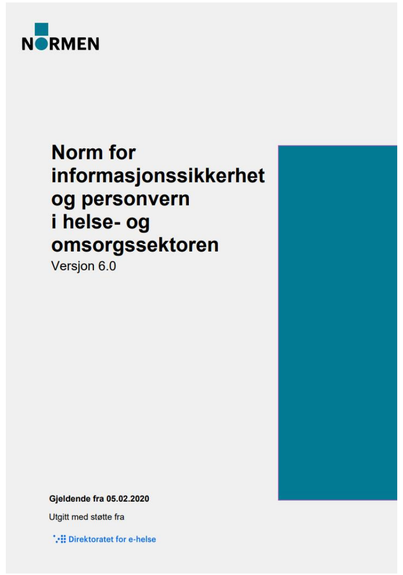
Noen utvalgte faktaark og veiledere

Oslo, 12.02.2020

Petter Ludvig Andersen
Direktoratet for e-helse, sekretariatet for Normen

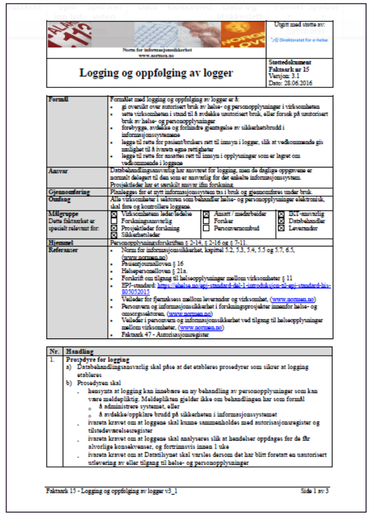
Norm for informasjonssikkerhet

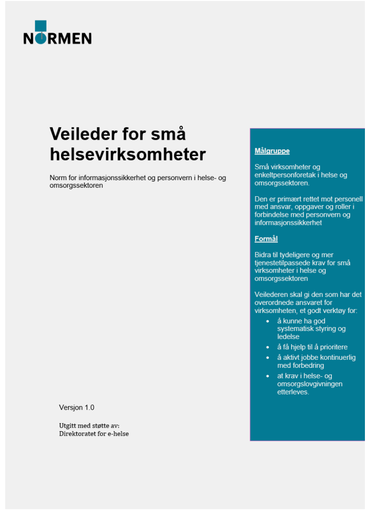


Bindende gjennom tilknytningsavtale med NHN

Veiledere
Faktaark

Ikke bindende





Normen (”Code of conduct”) og en del faktaark / veiledere er oversatt til engelsk

NORMEN

Innhold

- Normen.no
- Generelt om veiledere og faktaark
- Litt mer om følgende veiledere:
  - Veileder informasjonssikkerhet og personvern ved bruk av velferdsteknologi
  - Veileder med avtaleeksempler om samarbeid mellom virksomheter om felles journal
  - Veileder i bruk av skytjenester til behandling av helse- og personopplysninger
  - Veileder sosiale medier
- Litt mer om følgende faktaark:
  - Vedlegg – oversikt over Normens krav
  - Faktaark 27 (Retningslinjer for daglig informasjonssikkerhet)

