NORMEN

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

Versjon 2.0

31 oktober 2022

Publikasjonens tittel:
Veileder i bruk av skytjenester til behandling av helse- og personopplysninger

Versjonsnummer
2.0

Vedtatt av styringsgruppen for Normen:
27.04.2020

Gjeldende fra:
20.05.2020

Utgitt med støtte av:
Direktoratet for e-helse

Kontakt:
sikkerhetsnormen@ehelse.no

Publikasjonen kan lastes ned på:
www.normen.no

Forord

Skytjenester har etablert seg i markedet som en mulighet for å leie programmer og infrastruktur, som en tjeneste, i stedet for at virksomheten selv eier programmer og infrastruktur.

Skytjenester er tatt i bruk i helse- og omsorgssektoren. Denne veilederen gir råd, anbefalinger og praktiske eksempler innen personvern og informasjonssikkerhet ved bruk av skytjenester i sektoren.

Eksempler på områder, hvor bruk av skytjenester til helse- og personopplysninger er tatt i bruk, er:

- Journalsystemer for primærhelsetjenesten (f.eks. legekontor, tannklinikk, psykolog mv.)
- Velferdsteknologi, medisinsk utstyr og behandlingshjelpemidler
- Medisinsk avstandsoppfølging
- Mobilteknologi for å behandle helse- og personopplysninger
- Nettsteder for å involvere pasienten i behandling
- Ulike tjenester for spesialisthelsetjenesten

Denne versjon 2.0 av veilederen er overført til nytt design for veiledere og har fått en gjennomgående oppdatering iht. Normen 6.0. Noen tekstlige justeringer er tatt og alle referanser er oppdatert. Nye kapiteler i denne utgaven er:

- 2.3.3 DPIA ved skytjenester
- 2.3.4 Bruk av skytjenester i medisinsk avstandsoppfølging
- 3.4 Gjennomføring av DPIA
- 3.7.2 Bruk av Cloud Security Alliance (CSA)
- 5.2 Mapping Cloud Controls Matrix og Normen 6.0

Innhold

1 Innledning

1.1 Bakgrunn

Formålet med veilederen er å gi veiledning til etterlevelse av Normen ved bruk av skytjenester[1].

Punktene nedenfor viser noen eksempler på områder som kan være utfordrende for personvernet og informasjonssikkerheten ved bruk av skytjenester:

- Det kan være uklart hvem som er leverandøren med tilhørende ansvarslinjer
- Overføring av personopplysninger til utlandet og ivaretakelse av nåværende og fremtidige sikkerhetskrav etter Normen
- Dataansvarlig kan ha vanskeligheter med å få innsyn i hvordan tjenesten er sikret og forvaltet
- Sikring av opplysninger slik at disse ikke blir tilgjengelig for andre kunder av leverandøren
- Leverandøren av skytjenester bruker helse- og personopplysningene til kommersielle formål eller andre formål enn det som er avtalt og følger av instruksen fra dataansvarlig
- Den ansatte hos dataansvarlig benytter skytjenester som ikke er godkjent av virksomheten, for informasjonsdeling av virksomhetens helse- og personopplysninger
- Kontorstøttesystem levert som skytjeneste tas mer eller mindre uoverveid i bruk for behandling av helse- og personopplysninger
- Det kan være utfordrende å ha kjennskap til samtlige underleverandører som benyttes, noe som kan gi lange uoversiktlige verdikjeder
- Skytjenester utfordrer tradisjonelle sikkerhetsarkitekturer, ved at det kan innføres nye typer tiltak og produkter som utfordrer eksisterende kompetanse

Bruk av skytjenester kan også gi dataansvarlig støtte i å etterleve krav til informasjonssikkerhet. I kap. 2.4 blir fordelene beskrevet. Punktene nedenfor viser noen eksempler på områder som kan gi en positiv påvirkning (oppside) for personvernet og informasjonssikkerheten:

- Profesjonell ivaretakelse av informasjonssikkerheten
- Fleksibilitet og skalerbarhet på ytelsene
- Ikke behov for fysisk sikring av lokalt installerte servere
- Bedre tilgjengelighet, tilgangsmuligheter og ressurstilgang
- Ved bruk av PaaS (se kap. 2.2.1) vil leverandøren påse at de underliggende systemene alltid er oppdatert

Markedet for skytjenester er i kontinuerlig utvikling. Det anbefales på denne bakgrunn at den enkelte følger med og holder seg oppdatert.

[1] Med "skytjeneste" menes i denne veilederen en modell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som:
- er lett tilgjengelige over alt
- blir levert og priset etter behov (on demand)
- kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon eller involvering fra leverandøren

1.2 Leseveiledning

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
- Etabler databehandleravtale
- Behandling av helse- og personopplysninger under Normens virkeområde

Veilederen dekker ikke, eller i liten grad:
- Alminnelig bruk av Internett
- Generell bruk av skytjenester uten personopplysninger
- Konkrete produkter og tjenester som defineres som skytjenester
- Den forretningsmessige siden ved valg av leverandør og kontrakter
- Økonomiske sider ved skytjenester
- Sikring av annen informasjon som er viktig for virksomheten. F.eks. virksomhetskritisk informasjon, økonomisk informasjon, mv.
- Forholdet til arkivlovens regler om overføring til utlandet er ikke berørt

1.3 Om veilederen

Denne veilederen er et støttedokument under Normen, som forvaltes av styringsgruppen for Normen. Gjeldende versjon av Normen bygger på lov og forskrift og er à jour i forhold til gjeldende rett. Dette innebærer at Normen er kvalitetssikret mot gjeldende lovkrav.

Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den (jf. Normens kapittel 1.3). For virksomheter uten en slik avtale vil Normen være veiledende.

Normen gjelder fullt ut for alle som har avtale, uavhengig av hvor tjenesten driftes og med hvilken leverandør.

Veilederen har ikke som mål å gi veiledning i valg mellom ulike skytjenester. Ut fra dette vil veilederen ikke peke på konkrete kommersielt tilgjengelige skytjenester, annet enn som eksempler.

Faktaark som er referert til i veilederen, finnes på nettstedet til Normen.

Veilederen er utarbeidet for styringsgruppen for Normen med støtte av Direktoratet for e-helse og deltagere fra sektoren. Se kapittel **Feil! Fant ikke referansekilden.** - for deltagerne i referansegruppen. Kommentarer til veilederen kan sendes til: sikkerhetsnormen@ehelse.no.

