Helseopplysninger i skyen

13.02.2020

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?

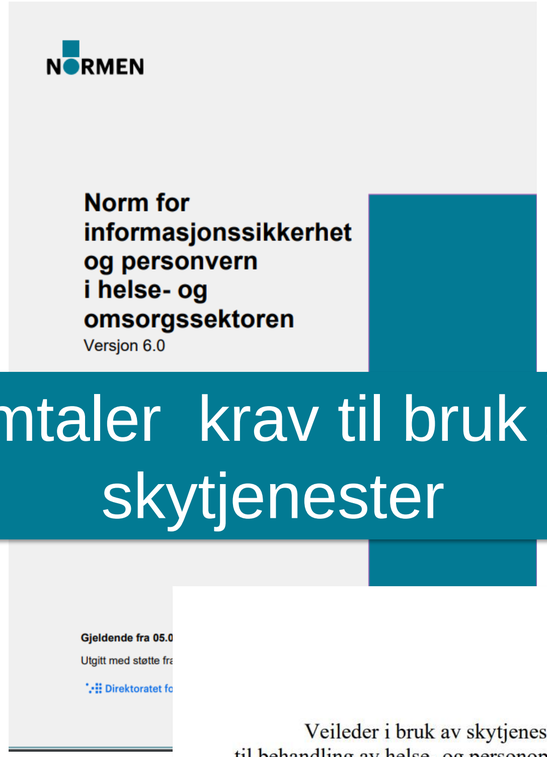
Lysbilde: Andre Meldal, Norsk Helsenett

https://www.geekculture.com/joyoftech/joyarchives/2340.html

Noen ressurser og verktøy

Noen ressurser og verktøy

Konkrete råd
i anskaffelser og
leverandøroppfølging



Omtaler krav til bruk av skytjenester

Under oppdatering

NORMEN

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

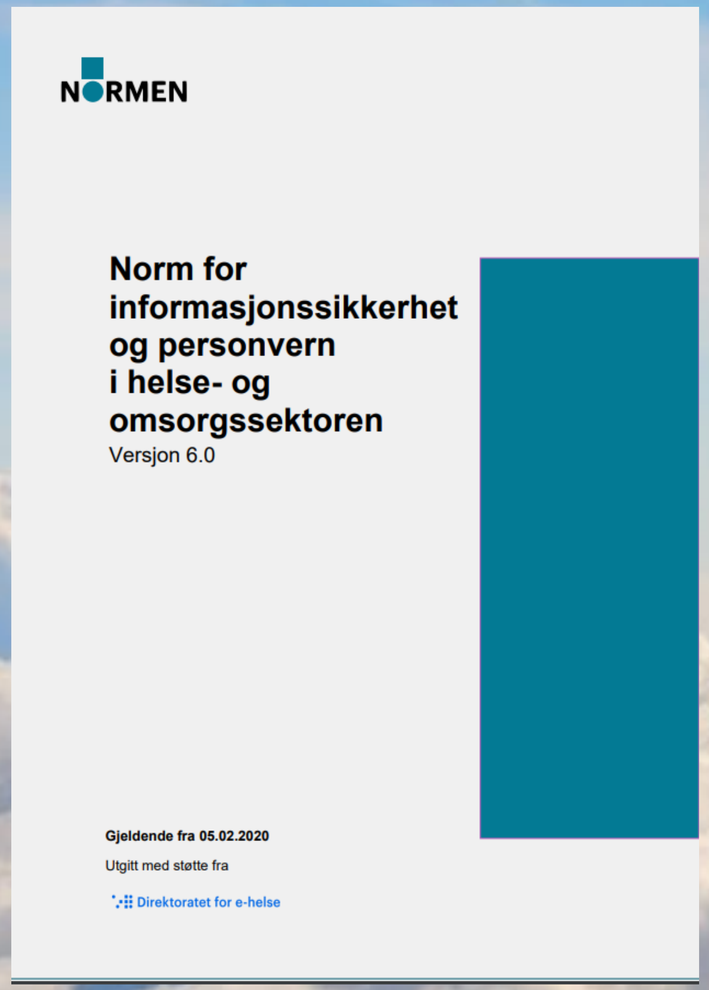
Kriterier og rutiner som bør implementeres i sektoren knyttet til:

- Sikre god og reell ledelsesforankring
- Tilstrekkelig kompetanse

- Helhetlig risikostyring

NORMEN

Om sky i Normen 6.0



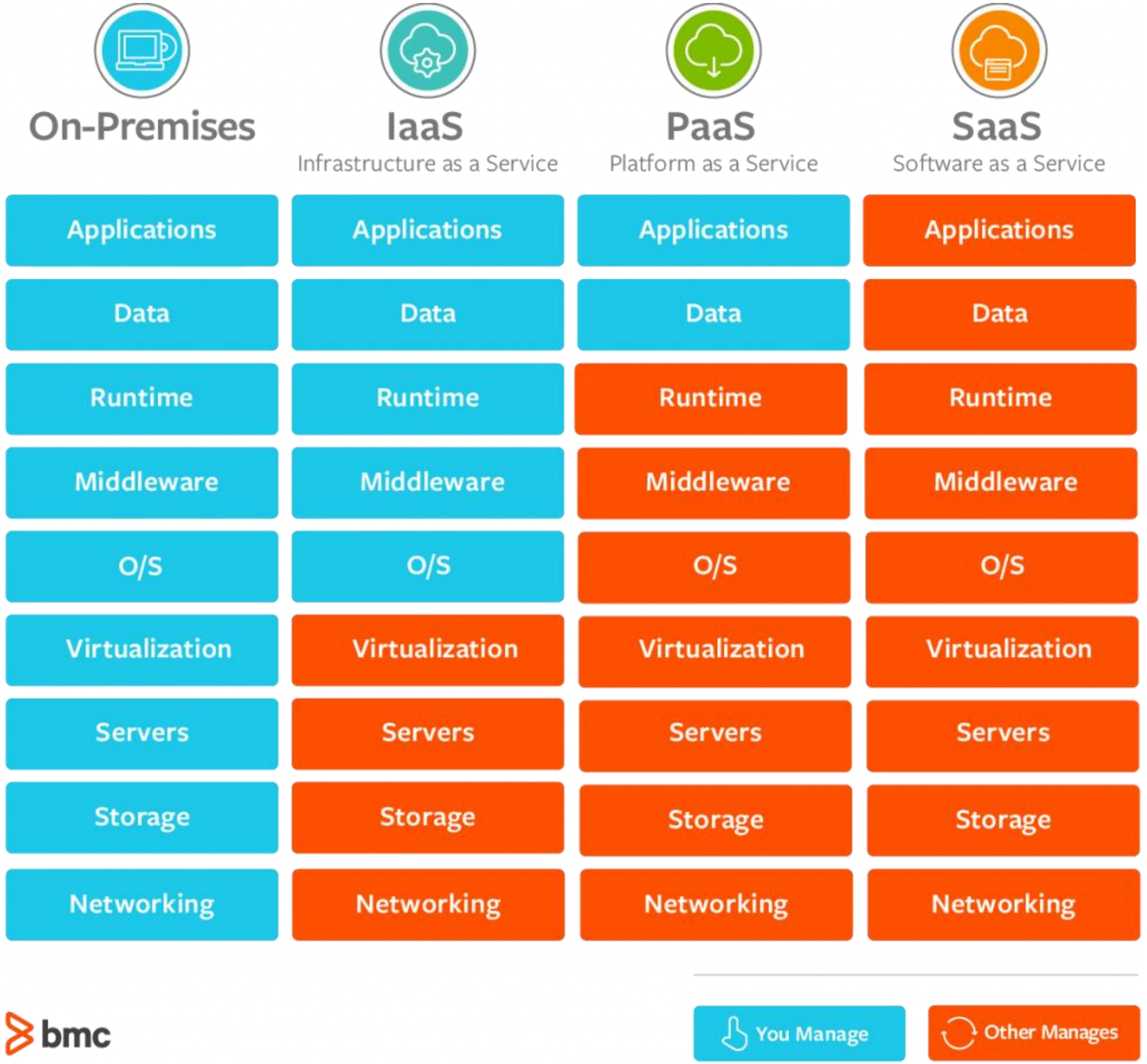
Noen grunnkrav

- 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

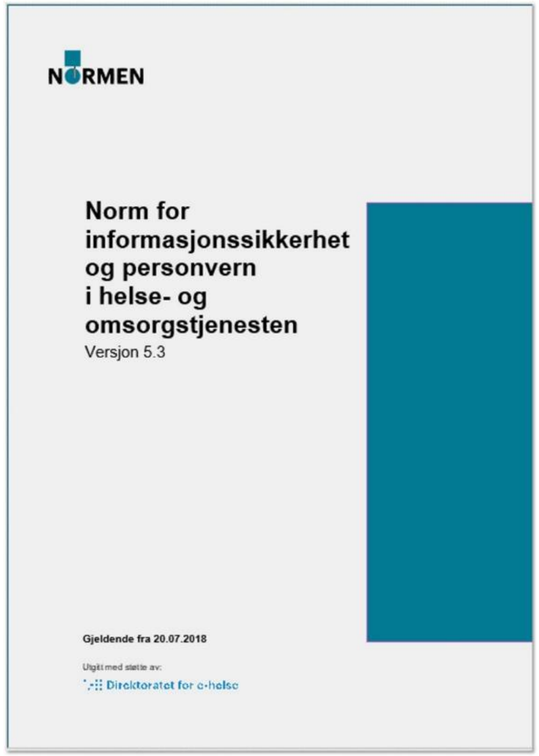
Ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset leveransemodellen som benyttes



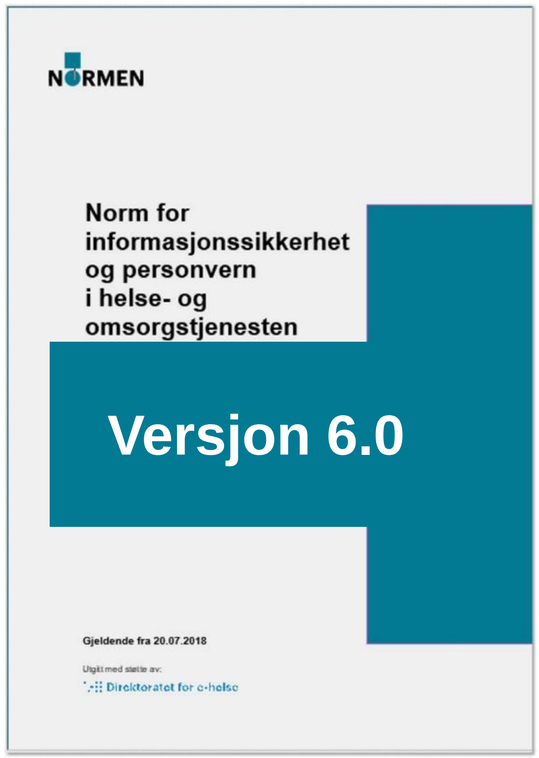
Dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med Normens krav

???

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

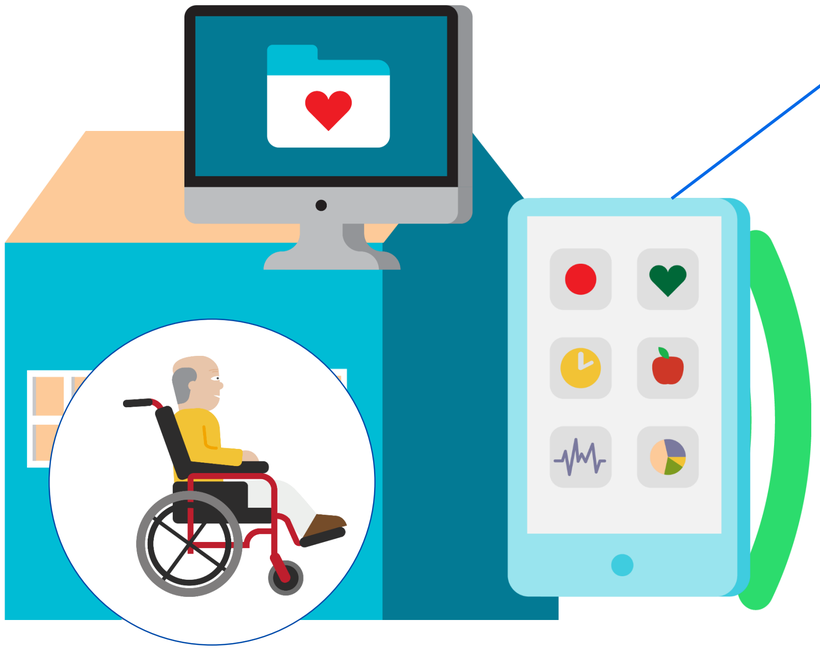
- Dataansvarlig skal sørge for å ha en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten

- 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.

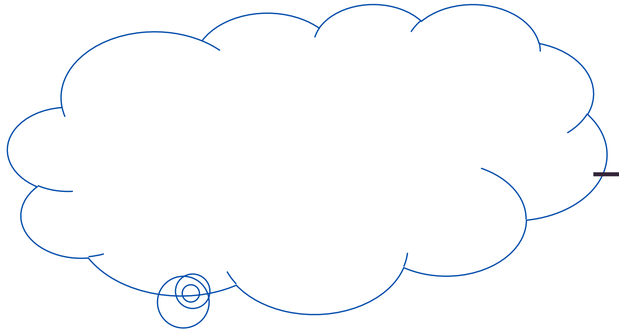
- Hvordan unngå lock-in?