Oppdatering veiledningsmateriell

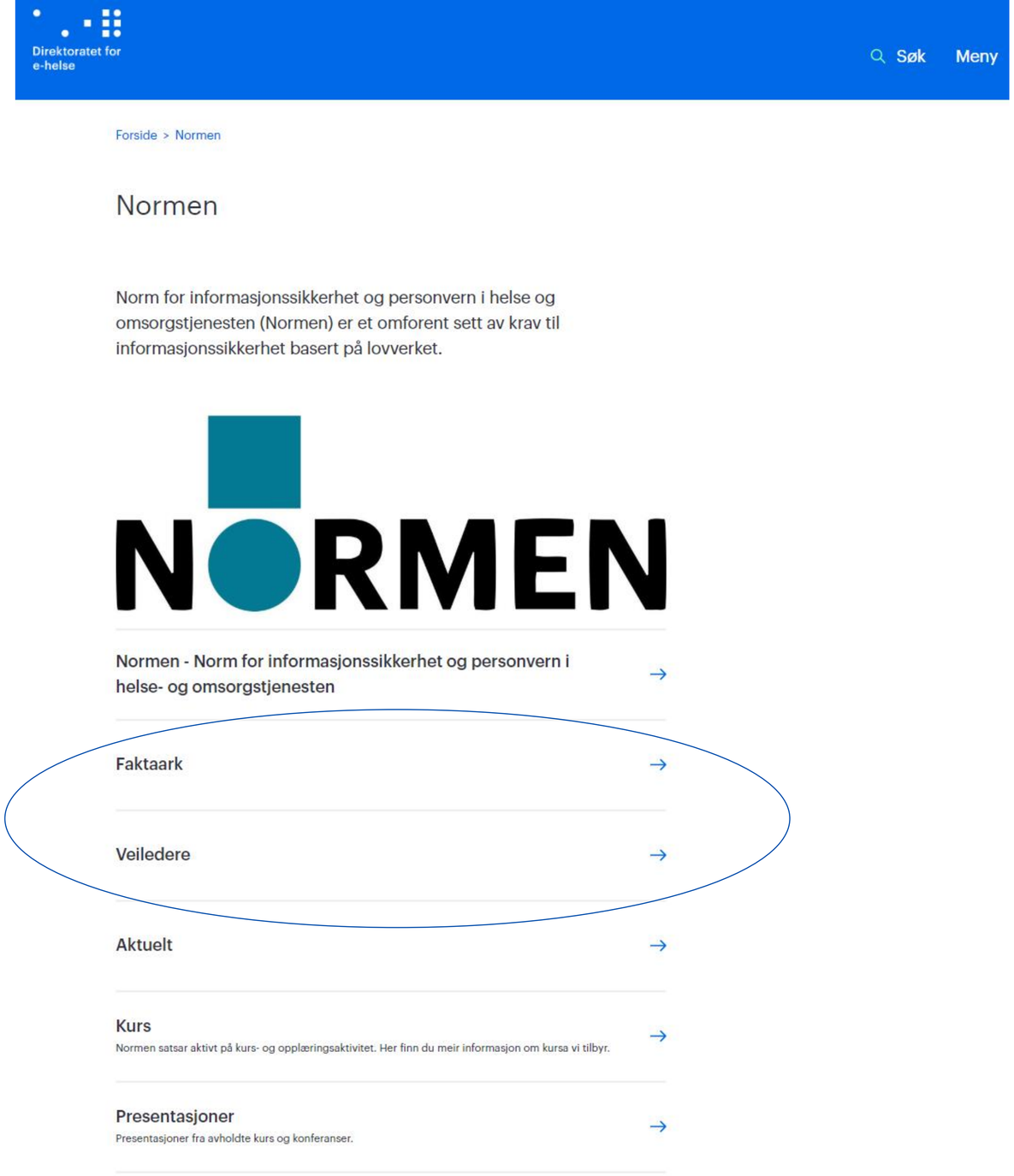
- Nytt materiell:
  - 55 – Sperret adresse i folkeregistret
  - Veileder små helsevirksomheter
- Pågående revideringer
  - Veileder om bruk av skytjenester
  - Veileder medisinsk utstyr
- Nylig publiserte versjoner det siste året:
  - 8 – Avviksbehandling
  - 13 – Oversikt over behandlinger av helse- og personopplysninger med vedlegg
  - 35 – Personvernombud
  - 2 – Styringssystem for informasjonssikkerhet og personvern (slått sammen med tidligere faktaark 3)

2020 er veiledningsmateriellets år!

- **Kommunepakke**
- **Tilgangsstyringspakke**
- **Personvernpakke**

NORMEN

Normen.no


Direktoratet for e-helse
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.
NORMEN
Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten
Faktaark
Veiledere
Aktuelt
Kurs
Normen satsar aktivt på kurs- og opplæringsaktivitet. Her finn du meir informasjon om kursa vi tilbyr.
Presentasjoner
Presentasjoner fra avholdte kurs og konferanser.

Normens veiledningsmateriell

- Krav til meldingsutveksling (Under revidering)
- Veileder for fjernaksess
- Veileder for forskning
- ~~Veileder for helse- og omsorgstjenester i kommuner~~ (Fjernet i påvente av revisjon)
- Veileder for små helsevirksomheter
  - Veileder for apotek
  - Veileder for legekontor
  - Veileder for psykologer, fysioterapeuter, manuellterapeuter og kiropraktorer
  - Veileder for tannhelsetjenesten
- Veileder i bruk av portalløsninger, sms og e-post
- Veileder i personvern og informasjonssikkerhet ved bruk av velferdsteknologi
- Veileder med avtaleeksempler ved samarbeid om felles journal
- Veileder sosiale medier
- Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter
- Veileder video-, lyd og bildeopptak i helse- og omsorgssektoren
- Veileder i bruk av skytjenester til behandling av helse- og personopplysninger
- Veileder i personvern og informasjonssikkerhet -medisinsk utstyr