1.4 Målgruppe

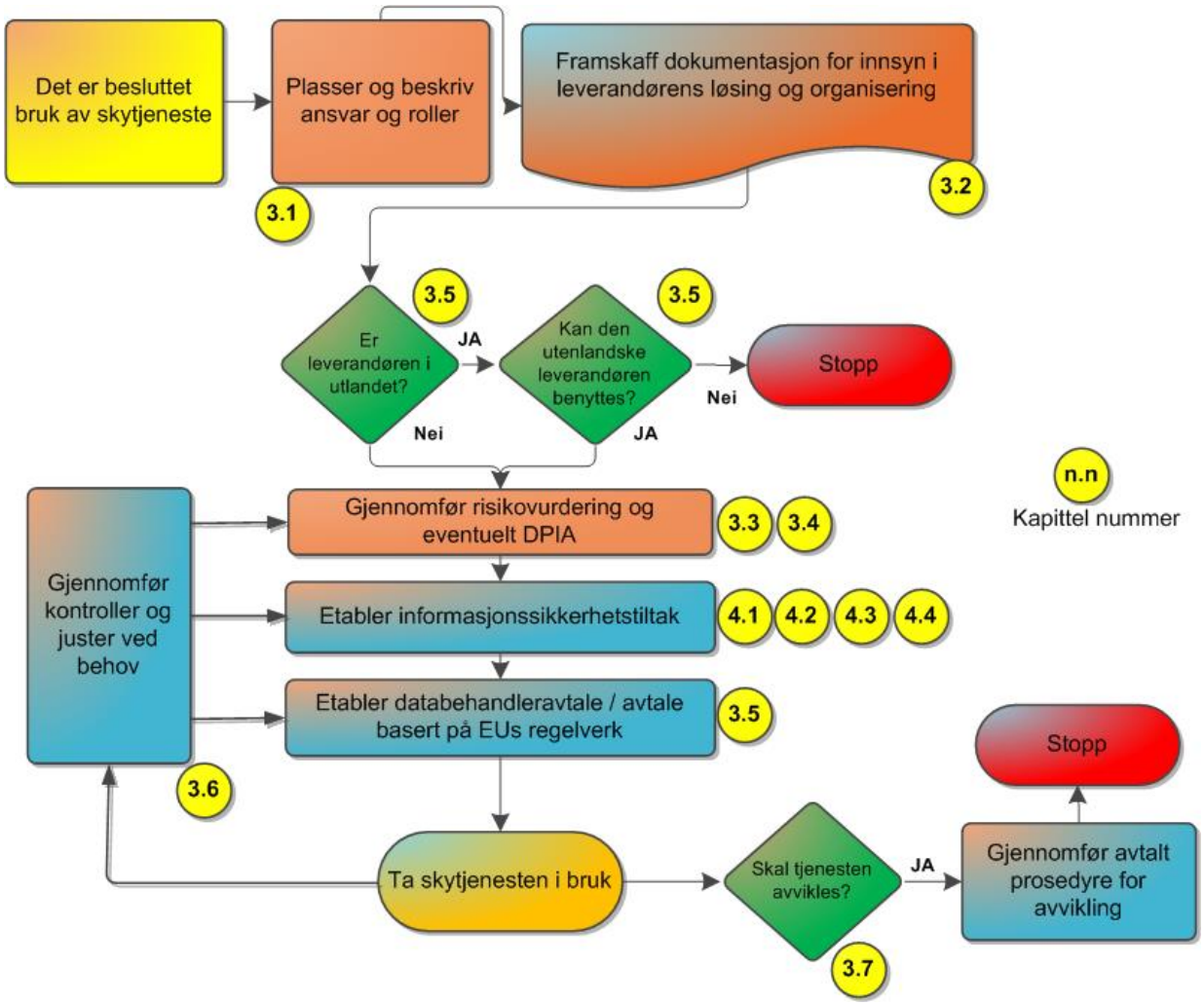
Målgruppen for veilederen er virksomheter som omfattes av Normen og som gjør bruk (eller planlegger å gjøre bruk) av skytjenester.

Følgende roller vil ha nytte av veilederen i den praktiske hverdagen:

- Virksomhetenes ledelse
- Databehandlingsansvarlig
- Leverandører (nettskytjenesteleverandør) / databehandler
- IKT-ansvarlig
- Sikkerhetsleder/ sikkerhetskoordinator
- Personvernombud
- Bestiller / innkjøpsfunksjon
- Systemeier
- Forskningsansvarlig og prosjektleder forskning
- Ansatte

1.5 Veilederens bruk og struktur

Figuren nedenfor gir veiledning til hvor i veilederen leseren kan finne krav og forslag til løsning i en tenkt prosess fra beslutning om bruk, til daglig drift og ved eventuell avvikling.



Veilederen har følgende kapittelinndeling:

Kapittel 1: Bakgrunn for og introduksjon til veilederen

Kapittel 2: Innføring i de ulike typene av skytjenester med eksempler fra helse- og omsorgssektoren. Beskriver risikoområder og fordeler med skytjenester

Kapittel 3: Beskriver ansvarsplassering, innhold i avtaler og kontrolltiltak

Kapittel 4: Beskriver tiltak innen informasjonssikkerhet

Kapittel 5: Inneholder definisjoner og referanser

2 Om skytjenester

2.1 Innledning

I dette kapitlet gis det først en innføring i begrep som karakteriserer skytjenester. Hvert av begrepene er supplert med en illustrasjon for å gi et eksempel på anvendelse. Deretter er det beskrevet noen trusler den dataansvarlig må ta hensyn til ved bruk av skytjenester. Til slutt i kapitlet er det gitt noen fordeler (gevinster) ved bruk av skytjenester.

En skytjeneste er en betegnelse for alt fra dataprosessering og datalagring til programvare på servere som står i eksterne serverparker, som vanligvis bruker Internett som bærer av datatrafikken.

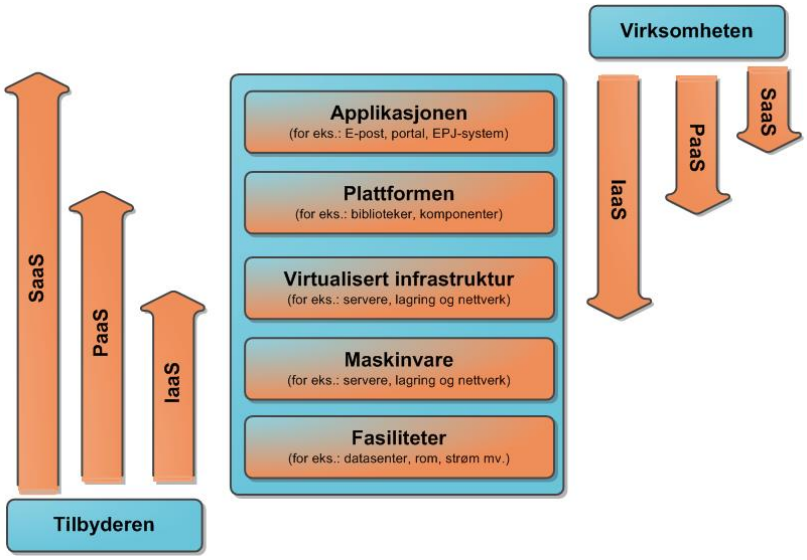
Tjenestene i skyen kjennetegnes ved at de er laget for dynamisk skalering ved kapasitetsbehov, og ved at det som regel betales for faktisk bruk. Leverandører tilbyr for eksempel serverkapasitet i skyen på timebasis.

Flere av tjeneste- og leveransemodellene for skytjenester er en form for tjenesteutsetting (outsourcing). Tjenesteutsetting er i bruk i stor grad i helse- og omsorgssektoren. En tradisjonell databehandler for drift av applikasjoner er et slikt eksempel på tjenesteutsetting.

Istedenfor å måtte kjøpe servere selv, kan virksomheten leie kapasitet ved behov. Virksomhetene trenger ikke å etablere egne dataløsninger og ha kompetanse til å forvalte disse.

2.2 Tjeneste - og leveransemodeller

Skytjenester finnes i ulike tjeneste- og leveransemodeller. Tjenestemodell er et begrep som benyttes på hvor mye av applikasjon og/eller infrastruktur som er med i tjenesten. Figuren[2] nedenfor viser graden av kontroll sett i lys av de ulike tjenestemodellene.



[2] Etter inspirasjon fra: https://csrc.nist.gov/publications/detail/sp/800-146/final

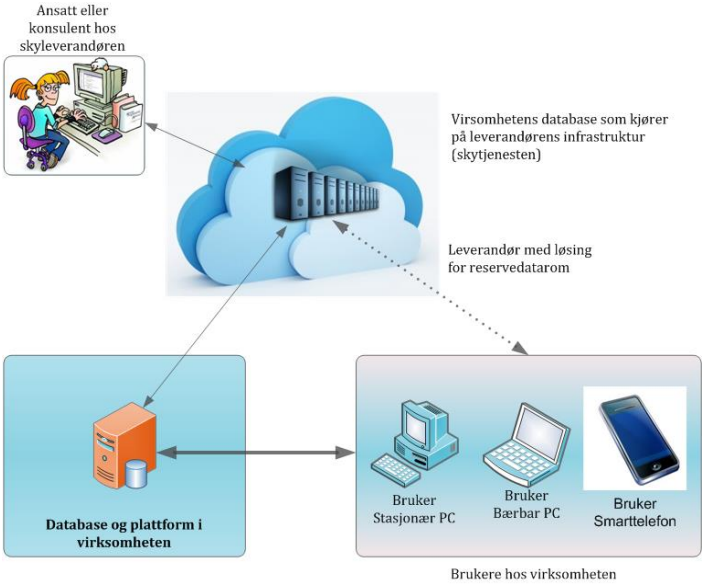
Med leveransemodell menes om skytjenesten kun er for virksomheten eller om den er delt med andre virksomheter i ulik grad. Tjenestemodeller og leveransemodeller er beskrevet i de følgende avsnittene.