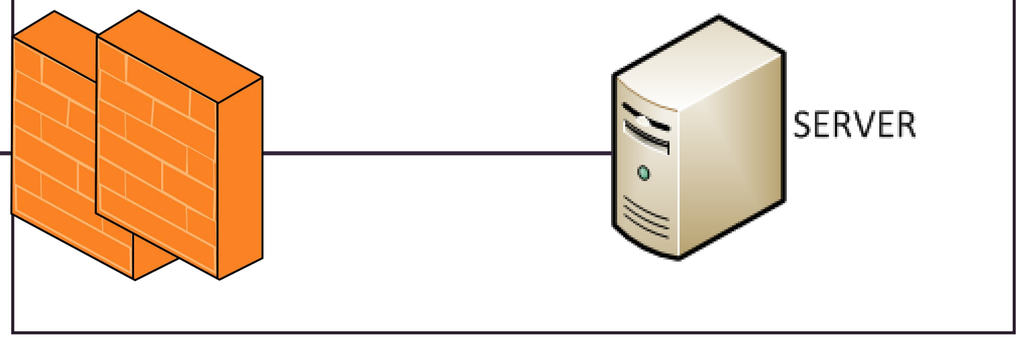
???

Leverandør
(f.eks utstyrsprodusent)



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

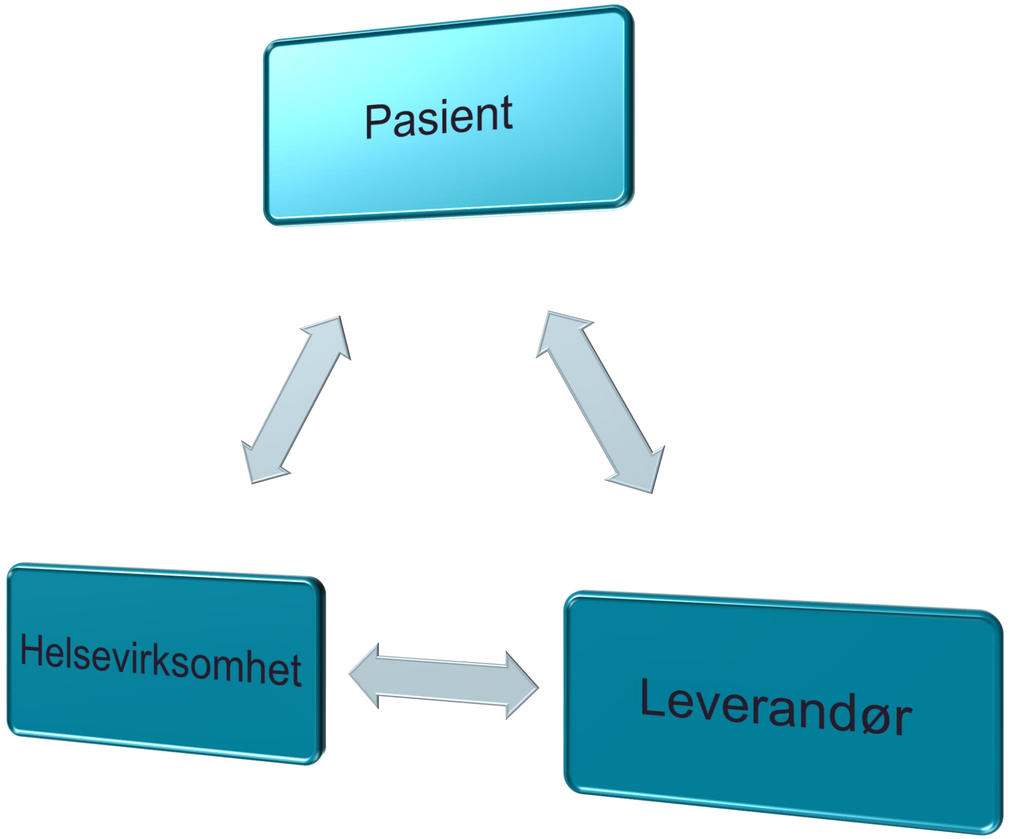




Når pasienten på egen hånd tar i bruk tjenester fra leverandøren?

- 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