Med maler for styringssystem tilpasset virksomhetstypen

Innhold i faktaark - tematisk inndelt

Styringssystem

01 - Ansvar og organisering

02 - Styringssystem for informasjonssikkerhet

04 - Kartlegge og klassifisere systemer

05 - Fastsette nivå for akseptabel risiko

06 - Sikkerhetsrevisjon

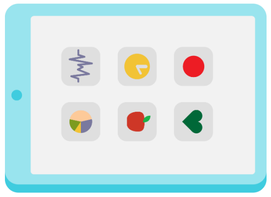
07 - Risikovurdering

08 - Avviksbehandling

13 - Oversikt over behandling av helse- og personopplysninger i virksomheten

37 - Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter

55 – Sperret adresse i folkeregistret



Behandling av helse- og personopplysninger

14 - Tilgangsstyring

15- Hendelsesregistrering og oppfølging

25- Lagringstid og sletting av helse- og personopplysninger

47 - Autorisasjonsregister

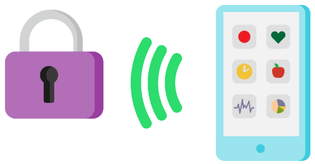
50 - Innsyn i hendelsesregistre

Databehandler / leverandør

10 - Bruk av databehandler

12 - Tilbakerapportering av resultater fra IT-driften

Innhold i faktaark - tematisk inndelt

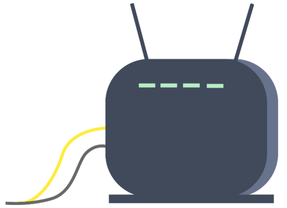


Tilgjengelighet og integritet

11 - Nødprosedyrer
53 - Tiltak ved konvertering og bytte av EPJ

Arkitektur og kommunikasjon

16 - Etablering av løsning for meldingskommunikasjon
20 - Sikkerhets- og samhandlingsarkitektur
21 - Sikkerhetskopi
26 - Sikring av trådløs teknologi
24 - Kommunikasjon over åpne nett
28 - Alternative tekniske løsninger for primærhelsetjenesten
36 - Fjernaksess mellom leverandør og virksomhet
49 - Krav ved bruk av PKI ved ekstern kommunikasjon



Fysisk / teknisk sikkerhet

17 - Fysisk sikring av områder og utstyr
18 - Sikring av bærbart utstyr
19 - Tiltak for å hindre ondsinnet programvare
29 - Hjemmekontor
30 - Sikring av mobilt utstyr utenfor virksomheten
31 - Passord og passordhåndtering
34 - Håndtering av lagringsmedia
52 - Krav til teknisk løsning ved bruk av betalingsterminal

Innhold i faktaark - tematisk inndelt

Forskning

23 - Avtaler og tillatelser vedrørende forskning
35 - Personvernombud
40 - Informasjonssikkerhet i forskningsprosjekter

Brukerrettet sikkerhet

09 - Opplæring av ledere og medarbeidere
27 - Retningslinjer for daglig informasjonssikkerhet

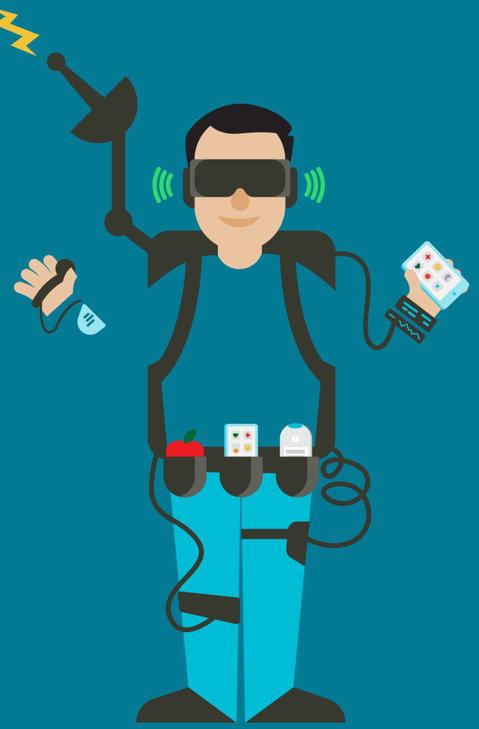
Test

43 - Bruk av testdata i systemer som inneholder helse- og personopplysninger
48 - Informasjonssikkerhet ved utførelse av testing

For kommuner

44 - Personvern og informasjonssikkerhet i helse- og sosialtjenesten - kortfattet oversikt for kommuneledelsen
45 - Personvern og informasjonssikkerhet - en kort orientering for det enkelte helse- og sosialpersonell i kommuner
46 - Databehandlingsansvar og avtaler i forbindelse med tjenesteutsetting

NORMEN



Veileder velferdsteknologi

Versjon 2.0

- Versjon 2.0 av veilederen med følgende endringer:
  - Behandler kun informasjonssikkerhet som er spesielt for velferdsteknologi
  - Personvern er tatt ut
  - Veilederen dekker ikke veiledning i juridiske problemstillinger (dokumentasjon, samtykke, helsehjelp eller ikke, hjemmel mv.)
  - Veilederen er strukturert som en tenkt prosess fra ide til anskaffelse i kap. 2
  - Fire nye eksempler
  - Tekst er skrevet om for å rendyrke det som er spesielt for velferdsteknologi og gi referanser til mer informasjon i faktaark og veiledere
  - Risikovurdering er framhevet
  - Personvernforordningen

Behovskartlegging

- Juridisk
  - Helsehjelp eller ikke? Vedtak?
  - Samtykke
  - Dokumentasjon
- Dataflyt - bevissthet
- Risikostyring – vurdering og håndtering
- Varierende kompetanse og bevissthet hos aktørene (både kommune og leverandør)
- Ulike roller
- Anskaffelser og krav – leverandøroppfølging
- Tilgangsstyring og brukerautentisering
- Medisinsk utstyr – behandlingshjelpemidler

NORMEN

Risikovurdering

- **All behandling av helse – og personopplysninger skal risikovurderes.**
- 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