2.2.1 Tjenestemodeller

1. **Infrastructure as a Service (IaaS)**: Tjenesten som tilbys virksomheten er ressurser til prosessering, lagring, nettverk. Virksomheten kan installere sine applikasjoner på leverandørens infrastruktur. Virksomheten kontrollerer ikke den underliggende infrastrukturen, men har kontroll over operativsystemer, lagring, applikasjoner som er tatt i bruk og kontroll på utvalgte nettverkskomponenter (f.eks. brannmurer som er dedikert til virksomheten).

   Eksemplet nedenfor illustrerer IaaS:

   Server og applikasjon eies og driftes av virksomheten i egne lokaler, mens det er etablert et reservedatarom som en tjeneste.

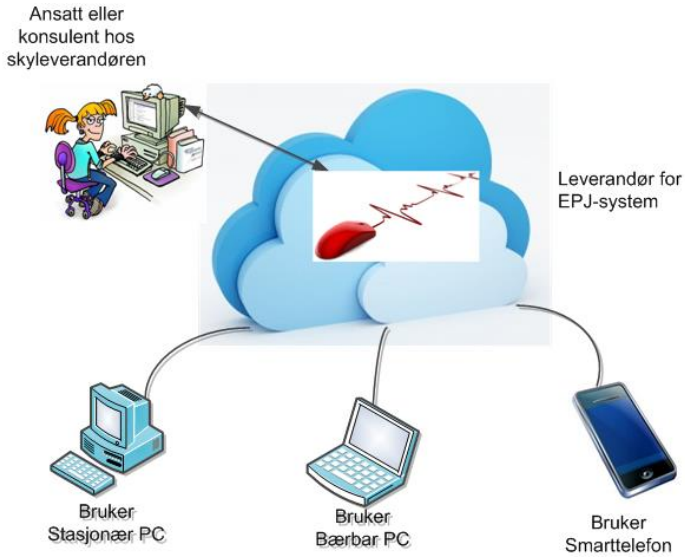


2. **Software as a Service (SaaS):** Leverandøren tilbyr tjenesten ved at applikasjonen kjører på en skyinfrastruktur. Applikasjonen kan være tilgjengelig fra ulike klienter som tynnklient, nettleser eller et program som installeres på virksomhetens infrastruktur. Virksomheten har ikke kontroll over applikasjonen og den underliggende infrastrukturen som nettverk, servere, operativsystemer, lagring mv.

   Det vanligste er at programvare som tilbys som en SaaS-tjeneste er tilgjengelig via Internett, som oftest via abonnement. Eksempler: Googles Gmail, Microsoft Office 365, Dropbox mv.

   Eksemplet nedenfor illustrerer SaaS:

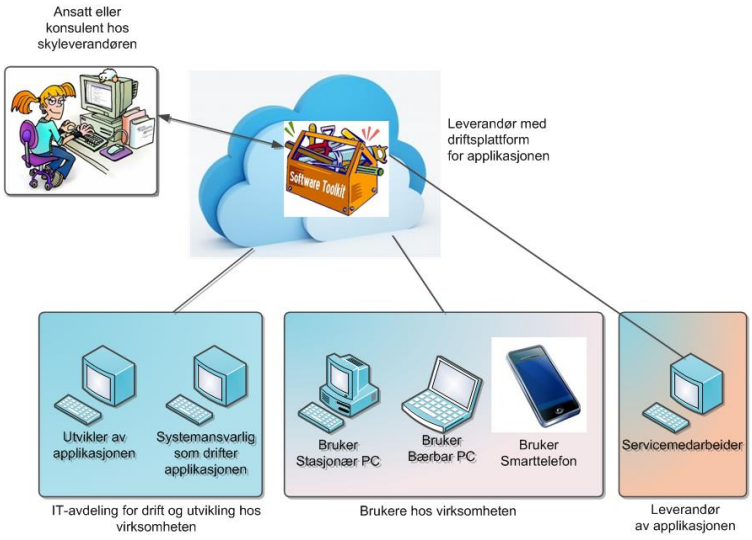
   Virksomheten leier system for EPJ. Brukerne kobler seg opp fra virksomhetens utstyr i lokalene og ved mobile løsninger til EPJ-systemet.



3. **Platform as a Service (PaaS)**: Tjenesten er tilgjengelig for virksomheten ved å ta i bruk skyinfrastrukturen med virksomhetens egenutviklede eller ervervede applikasjoner ved bruk av leverandørens utviklingsverktøy (plattform), biblioteker, tjenester og komponenter. Virksomheten kontrollerer ikke den underliggende skyinfrastrukturen som nettverk, servere, operativsystemer og lagring. Men virksomheten har kontroll på applikasjonene som tar i bruk PaaS-tjenesten.

   <u>Eksemplet nedenfor illustrerer PaaS:</u>

   Driftsplattformen eies av leverandøren, og gjøres tilgjengelig via Internett. Kunden har selv ansvar for å drifte programvare på plattformen, mens leverandøren drifter infrastruktur, operativsystem, database og webserver.

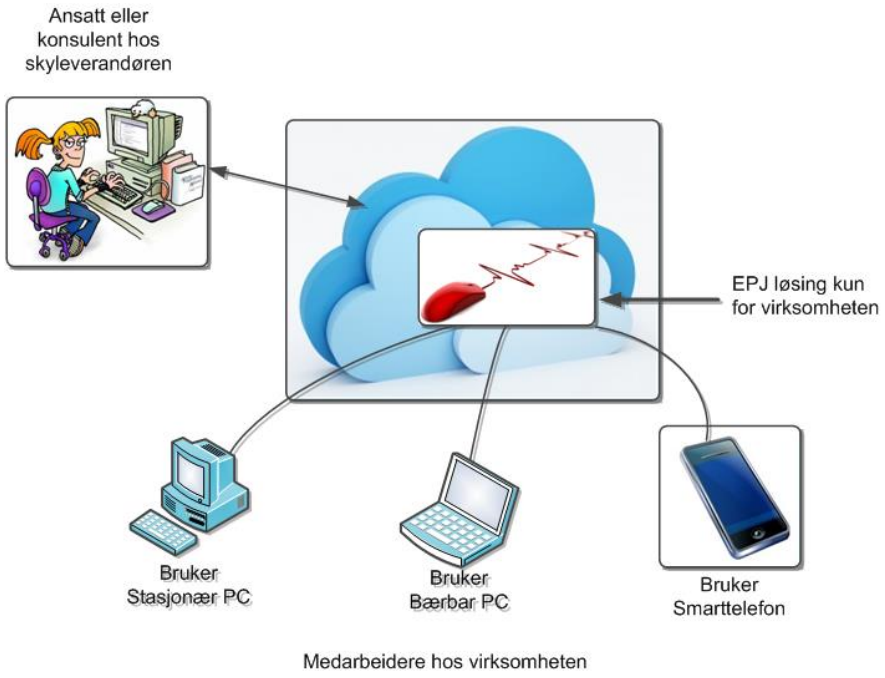


2.2.2 Leveransemodeller

1. **Privat sky (Private cloud)**: Sky-infrastrukturen er tilbudt eksklusivt for en virksomhet. Den kan være eiet, kontrollert og driftet av virksomheten (og være i eget datasenter som tar i bruk prinsippene for skytjenester), en tredjepart, eller en kombinasjon av disse.

