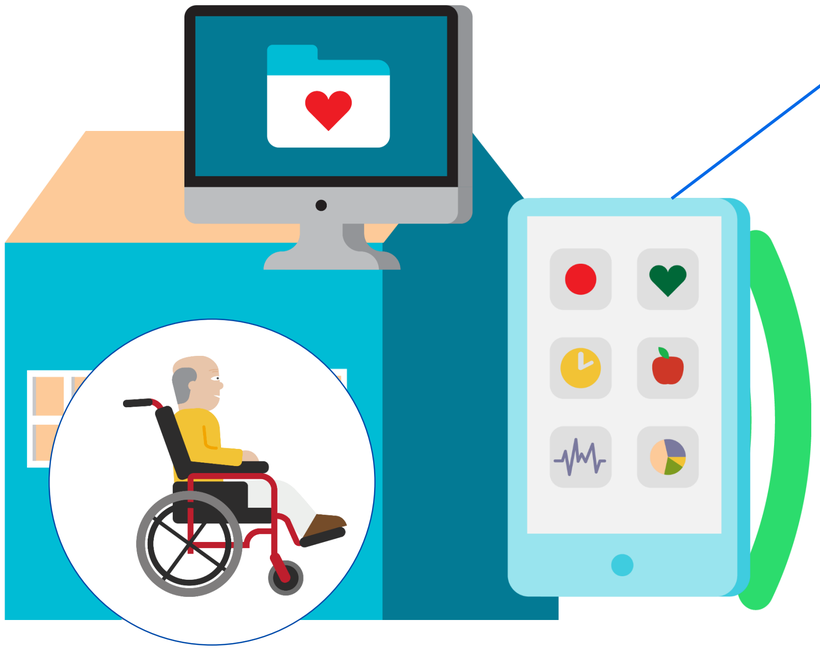
- Ved terminering av kontrakten skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid.

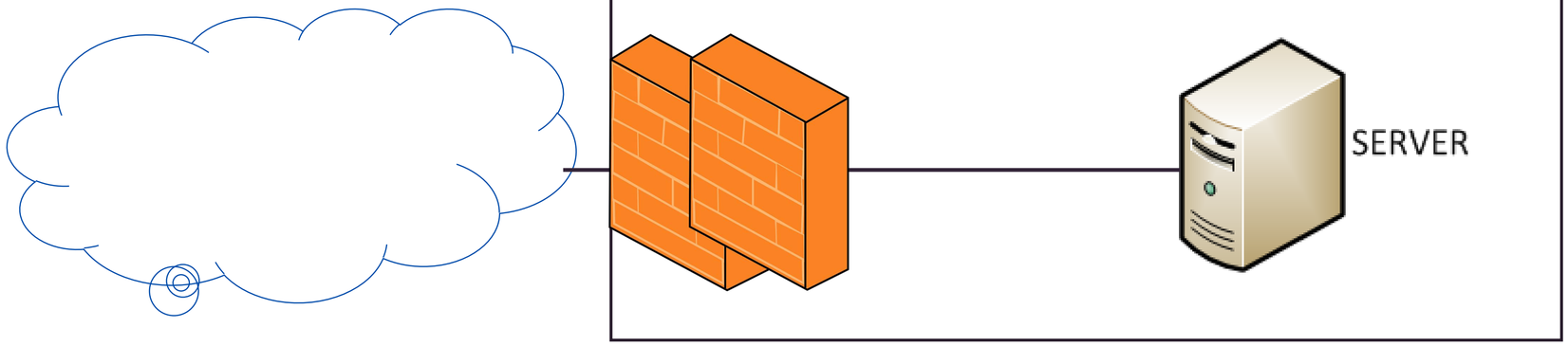
- Hvordan unngå lock-in?

???

Leverandør
(f.eks utstyrsprodusent)

Pasienten
tar i bruk
tilleggsfunksjonalitet
som tilbys av
f.eks utstyrsleverandør

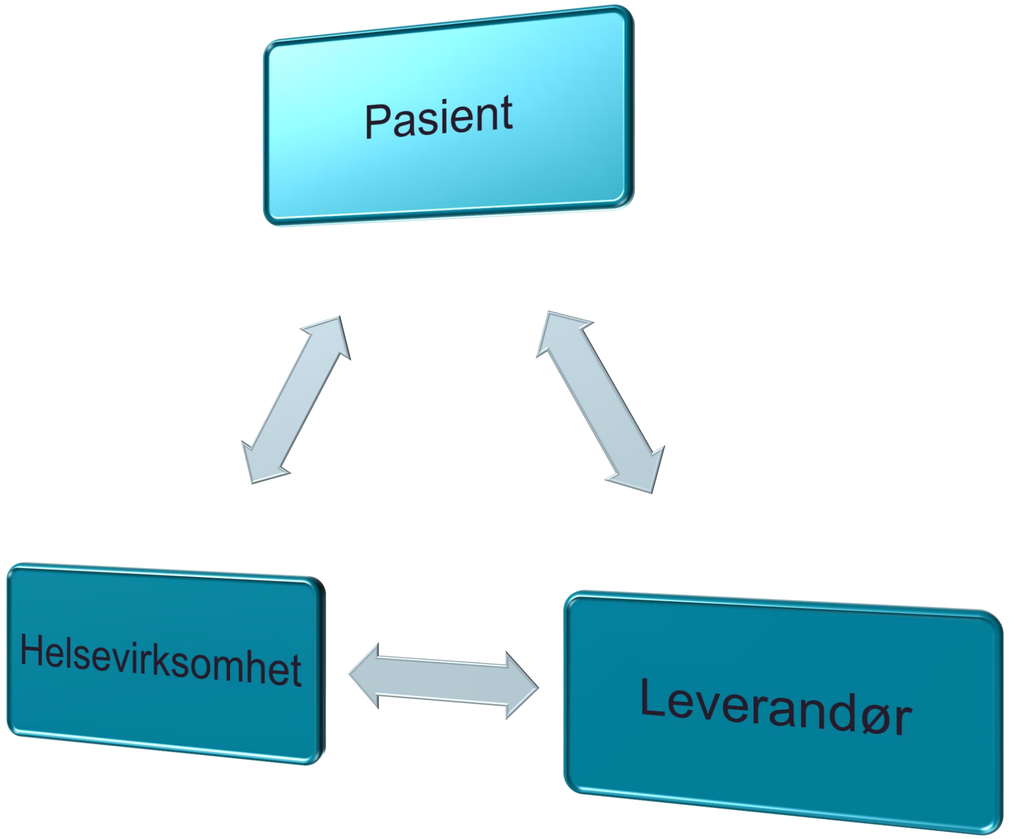




Når pasienten på egen hånd tar i bruk tjenester fra leverandøren?

- Ansvarsforhold – hvem er dataansvarlig?

- Problemstillinger i følge *Helsedata til salgs? (Forbrukerrådet 2017):*
  - Omfattende brukervilkår (i gjennomsnitt 14 sider)
  - Overføring til andre formål / til tredjepart
  - Manglende sletting
  - Krav til brukerkontoer for lagring



Takk for meg!

sikkerhetsnormen@ehelse.no
www.normen.no

Facebook – Norm for informasjonssikkerhet