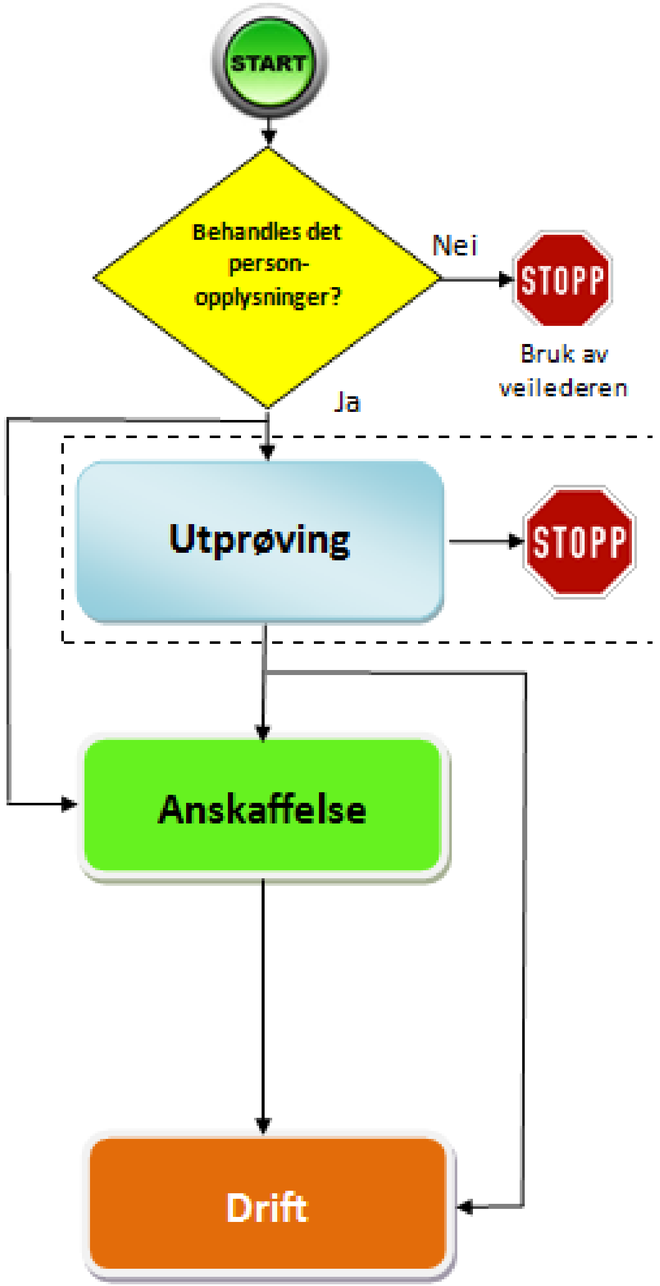
- **Uautorisert endring av helse- og personopplysninger og konfigurasjon ved tilgang fra eksterne nett (f.eks. Internett, trådløse nett og mobilnett)**

Konfidensialitet

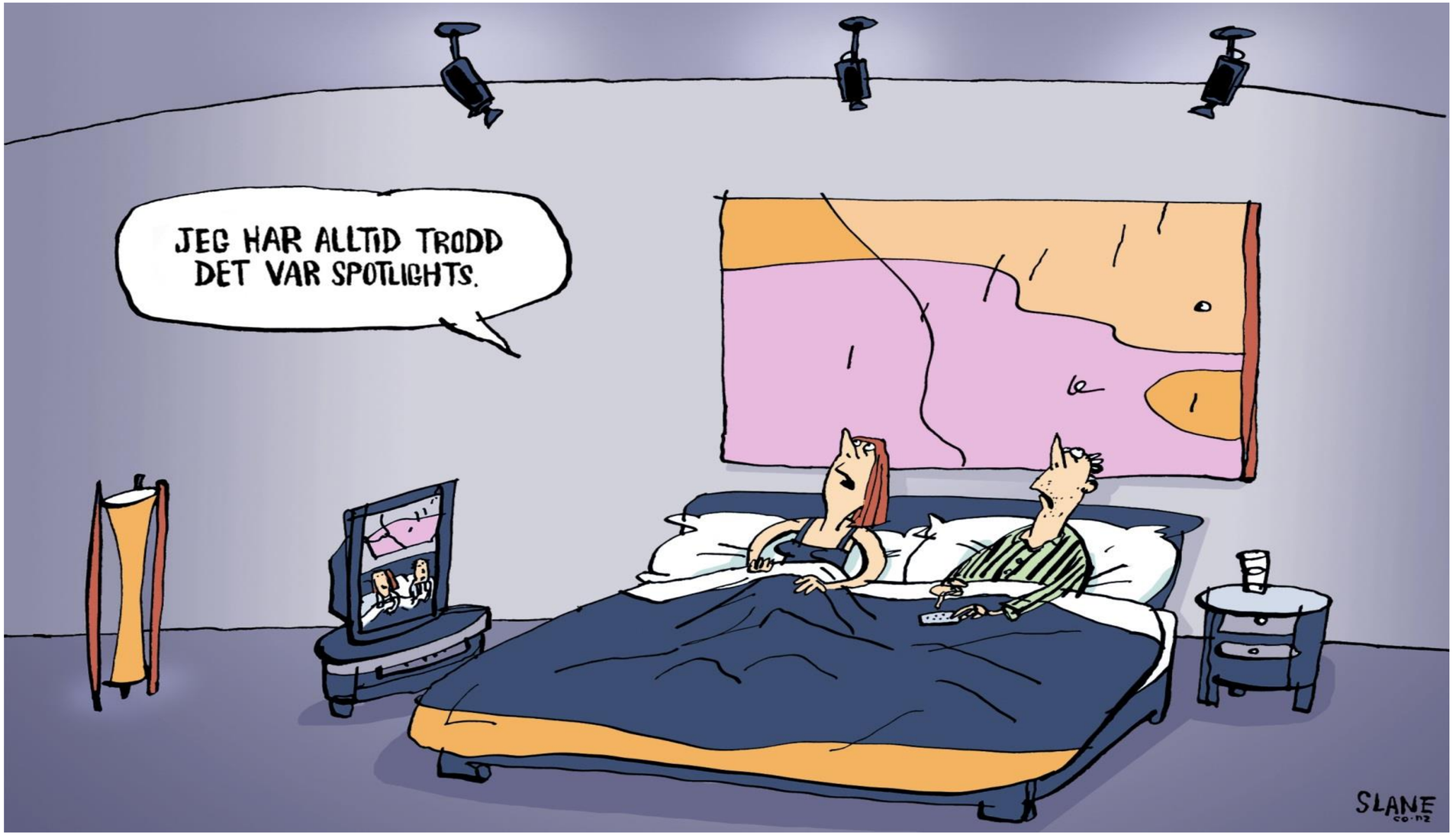
- **Tilgangsstyring hos bruker (f.eks. nettbrettet, rapporteringsløsninger, dørlåser, mv.)**
- **Leverandørs løsning for fjernaksess**