   Eksemplet nedenfor illustrerer privat sky:

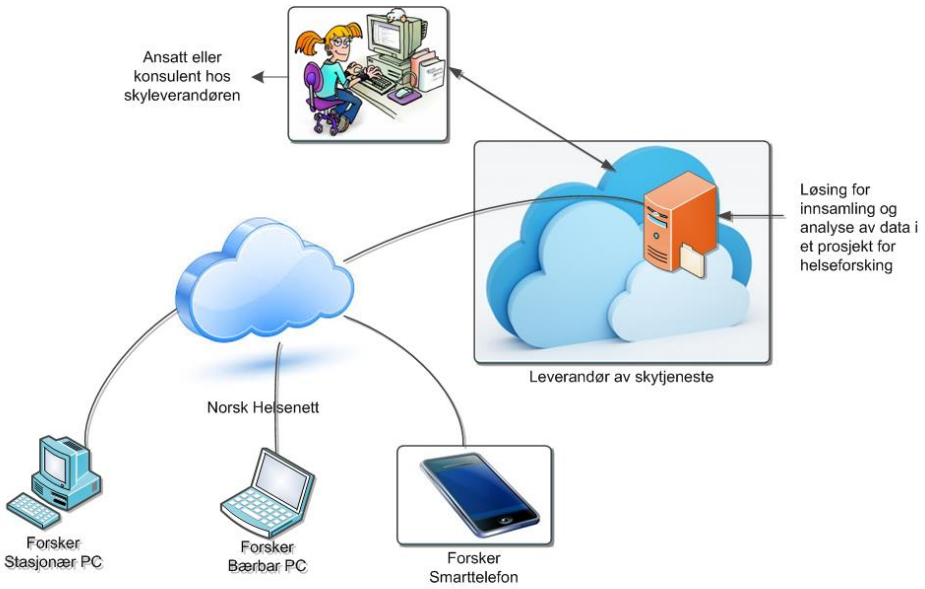
   Virksomheten leier EPJ-system som er tilbudt kun for virksomheten.



2. **Fellesskap sky (Community cloud)**: Infrastrukturen er tilbudt eksklusivt for et fellesskap av virksomheter som har de samme utfordringer (for eksempel formål, sikkerhetsbehov, policy og krav til etterlevelse av regulatoriske bestemmelser). Den kan være eiet, kontrollert og driftet av en eller flere av virksomhetene, en tredjepart, eller en kombinasjon av disse.

   Eksemplet nedenfor illustrerer fellesskap sky:

   Virksomheten leier system for analyse av data som er tilbudt for mindre virksomheter i helsesektoren. Datasystemet er plassert på innsiden av Norsk Helsenett. Leverandøren er en tredjepartsleverandør i Norsk Helsenett.

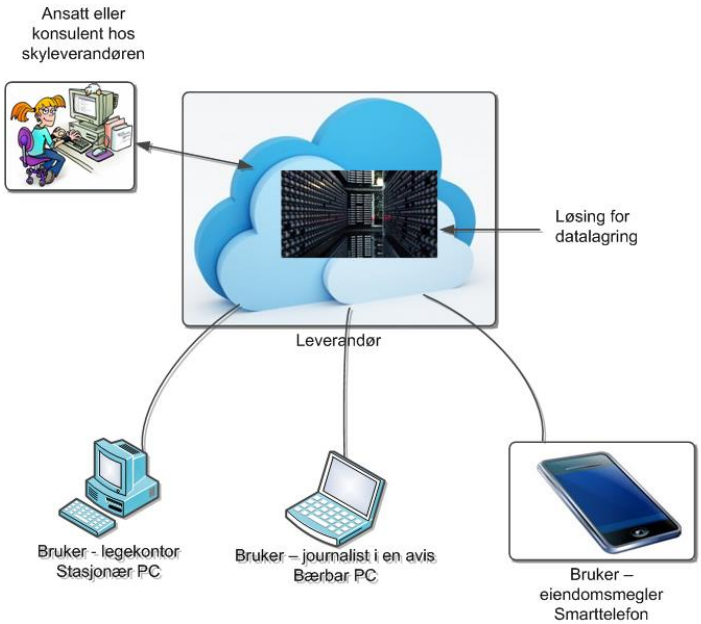


Forskere som er tilknyttet helseforskingsprosjektet

3. **Allmenn sky (Public cloud)**: Infrastrukturen er tilbudt for åpen bruk for alle virksomheter og privatpersoner. Siden tjenesten er åpen for alle, krever det særlig aktsomhet ved profesjonell bruk (jf. legekontoret i figuren nedenfor). Den kan være eiet, håndtert og operert av en kommersiell, akademisk, ideell eller offentlig organisasjon eller en kombinasjon av slike. Applikasjon og infrastruktur er iht. premissene fra leverandøren.

   Eksemplet nedenfor illustrerer allmenn sky:

   Virksomheten leier system for datalagring av ikke sensitive personopplysninger som er tilbudt for enhver som måtte ønske å benytte løsningen. Virksomheten deler datalagring med et ukjent antall andre aktører.



4. **Hybrid sky (Hybrid cloud)**:

For alle praktiske formål vil de fleste skytjenestene være en miks av de definerte tjeneste- og leveransemodellene ovenfor. Dette er også den mest vanlige modellen. En hybrid skytjeneste kan være en kombinasjon av en privat sky, allmenn sky eller felles sky. En hybrid sky er en spesielt aktuell modell for virksomheter som behandler data av ulik karakter og som møter ulike regulatoriske krav til behandlingen av disse.

2.3 Risikostyring ved skytjenester

I dette kapitlet belyses risiko- og trusselområder som er spesielle for kontroll og styring av skytjenester.

Først beskrives noen generelle risikoområder. Deretter blir spesifikke risikoområder for de ulike tjeneste- og leveransemodellene beskrevet.

Risikoområder som er beskrevet i dette kapitlet er ikke uttømmende. Den aktuelle situasjonen i virksomheten og hos leverandøren kan medføre andre problemstillinger innenfor de områdene som er beskrevet. Situasjonsbildet for trusler knyttet til tjenester som benytter Internett, endres raskt og kan gi nye eller endrede trusler som kan innebære risiko.

2.3.1 Generelle risikoområder

Skytjenester kan være etablert på tvers av flere land og det kan være vanskelig å ha oversikt over hvilke land som er involvert. Dette kan gi et komplekst bilde selv om det alltid er norsk rett som gjelder. Utfordringene kan være på områder som sikring, generell behandling, innsyn, logger, lagring, sletting mv. av helse- og personopplysninger. Andre problemområder er ansvars- og risikofordeling, og rolledeling mellom virksomhet, leverandør og underleverandør. Dette kan ofte være en kjede på tvers av landegrenser som det fort kan bli komplisert og vanskelig å holde oversikt over. I de forskjellige tjeneste- og leveransemodellene kan det være ulike grader av sikkerhetsutfordringer. Se kap. 3.6 for mer om overføring av personopplysninger til utlandet.

Det finnes flere eksempler på områder som kan utgjøre en trussel:

- Virksomheten mister kontroll på helse- og personopplysningene ved at leverandøren behandler opplysningene på annen måte eller til andre formål enn det som er avtalt med og følger av instruksen fra dataansvarlig.
- Ved bruk av skytjenester kan det produseres mer overskuddsinformasjon som benyttes til andre formål
- Leverandøren selger eller uautorisert deler data/informasjon til kommersielle formål. Denne type risiko vil også være knyttet til annen form for tjenesteutsetting
- Leverandør behandler helse- og personopplysningene i strid med databehandleravtalen Leverandøren benytter eller skifter underleverandører som ikke meldes til virksomheten. Virksomheten skal vite hvem som er involvert i behandling av helse- og personopplysninger.
- Leverandører presser fram avtaletekster som ikke følger opp personvernforordningen.
- Skytjenesten er av en slik karakter at virksomheten er innlåst i leverandørens løsning der det er krevende eller umulig å skifte fra en leverandør til en annen.
- Avhengighet mot leveranser fra annen skyleverandør (f.eks lisenser på produkter)

2.3.2 Risikoområder for tjeneste- og leveransemodellene

Tabellene nedenfor beskriver risikoområder knyttet til tjeneste- og leveransemodellene som er beskrevet i kap. 2.2.