- Personvernkonsekvensvurdering – Personvernforordningen (GDPR)

Prosessorientert

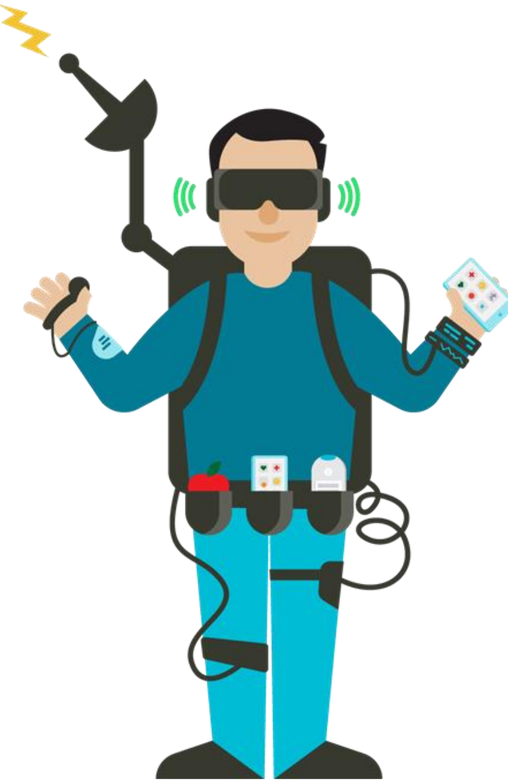


Utprøving



Anskaffelser

- Anbefalte krav til bruk ved kjøp av utstyr og tjenester
- Risikovurdering
- Databehandleravtaler



14.	29	Følgende skal som minimum registreres i logger: - entydig identifikator for den autoriserte brukeren - hvilke type opplysninger det er gitt tilgang til - hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer - grunnlaget for tilgangen - tidspunkt og varighet for tilgangen	5.5.2	☐Ja ☐Nei ☐ IR	
Integritet					
15.	36	Helse- og personopplysninger skal henføres til rett identifisert person	4.4.2	☐Ja ☐Nei ☐ IR	
Tilgjengelighet					
16.	Ingen	Batteritid skal varsles slik at batteri kan byttes tidsnok		☐Ja ☐Nei ☐ IR	
17.	Ingen	Utstyret sender "Heart-Beat" – for nedetidsovervåkning		☐Ja ☐Nei ☐ IR	
18.	Ingen	Kabler og tilkoblinger skal være sikret for utilsiktet frakobling		☐Ja ☐Nei ☐ IR	
Innebygget personvern					
19.		Systemets standardinnstillinger er på forhånd satt til å være mest mulig personvernvennlig		☐Ja ☐Nei ☐ IR	
20.		Utstyret innhenter kun nødvendige personopplysninger iht. det besluttede formålet		☐Ja ☐Nei ☐ IR	