Tjeneste-modell	Risikoområder (**K**onfidensialitet, **I**ntegritet, **T**ilgjengelighet)
SaaS	- (**K,I**) Trussel mot konfidensialitet og integritet om skytjenesten ikke separerer de ulike kundene på en tilstrekkelig måte slik at uautoriserte kan få innsyn og / eller kan endre helse- og personopplysninger - **(K,I,T)** Virksomheten har svært begrenset kontroll på tjenesten slik at det stiller store krav til innsyn i leverandørens dokumentasjon
PaaS	- **(I)** Virksomheten har ikke kontroll på underliggende plattform slik som utviklingsverktøy, databaser og biblioteker - **(K)** Kan føre til at integrasjoner med applikasjoner i virksomheten eksponerer virksomheten for ikke-akseptabel risiko
IaaS	- **(K,I,T)** Virksomheten har ikke kontroll på den underliggende infrastrukturen - **(K,I)** Virtuelle og fysiske maskiner, lagringssystemer, system for sikkerhetskopiering og nettverkskomponenter kan være delt med andre - **(K,I,T)** Konfigurasjonsfeil eller for svak konfigurasjonsstyring kan føre til uautorisert innsyn og tilgang mellom ulike virksomheters opplysinger og konfigurasjoner

Leveranse-modell	Risikoområder (**K**onfidensialitet, **I**ntegritet, **T**ilgjengelighet)
Privat sky	- **(K,I,T)** Løsningen gir presumptivt lavest risiko ved at virksomheten har større grad av kontroll - **(K,I)** Infrastrukturen som applikasjonen og databasen kjører på kan i noen tilfeller være delt med andre kunder. For svak konfigurasjonskontroll hos leverandøren eller feil i programvaren kan medføre lekkasje mellom virksomhetene
Felles sky	- **(K,I,T)** Løsningen vil ha et høyere risikonivå enn for privat sky fordi det er flere virksomheter som deler skytjenesten. - **(K,I)** Andre strekpunkt under privat sky vil også gjelde for denne tjenesten, men kan gi et høyere risikonivå
Allmenn sky	- **(K,I,T)** Løsningen medfører det høyeste risikonivået fordi tjenesten er delt med alle andre virksomheter, bransjer og land. Både private og offentlige virksomheter - **(K)** Mange allmenne skytjenester tilbys gratis. Det kan være grunn til å anta et høyt risikobilde ved at virksomhetens opplysninger kan være eksponert for salg i kommersiell interesse

2.3.3 DPIA ved skytjenester

Virksomheten skal selv foreta en vurdering om det er nødvendig å gjennomføre en DPIA (personvernkonsekvensvurdering) når skytjenester skal tas i bruk ved behandling av helse- og personopplysninger. Hovedregelen er at det skal gjennomføres når risikoen er vurdert til høy. Det anbefales å konsultere Datatilsynets veileder som underlag/sjekkliste i beslutningen om virksomheten må gjennomføre en DPIA.

Datatilsynet har laget en liste over behandlingsaktiviteter som alltid krever at det gjennomføres en personvernkonsekvensvurdering. Denne må konsulteres om det skal gjennomføres DPIA ifm. å ta i bruk skytjenester.

Veileder og listen finnes hos Datatilsynet.

2.3.4 Bruk av skytjenester i medisinsk avstandsoppfølging

Virksomheter som yter helse- og omsorgstjenester tilbyr i større grad tjenester hjemme hos pasient/ bruker enn tidligere. I slike tjenester er det vanlig å bruke en eller annen form for skytjeneste. Dette kan skje på forskjellige måter. Enten ved at pasient rapporterer data i form av skjemaer, eller ved å kombinere et medisinsk utstyr eller velferdsteknologi med en skytjeneste hvor data kan sendes direkte fra utstyret via eller til skytjenesten hvor kan lagres og/eller sendes over til dataansvarlig og lagres i et behandlingsrettet helseregister (f.eks. pasientjournal).

De generelle risikoområdene i kapittel 2.3.1 gjelder også her, men det i tillegg noen særlige risikoområder som bør belyses når virksomheten tilbyr medisinsk avstandsoppfølging (digital hjemmeoppfølging mv.):

- Det er utfordringer med sikker autentisering, særlig blant pasientgrupper med kognitiv svikt.
- Leverandør pre-prosesserer og mellomlagrer data i skyen før data overføres til dataansvarlig. Det er viktig at databehandleravtalen dekker slike behandlinger, og særlig hvor flere underleverandører har tilgang til dataene.
- Det samles inn overskuddsinformasjon som ikke nødvendigvis er begrenset til det som er nødvendig for formålene de er samlet inn for. Disse kan bli liggende lagret i skytjenesten. Det er viktig med dekkende sletterutiner og eget behandlingsgrunnlag dersom overskuddsinformasjonen[3] benyttes videre.
- Leverandør tilbyr i økende grad tilleggsfunksjonalitet til utstyret (f.eks en egen brukerkonto med ytterligere informasjon og funksjonalitet til pasient/bruker). Det kan være tilfeller hvor tilleggsfunksjonalitet tilbys uten at dette er kjent eller avtalt mellom dataansvarlige virksomhet og leverandør. Data som samles inn fra pasient/bruker som benyttes til andre formål enn det de samles inn for kan føre til utilsiktede hendelser som f.eks. utilsiktet utlevering dersom dataansvarlig ikke er kjent med praksisen.

2.4 Fordeler med skytjenester

I dette kapitlet belyses noen fordeler med skytjenester, sett i lys av Normens krav. Det vil også være andre fordeler med skytjenester som ikke direkte vil ha betydning for

[3] Overskuddsinformasjon (prinsippet om dataminimering): mengden innsamlede personopplysninger er større enn til det som er nødvendig for å realisere innsamlingsformålet. Dersom personopplysninger ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn.

personvernet og informasjonssikkerheten, men som indirekte kan ha betydning. Av disse årsaker er dette kapitlet gitt den inndeling som følger nedenfor.

Det er ikke automatikk i at fordelene kan hentes ut ved å ta i bruk skytjenester, men tjenesten kan gi et potensial for det.

Drift og sikkerhet:
- Høyere grad av fysisk sikkerhet (datarom, kjøling, strøm, vanninntrenging, brann og innbrudd) for servere og nettverksutstyr.
- I stedet for å kjøpe og installere ressurskrevende oppgraderinger selv, kan leverandøren håndtere dette for virksomheten.
- Profesjonell administrasjon av sikkerhet i applikasjoner og nettverk.
- Rask håndtering av patching (oppdateringer).
- Robust og effektiv sikkerhetskopiering.
- Kan raskt få tilgang til moderne teknologi som forbedrer sikkerhet og ytelse.
- Kjøp av profesjonelle skytjenester kan gi en bedre sikkerhet for den registerte enn den løsningen virksomheten klarer å etablere og forvalte i egen regi ved at tilgjengeligheten kan være bedre enn lokalt installerte tjenester.

Skalerbarhet
- Kan raskt skalere opp eller ned prosesseringsytelse og lagringskapasitet, ved behov.
- Virksomheter som gjennomfører test av applikasjoner kan enkelt etablere ny infrastruktur for dedikerte testmiljø.

Brukervennlighet
- Skytjenesten kan være tilgjengelig uavhengig av hvor brukeren er lokalisert. Dette kan gi fordeler om brukeren er mobil med helsetjenester til bruker / pasient.
- Ved behov kan virksomheten raskt etablere tilgang til brukervennlige og fleksible tjenester.

Økonomi
- Virksomheten kan raskt anskaffe tjenester som er mer operative til en fordelaktig pris enn å anskaffe og eie aktiva.
- Tilgang til tjenester (applikasjoner, infrastruktur) som det er behov for kun i en kort periode. Når leien av tjenesten opphører, opphører også kostnadene som ellers måtte avskrives i regnskapet over år.
- Virksomheten retter fokus på sine kjernetjenester i stedet for å anvende mye tid på IKT.
- Lavere totalkostnader ved at kostnadene for applikasjoner, infrastruktur, driftspersonell og styringssystemer er delt med andre.