Drift

Nr.	Tema	Ref. Kap.	Sjekk
1.	Plasser ansvar og etabler roller	6.1	☐ Ja ☐ Nei
2.	Oppdater styringssystemet for informasjonssikkerhet	6.2	☐ Ja ☐ Nei
3.	Oppdater oversikten over behandling av personopplysninger	6.3	☐ Ja ☐ Nei
4.	Gi opplæring	6.4	☐ Ja ☐ Nei
5.	Etabler / vedlikehold tilgangsstyring	6.5	☐ Ja ☐ Nei
6.	Vurder å slette overskuddsinformasjon	6.6	☐ Ja ☐ Nei
7.	Vurder lagringstid påopplysningene	6.7	☐ Ja ☐ Nei
8.	Gjennomfør logging	6.8	☐ Ja ☐ Nei
9.	Etabler og følg opp informasjonssikkerhetstiltak	6.9	☐ Ja ☐ Nei
10.	Gjennomfør avviksbehandling	6.10	☐ Ja ☐ Nei
11.	Rydd opp ifm. avvikling hos bruker	6.11	☐ Ja ☐ Nei

Drift – Oppdatere styringssystem (rutiner) og behandlingsoversikt

- Eksempel på rutiner
  - Håndtering av velferdsteknologien på mobilt datautstyr
  - Autorisasjon av bruker og pårørende
  - Prosedyre for sletting av data
  - Håndtering og sletting av overskuddsinformasjon
  - Tilbakestilling til fabrikkinnstillinger
  - ”Enkle driftsrutiner” for bruker (ladning, batteri, kabler, koblinger, reset, osv)
  - Avklare hvilke rutiner databehandler ivaretar (i og med at dette er komplekst vil det være nyttig at databehandlingsansvarlig vet hvilke rutiner databehandler ivaretar i den komplette løsningen)
  - Håndtering av feilmeldinger fra bruker
  - Driftsrutiner teknisk løsning (mange rutiner)
  - Opplæring av pårørende

Behandling:	Gi borger trygghetsalarm
Formål:	Kommunikasjon med responssenterløsning med hvem som har hvilken alarm og hvilken alarmsone de tilhører, registrering/ dokumentasjon av utløste alarmer og utrykninger, aktivitetsbaserte inntekter statistikk og styringsinformasjon
Hjemmel:	Helse- og omsorgstjenesteloven § 3-2, første ledd nr. 6 bokstav b
Databehandler:	Nei
Type opplysninger:	Helse- og personopplysninger

Eksempler og anbefalinger

- Privat bruk
- 4 eksempler
- Velferdsteknologiens ABC

Nr.	Problemstilling	Antatt risiko	Forslag til tiltak
1.	Medarbeider i responssenteret er ikke kjent med når kan de kan gå inn og sjekke koordinatene	Lav	Opplæring av medarbeiderne i korrekt uthenting av koordinater
1.	Hvem skal sjekke koordinatene?	Middels	Definer roller i responssenteret og før rollene opp i autorisasjonsregisteret
1.	Koordinatdata lagres til all tid	Høy	Erfaring tilsier at koordinater skal slettes etter 30 dager

- Vedlegg - Anbefaling til autentisering fra Nasjonalt velferdsteknologiprogram
  - Alternativ 1- Sikkerhetsnivå ¾
  - Alternativ 2 – Brukernavn/passord og offentlig/privat nøkkel
  - Alternativ 3 – Unik identifikator på utstyr

	Alternativ 1	Alternativ 2	Alternativ 3
Nettleser mot portalløsning	✓		
Smarttelefon/nettbrett med app	✓	✓	✓
Avansert maskinvare		✓	✓
Enkel maskinvare			✓

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

- et samarbeidsprosjekt!

https://vimeo.com/383994887

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

NORMEN

Deling av helseopplysninger

Felles journal
Rettslig grunnlag for felles journal – pasientjournalloven § 9

- Åpner for samarbeid mellom virksomheter om felles journal
- Krav om avtale
  - Hva samarbeidet omfatter
  - Hvordan pasientens rettigheter skal ivaretas
  - Hvordan helseopplysninger behandles og sikres – også ved endring/opphør
  - Dataansvar
- Samme ansvar for behandling av helseopplysninger for de virksomhetene som deltar i samarbeidet
- Hver virksomhet har selvstendig plikt til å oppfylle lovkravene
  - dataansvaret kan **ikke avtales bort**– ligger hos hver deltakende virksomhet, enten som flere selvstendige dataansvarlige, eller felles dataansvarlige

NORMEN

Tilgang på tvers – §19

- § 19.*Helseopplysninger ved helsehjelp*
- Innenfor rammen av taushetsplikten: sørge for relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell
  - Ved nødvendig for å yte, administrere eller kvalitetssikre helsehjelp
- Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten.
- Eksempler på behov som kan være aktuelle å vurdere:
  - *Pasienter* med forløp og overganger mellom spesialisthelsetjenesten, fastlege og den øvrige delen av den kommunale helse- og omsorgstjenesten
  - *Pasienter* som mottar helsehjelp ved flere *virksomheter*
  - *Pasienter* som mottar helsetjenester fra flere nivåer og over lengre tid
  - Akuttoppmøte av *pasienten* på legevakt hvor ordinær utredning og behandling er pågående i en annen *virksomhet*

Annet nyttig veiledningsmateriell

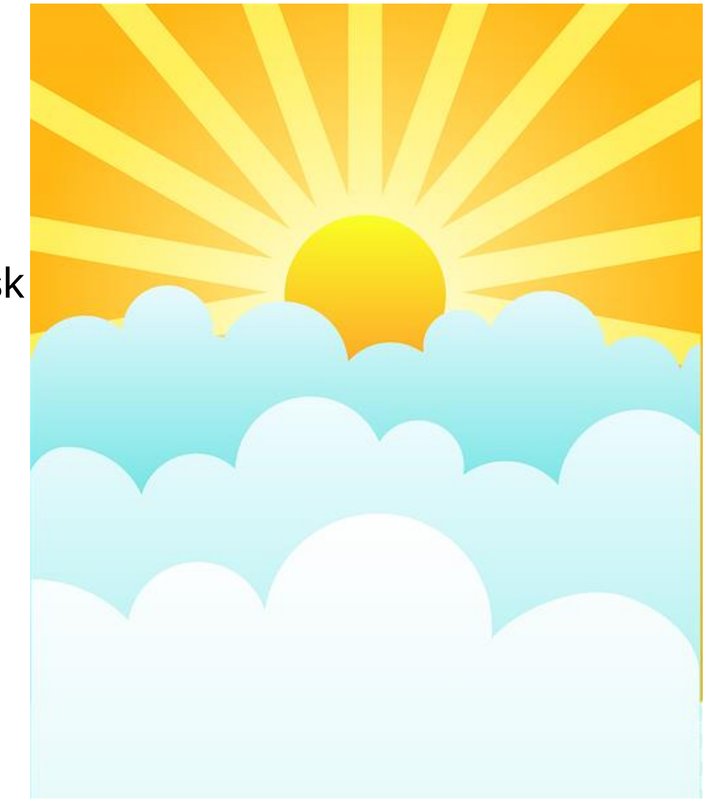
Veileder sosiale medier

- Praktisk verktøy når virksomheten skal utforme retningslinjer for bruk av sosiale medier
- Tre deler:
  - **Overordnede problemstillinger** ledelsen må ta stilling til
  - **Tekstforslag** ”Råd for bruk av sosiale medier for deg som jobber i <virksomheten>”
  - **Tekstforslag** ”Gode råd for bruk av sosiale medier for pasienter / brukere og deres pårørende”

Veileder i bruk av skytjenester til behandling av helse- og personopplysninger

Veilederen gir praktisk hjelp innenfor områdene:

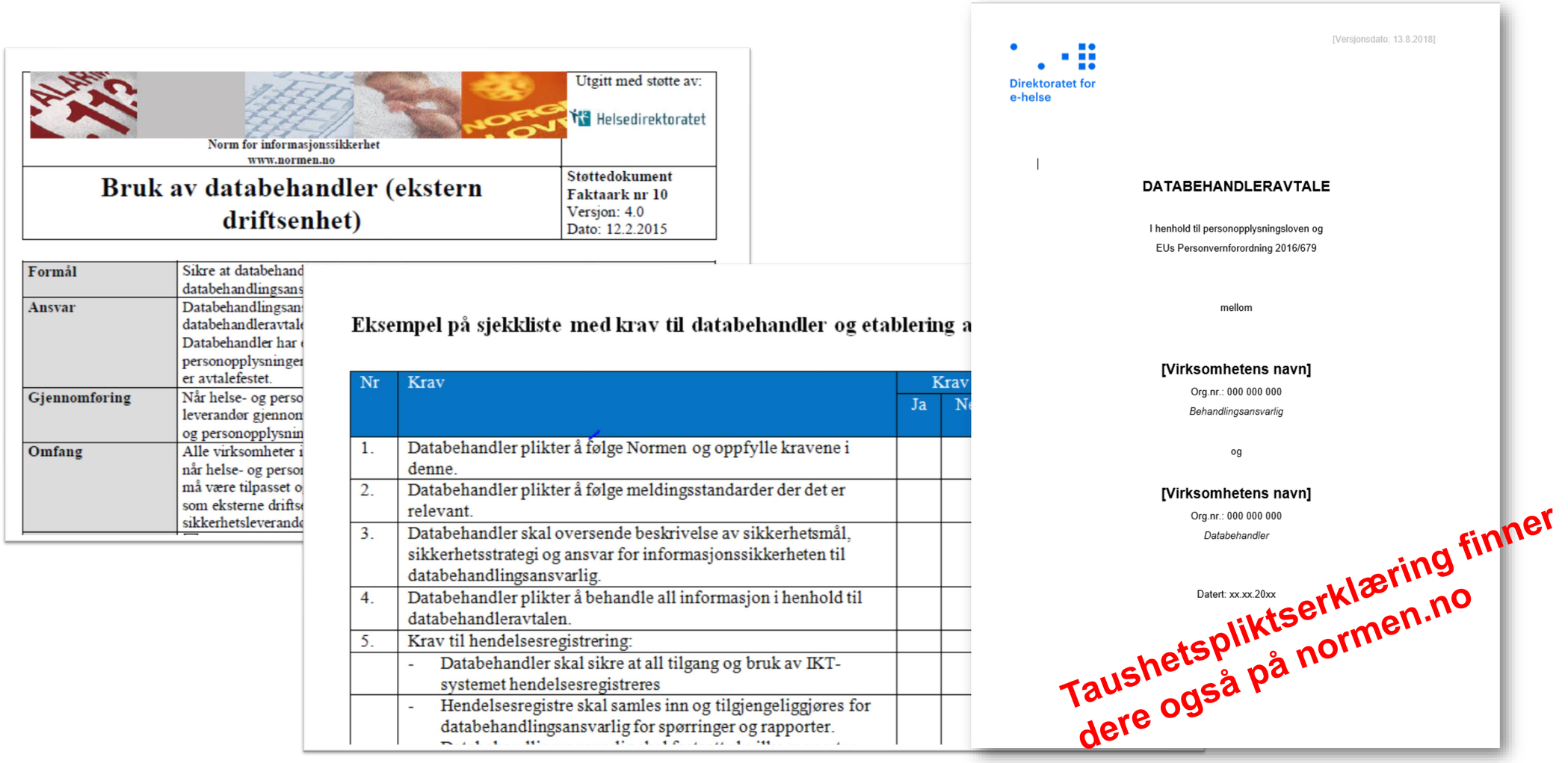
- Hva er sky? Modeller for skytjenester
- Fastsette ansvar, inngå avtaler, ivareta kontroll og vurdere risiko
- Belyse fordeler ved teknologien (sikkerhetskompetanse hos lev, skalerbarhet, fysisk sikring)
- Synliggjøre trusler og behov for kontroll
- Ivaretakelse av pasientens rettigheter til samtykke, innsyn, retting sletting mv.
- Eksempler på risikoområder som det er naturlig å belyse'
  - Leverandør har kontroll, lagring i utland