3 Fra etablering til avvikling av skytjeneste

Kravstilling og nødvendige sikkerhetstiltak ved bruk av leverandører skal bygge på en dekkende risikovurdering. Risikovurderingen skal alltid omfatte scenarioer som omfatter leverandørens autoriserte og ev. uautoriserte tilgang til helse- og personopplysninger og annen taushetsbelagt informasjon.

Virksomheten skal sikre at relevante sikkerhetskrav inngår i alle anskaffelser. Virksomheten skal sørge for at den har tilstrekkelig bestillerkompetanse tilgjengelig.

I dette kapitlet beskrives ansvar og plikter for dataansvarlig og databehandler samt momenter til innholdet i en databehandleravtale.

3.1 Plassering av ansvar og roller

Det ligger til grunn i Normen at virksomhetens leder er ansvarlig for personvernet og informasjonssikkerheten i virksomheten. De operative oppgavene for å ivareta ansvaret kan, etter Normen, delegeres til andre roller. Disse rollene kan være internt i virksomheten eller hos en ekstern part (databehandler). Det er viktig at ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset leveransemodellen som benyttes.

Outsourcing av drifts- og systemutviklingsoppgaver til leverandører som befinner seg i andre land kan reise en rekke sikkerhets- og beredskapsutfordringer. Lokale driftsforhold, nasjonale regler og praksis på området kan avvike fra norske krav til sikker IT-drift eller regelverk knyttet til behandling av helse- og personopplysninger. Nasjonalt tilsyn og mulighetene til å føre kontroll med hvordan med hvordan leverandøren håndterer data kan være svekket.

Det er dataansvarlig som beslutter at skytjenester skal tas i bruk for et bestemt formål. Dataansvarlig bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke hjelpemidler som skal brukes.

Det ligger i skytjenestens egenskaper (jf. kap. 2) at oppgaver delegeres til leverandøren for den delen av behandlingen skytjenesten dekker. Omfanget vil avhenge av hvilken tjeneste- og leveransemodell skytjenesten er basert på. Jf. figuren i kap. 2.1 vil leverandørens operative ansvar strekke seg lenger ved en PaaS-tjeneste enn ved IaaS-tjeneste.

Uansett valg av tjenestemodell, vil leverandøren utføre sentrale deler av behandlingen av helse- og personopplysninger. Uansett valg av tjeneste- og leveransemodell vil alle krav knyttet til behandling av helse- og personopplysninger måtte følge norsk rett. På den bakgrunn er det viktig at dataansvarlig påser at alle oppgavene etter Normen blir ivaretatt og nedfelt i en databehandleravtale (jf. kap. 3.4).

Leverandøren av skytjenesten har et selvstendig ansvar etter Normen, jf. databehandleravtalen. Om leverandøren benytter en eller flere underleverandører, har leverandøren et selvstendig ansvar for å påse at Normen etterleves hos underleverandørene.

Om leverandøren benytter underleverandører, skal det gjennom databehandleravtalen pålegges leverandøren uten opphold å rapportere til virksomheten om hvem den/de er. Det skal også rapporteres når det skjer endringer i dette.

Hensikten med å tydeliggjøre ansvarslinjene i databehandleravtalen er å sikre at ansvaret for oppgavene blir ivaretatt og at forvaltning og sikkerhetsløsninger er transparente fra dataansvarlig og helt til ytterste ledd (underleverandørene).

I kap. 3.4framgår det forslag til tema som bør innarbeides i en databehandleravtale ved bruk av skytjenester. Faktaark 1 - Ansvar og organisering – gir mer veiledning

Som tidligere nevnt har databehandler en selvstendig plikt til å etterleve alle krav i Normen, herunder bestemmelsene som er nedfelt i databehandleravtalen.

Nedenfor beskrives noen temaer som virksomheten bør ha spesiell fokus på slik at databehandler ivaretar følgende ifm. leveranse av skytjenester til behandling av helse- og personopplysninger:

- Leverandøren har plikt til å innhente godkjennelse fra virksomheten for bruk av underleverandører.
- Gi varsel til virksomheten om hvem som er underleverandør(er).
- Leverandøren skal ha kontroll med at underleverandører har tilfredsstillende informasjonssikkerhet.
- Leverandøren har ikke anledning til å benytte (behandle) helse- og personopplysningene på noen annen måte enn det som er avtalt med virksomheten.

Dokumentet ”Vedlegg – Samlet oversikt Normens krav”, gir en heldekkende oversikt som virksomheten kan benytte for å etterleve kravene i Normen. Dette vedlegget er også mappet mot ISO/IEC 27001.

3.2 Innsyn i leverandørens løsning

I dette kapitlet omtales noen av pliktene til dataansvarlig, samt noen anbefalinger. Dataansvarlig har langt flere plikter enn det som framkommer av dette kapitlet. Det som er tatt fram i denne veilederen er de pliktene som er sentrale å ivareta ved bruk av skytjenester.

Etter Normen har dataansvarlig rett til innsyn i databehandlers tekniske løsning og organisering. Det er ikke nødvendig med fysisk tilstedeværelse for innsyn. Dokumentasjon er tilstrekkelig. All dokumentasjon skal også kunne tilgjengeliggjøres for Datatilsynet ved tilsyn. Det kan ikke inngås avtale (f.eks. Non-Disclosure Agreement) som er i strid med lovverket om innsyn i dokumentasjon.

Det anbefales å benytte retten til innsyn for å framskaffe så god dokumentasjon som mulig for gjennomføring av risikovurderinger.

Punktene nedenfor tar opp tema som er viktig ved bruk av skytjenester:

- Kontroll med hvor helse- og personopplysninger behandles:
    a. Dataansvarlig skal alltid vite hvor opplysningene behandles. Hvor nøyaktig informasjon om lokasjon skal være må alltid vurderes basert på om informasjonen kan gi et bilde av beskyttelsesnivå (på personopplysningene), og om det kan

bidra til etterlevelse av personvernforordningen (GDPR). Det er derfor alltid nødvendig å avklare om det er innenfor/utenfor EU/EØS (som minimum).

b. Leverandøren kan være lokalisert med datasentre i ett eller flere land for den samme tjenesten (f.eks. ved behov for redundans, sikkerhetskopiering på alternativt sted, ressursdeling, oppskalering av ytelser mv.).

- Påse at leverandøren ikke behandler opplysningene til andre formål enn det som er avtalt med dataansvarlig(f.eks. utleverer til andre, uautorisert intern bruk f.eks. statistikk/markedsføring for egen del, m.v.).
- Innsyn i hvem underleverandøren(e) er og hvor de er lokalisert.
- Innsyn i underleverandørenes tekniske løsninger.
- Hvilken mulighet dataansvarlig har til å føre kontroll med om opplysningene behandles i henhold til regelverket.

3.3 Gjennomføring av risikovurdering

Dataansvarlig skal alltid foreta en konkret vurdering av hvorvidt skytjenester er egnet til bruk ved behandling av helse- og personopplysninger. I denne vurderingen skal det blant annet legges vekt på informasjonsbehandlingenes art, omfang, formål og sammenhengen den utføres i. Ved behandling av sensitive personopplysninger stilles det høyere krav til sikkerhet i løsningen. Behandlingens formål må også vurderes i hvert enkelt tilfelle, da enkelte behandlingsformål kan være mer belastende for personvernet enn andre. Dersom behandlingen skal foregå over lengre tid, vil det også stilles strengere krav.

Risikovurderinger skal gjennomføres:
- alltid når det tas i bruk skytjenester
- etablering eller endring i behandling av helse- og personopplysninger
- ved større konfigurasjonsendringer
- når det oppstår avvik av betydning og alltid ved uautorisert utlevering av helse- og personopplysninger med betydning for konfidensialitet
- som en del av kontroll og oppfølging

Mer tilgjengelighet av helse- og personopplysninger i skyen kan være en trussel ved at store globale aktører er et større mål for angrep enn småaktører, og risikobildet og teknologien endrer seg fort.