- Fra etablering til avvikling
  - Roller og ansvar
  - Etabler databehandleravtale
  - Overføring til utlandet
  - Arkivloven
- Sikkerhetstiltak
  - Tilgangsstyring
  - Hendelsesregistrering
  - Kryptering
  - Konfigurasjonskontroll
  - Pasientens rettigheter og personvern

NORMEN

Faktaark 10 – Bruk av databehandler



Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av: Helsedirektoratet

Bruk av databehandler (ekstern driftsenhet)

Støttedokument
Faktaark nr 10
Versjon: 4.0
Dato: 12.2.2015

Formål	Sikre at databehand databehandlingsans
Ansvar	Databehandlingsan databehandleravtal Databehandler har personopplysninger er avtalefestet.
Gjennomføring	Når helse- og perso leverandør gjennon og personopplysnin
Omfang	Alle virksomheter i når helse- og perso må være tilpasset o som eksterne drifts sikkerhetsleverand

Eksempel på sjekkliste med krav til databehandler og etablering a

Nr	Krav	Krav Ja	Krav N
1.	Databehandler plikter å følge Normen og oppfylle kravene i denne.		
2.	Databehandler plikter å følge meldingsstandarder der det er relevant.		
3.	Databehandler skal oversende beskrivelse av sikkerhetsmål, sikkerhetsstrategi og ansvar for informasjonssikkerheten til databehandlingsansvarlig.		
4.	Databehandler plikter å behandle all informasjon i henhold til databehandleravtalen.		
5.	Krav til hendelsesregistrering:		
	- Databehandler skal sikre at all tilgang og bruk av IKT-systemet hendelsesregistreres		
	- Hendelsesregistre skal samles inn og tilgjengeliggjøres for databehandlingsansvarlig for spørringer og rapporter.		

[Versjonsdato: 13.8.2018]

Direktoratet for e-helse

DATABEHANDLERAVTALE

I henhold til personopplysningsloven og
EUs Personvernforordning 2016/679

mellom

[Virksomhetens navn]
Org.nr.: 000 000 000
Behandlingsansvarlig

og

[Virksomhetens navn]
Org.nr.: 000 000 000
Databehandler

Datert: xx.xx.20xx

Taushetspliktserklæring finner dere også på normen.no

NORMEN

Faktaark 27 - Retningslinjer for daglig informasjonssikkerhet

- Kjøreregler for informasjonssikkerhet i praksis:
  - Passord
  - Tilgang til og bruk av pasientjournal
  - Logge av / låse pc
  - Pasientopplysninger på minnepinner o.l.
  - Kontroll på dokumenter
  - Du vet hva du kan og ikke kan lese

- Mal for sikkerhetsinstruks
  - Deling av pasientinformasjon
  - Pasientinformasjon på SMS eller på e-post
  - Sosiale medier
  - Avvik
  - Nettvett:
    Lenker og innhold i e post

Hva skjer videre i 2020

- Full revisjon av kommuneveiledning inkl. velferdsteknologiveilederen
- MU veilederen revideres nå! Ferdigstilles i løpet av våren
- Ny veiledning på personvern, bl.a. om personvernkonsekvensvurdering og behandlingsgrunnlag
- Tilgangsstyring
- Kurs – se www.normen.no om kurs!
- **Vi vil gjerne ha innspill fra deg**! Vil du være med i referansegruppe?, har du gode case?, innspill til hva som bør være med i veiledningsmateriell og kurs? Ta kontakt på sikkerhetsnormen@ehelse.no

Kapittel 2: Ledelse og ansvar

Takk for meg!

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