Nedenfor er det ført opp noen eksempler på områder som bør inngå i en risikovurdering:

Tema (Referanse til kapittel)	**Område**	**Konfidensialitet**	**Integritet**	**Tilgjengelighet**
Tilgangstyring (4.1)	Brukerkontoer og roller er iht. tjenestelige behov	☒	☒	☒
	Autentiseringsmetode	☒	☐	☒
Logging (4.2)	Logger i tilknytning til helse- og personopplysninger	☐	☒	☒
	Logger for infrastruktur	☐	☒	☒
Kryptering (4.3)	Mellom bruker (klienten), leverandøren, internt hos leverandøren og eventuelle underleverandører	☒	☒	☐
Konfigurasjonskontroll	Separering mellom kunder	☒	☐	☐

Tema (Referanse til kapittel)	Område	Konfidensialitet	Integritet	Tilgjengelighet
(4.4)	Bevissthet rundt hvor data ligger i leverandørens ulike datasenter, i ulike land	☒	☐	☒
Pasientrettigheter og personvern (4.5)	Pasienten/brukeren må sikres innsyn i egne helse- og personopplysninger og logger	☐	☒	☒
	Pasientens/brukerens rettigheter til retting/sletting av helse- og personopplysninger må ivaretas	☐	☒	☐
Tilbakelevering (3.8)	Virksomheten har ikke tilgjengelig en applikasjon for å behandle helse- og personopplysninger som er tilbakelevert	☐	☒	☒

Ved bruk av skytjenester kan virksomheten velge å la leverandøren gjennomføre risikovurdering av løsningen som tilbys. Denne skal dokumenters, og virksomheten (kunden) skal ha innsyn i eller tilgang til vurderingen. I tillegg skal virksomheten gjennomføre risikovurdering for egen behandlingen av helse- og personopplysninger.

Se også veileder om risikostyring i informasjonssikkerhet og personvern.

3.4 Gjennomføring av DPIA

For gjennomføring av DPIA vises det til metodebeskrivelse publisert på nettstedet til Datatilsynet.

Følgende sjekkliste bør benyttes til å kontrollere om alt er med.

Direktoratet for eHelse har publisert en mal for gjennomføring av DPIA. Denne er omfattende og må tilpasses / skaleres i forhold til den enkelte DPIA.

3.5 Databehandleravtale

I dette kapitlet omtales databehandleravtale når helse- og personopplysningene behandles i EU/EØS området.

Alle virksomheter skal inngå en databehandleravtale når helse- og personopplysninger behandles eksternt (jf. personvernforordningen artikkel 28). Virksomhetens ledelse har ansvaret for å inngå en databehandleravtale med databehandler.

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

I en databehandleravtale et det visse krav til innhold. Det er dataansvarlig som har ansvaret for at avtalen oppfyller kravene i gjeldende regelverk. Databehandleravtalen går foran eventuelle standardvilkår brukt av leverandøren. En databehandleravtale kan gjerne inngå som et vedlegg i andre avtaler.

Innledningsvis i avtalen må det presiseres formålet med behandlingen av helse- og personopplysninger hos databehandler. Dette vil avhenge av valgt tjeneste og leveransemodell (jf. kap. 2.2). Det er dataansvarlig som bestemmer hvem som skal ha tilgang til virksomhetens helse- og personopplysninger.

I Bruk av databehandler (faktaark 10) framgår minimumskravene til en databehandleravtale.

Virksomheten bør vurdere om punktene nedenfor skal innarbeides i avtalen om skytjenester:

- Prinsippene for tilgangsstyring (Både internt hos leverandør og i virksomheten som skal bruke løsningen).
- 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 med korrekt adresse(r).
- Hvordan tilbakelevering av data / applikasjon skal skje ved avslutning av avtalen / avvikling av samarbeidet.
- Hvordan virksomheten kan få innsyn i den tekniske løsningen.
- Hvordan virksomheten skal få innsyn i logger.
- Administrasjon av taushetserklæringer. Det anbefales at leverandøren administrerer disse for sine ansatte og eventuelle underleverandører.
- Hvordan pasientens rettigheter til innsyn i personopplysningene, retting og sletting ivaretas, samt innsyn i logger.
- Gjennomføring av sikkerhetsrevisjoner og innsyn i resultat fra eksterne revisjoner.
- Tilrettelegge for dokumentasjon slik at virksomheten kan ivareta sin kontrollplikt.
- Leverandørens plikt til å informere virksomheten når det tas i bruk underleverandører og ved endring i bruk av underleverandør med korrekt adresse.
- Plikt til å iverksette avviksbehandling og rapportering til dataansvarlig.
- Krav om at leverandør gjennomfører risikovurderinger og at disse revideres ved endringer, samt at virksomheten har rett til innsyn eller tilgang til vurderingene.

For øvrige vises det til ulike veiledere og faktaark under Normen som kan gi ytterlige informasjon om spesifikke tema.

3.6 Bruk av databehandler utenfor EU/EØS

Virksomheter som overfører personopplysninger til utlandet, skal påse at beskyttelsesnivået i personopplysningsloven ikke undergraves ved overføringen.

Alle landene innenfor EU/EØS-området har innført personvernforordningen og slik sikret at personopplysninger behandles forsvarlig. Europakommisjonen har i tillegg anerkjent at noen tredjeland[4] har et tilstrekkelig nivå for vern av personopplysninger. Derfor kan personopplysninger fritt overføres til disse statene. Dette forutsetter at personopplysningslovens øvrige vilkår er oppfylt.

[4] Med "tredjeland" menes i denne veilederen alle land utenfor EU/EØS landene. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Dersom det skal benyttes leverandører eller tjenester etablert utenfor EU/EØS, kan det gjelde spesielle krav. Disse kravene skal sikre at opplysningene er underlagt samme beskyttelsesnivå som i EU/EØS-området. Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene i forordningen.

Ved overføring av opplysninger til land utenfor EU/EØS skal virksomheten sikre at den har tilstrekkelig kompetanse (f.eks. juridisk kompetanse) tilgjengelig for å gjennomføre dette i tråd med relevante krav.

Se Datatilsynets nettside for oppdaterte og utfyllende opplysninger om overføring til utlandet.

3.7 Plikt til å kontrollere

Nedenfor er det vist noen verktøy virksomheten kan benytte for å kontrollere om databehandler etterlever Normens krav:

- Rapporter fra avvikshåndtering. Se Veileder om internkontroll i informasjonssikkerhet og personvern.
- Resultat fra sikkerhetsrevisjon. Se Sikkerhetsrevisjon (faktaark 6)
- Analyser fra logger. Se Logging og innsyn i logg (faktaark 15) Resultat fra risikovurderinger. Se Veileder om risikostyring i informasjonssikkerhet og personvern
- Resultater/rapporter fra internkontroll og etterlevelse av avtaler. Veileder om internkontroll i informasjonssikkerhet og personvern
- Innsyn i konfigurasjonskart og dokumentasjon av teknisk løsning

Om virksomheten ikke selv har mulighet til å gjennomføre kontrollene kan virksomheten benytte en tredjepart til dette.

Det bør innarbeides i databehandleravtalen at leverandøren uten opphold oversender dokumentasjon fra kontrollene som er nevnt ovenfor. Virksomheten har rett til å få dokumentasjonen utlevert fra leverandøren.

Leverandøren har som nevnt et selvstendig ansvar for å påse at eventuelle underleverandører etterlever kravene i Normen.

3.7.1 Bruk av ISO 27001 for kontroll

Virksomheten må selv gjøre egne vurderinger selv om leverandøren har gjennomført sertifiseringer etter ISO/IEC 27001. Leverandørens sertifisering (sertifikat) med Statement of Sertifiseringssertifikater (Statement of Applicability [SOA]) kan forenkle dataansvarliges arbeid med innsyn og kontroll. Dette kan være gjeldende i de tilfeller at krav i ISO 27001 er sammenfallende med Normens krav. Det vil derfor være en fordel å få innsyn i leverandørens eksterne revisors rapporter fra sertifiseringsrevisjoner.

Det er videre viktig å vurdere om sertifiseringens omfang («scope» som beskrevet på sertifikatet) er relevant for ivaretakelse av informasjonssikkerhet i behandlingen av helse- og personopplysninger som skjer på vegne av dataansvarlig.

Etterlevelse av relevant lovverk er ett av sikkerhetstiltakene som følger av standarden (beskrevet i A.18.1 kapitlet), men det vil også være relevant å sjekke at dette tiltaket er tatt med SOA. En mer utdypende kontroll av etterlevelse av krav bør følge av de øvrige kontrollene som er nevnt ovenfor.

Innsyn i slik dokumentasjon kan, i tillegg til informasjon i tjenestebeskrivelsene, bidra til at kunden får en bedre forståelse av hva leverandøren tar ansvar for, og hva kunden må sørge for selv.

3.7.2 Bruk av Cloud Security Alliance (CSA) sjekkliste

Cloud Security Alliance (CSA) Norge har utarbeidet en kryssreferanse mellom Normen 6.0 og de 16 kontrollområdene i Cloud Controls Matrix (CCM).

CSA CCM er et rammeverk som er spesielt utviklet for å veilede skyleverandører i hvordan sikre totaliteten av sin leveranse. Videre er CCM utviklet for å gi skykunder et verktøy for å vurdere sikkerhetsrisiko forbundet med en skyleverandør. CSA har også utviklet ja/nei-spørsmål som kan stilles til skyleverandører om ulike kontrolltiltak er ivaretatt (CAIQ). Denne følger samme struktur som CCM. Kryssreferansetabellen finnes i vedlegg kap. 5.1.

3.8 Tiltak ved avvikling av tjenesten

Avvikling av skytjenesten kan f.eks. være knyttet til at avtalen opphører, leverandøren avvikler tjenesten eller at leverandør går konkurs. Andre forhold som kan knyttes til avvikling er om virksomheten ønsker å si opp avtalen. Avviklingsstrategi bør innarbeides i avtalen med leverandøren.

Det er et grunnleggende krav at leverandøren plikter å levere tilbake alle opplysninger, inkludert helse- og personopplysninger, herunder sikkerhetskopier til virksomheten. Logger er en del av pasientjournalen og skal inngå i tilbakeleveringen.

Når tilbakeleveringen er utført plikter leverandøren å slette helse- og personopplysningene på alle medier og aktuelle lokasjoner, herunder hos eventuelle underleverandører, for datasentre. Det anbefales at virksomheten innhenter en erklæring fra leverandør om at sletting har funnet sted.

Tilbakelevering kan være komplekst og gi utfordringer. Ved bruk av SaaS er applikasjonen leid fra leverandør. Dette kan innebære at tilbakeleverte data medfører utfordringer ift:
- Tilgjengelighet ved at det ikke finnes en applikasjon som kan behandle opplysningene
- Integritet ved at det f.eks. ikke fins tolkning av kodeverk, ved at kodeverket er i applikasjonen og ikke i dataene

Denne veilederen tar ikke mål av seg å gi utfyllende sjekkliste for dette området. Ut fra momentene ovenfor må virksomheten ta stilling til utfordringene gitt den tjeneste- og leveransemodell som benyttes.

Det anbefales at det etableres nødprosedyrer for alternativ drift om avvikling skjer brått. Mer om nødprosedyrer finnes i Nødprosedyrer ved bortfall av IKT (faktaark 11).

4 Sikkerhetstiltak ved bruk av skytjenester

Informasjonssikkerheten skal være tilfredsstillende og handler om å ivareta konfidensialitet, integritet og tilgjengelighet ved behandling av helse- og personopplysninger.

I dette kapitlet beskrives et utvalg av informasjonssikkerhetstiltak som er viktige å følge opp ved bruk av skytjenester. Utvalget er basert på beste praksis for områder som er spesielle for skytjenester. Etter Normen er det stilt krav om en rekke flere tiltak enn det som framkommer av dette kapitlet. Vedlegg til Normen – Vedlegg – Samlet oversikt Normens krav – gir en heldekkende oversikt over informasjonssikkerhetstiltakene etter Normen.

4.1 Tilgangsstyring

Som nevnt flere ganger i denne veilederen er det ofte flere aktører/roller involvert i skytjenester. Skytjenestene er normalt delt med en rekke andre kunder av leverandøren. Det er derfor av særlig betydning at virksomheten påser at det blir etablert tilstrekkelige prinsipper for tilgangsstyring.

Prinsippene for tilgang til helse- og personopplysninger skal følge tjenstlige behov hos den Dataansvarlig, uansett hvilken aktør som har tilgang. All tilgang skal gis under bestemmelsene om taushetsplikt.

Om det benyttes roller skal dataansvarlig etablere roller som bygger på prinsippene om tilgangsstyring. Tilgangsstyring skal etableres i alle systemer.

Systemet som administrerer autorisasjon av tilganger til skytjenestene skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger. All tildeling av autorisasjon skal registreres i et autorisasjonsregister. For detaljer om autorisasjonsregister vises det til Veileder om tilgang til helseopplysninger.

I prinsippene og løsningen for tilgangsstyring må tilgjengelighet for brukeren fastsettes slik at brukeren får de rette tilganger iht. sitt tjenestelige behov til enhver tid.

For admin kontoer gjelder Normens krav:

- Bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver
- Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger

All autentisering for tilgang til helse- og personopplysninger i skytjenestene skal være personlige. For tilgang til helse- og personopplysninger skal det benyttes en sikker autentiseringsløsning. Risikovurderingen må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.

Tilgangsstyring (faktaark 14) gir mer hjelp ifm. å etablere tilgangsstyring.

4.2 Logging

Virksomheten skal påse at det er etablert logging og rutine for kontroll av logger, slik at den har kontroll med aktiviteten i skytjenesten.

Loggene som er knyttet til pasientjournalen har de samme lovregler for tilgang, endring, innsyn, oppbevaring og sletting som selve pasientjournalen.

Nedenfor behandles logger som ikke er en del av pasientjournalen. Eksempler på slike logger er:

- Autentiseringsinformasjon i skytjenesten
- Systeminformasjon med betydning for informasjonssikkerheten
- Sikkerhetsbarrierer (brannmurer mv.)

All autorisert bruk og forsøk på uautorisert bruk av løsningene skal registreres. Loggene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.

Det skal etableres rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser.

Loggene skal sikres mot endring og sletting.

Alle oppføringer i loggene skal oppbevares til det ikke er bruk for dem lenger.
Det anbefales å skille på relevante og ikke relevante logger for tilgang til helse- og personopplysninger.

Om det avdekkes hendelser som viser uautorisert bruk, skal det opprettes en avviksmelding som skal håndteres iht. etablerte rutiner.

Logging og innsyn i logg (faktaark 15) - gir mer hjelp.

4.3 Kryptering

Kryptering er et virkemiddel for å sikre konfidensialitet til helse- og personopplysninger.
I denne forbindelse kan kryptering brukes til tre formål:

1. Kryptering av data som er i transport over datanettverket kan være et godt alternativ for sikring fra ende til ende
2. Kryptering av kanalen for overføring – et annet alternativ. Sikring av overføringskanal omfatter som hovedregel kun én kanal, men det kan også være ulike kanaler for ansatte og pasienter, samt leverandører
3. Kryptering av data som lagres - et godt alternativ for sikring mot misbruk

Disse tre formålene er utdypet nedenfor.

1. Kryptering av data som overføres over datanettverket

All datakommunikasjon med helse- og personopplysninger, som skjer i datanettverk som virksomheten ikke selv har kontroll over, skal krypteres[5]. Overføring av helse- og personopplysninger mellom leverandøren og eventuelle underleverandør(er) skal sikres tilsvarende.

Virksomheten må påse at helse- og personopplysninger som overføres er krypterte . Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med. Kontrollen kan ivaretas gjennom avtale.

Kryptering forutsetter en forsvarlig behandling av partenes krypteringsnøkkel(er). Virksomheten må utarbeide prosedyrer som sikrer at krypteringsnøkler og/eller sertifikater blir forsvarlig sikret og at krypteringsnøklene er unike for hver enkelt bruker iht. krav beskrevet i "Kravspesifikasjon for PKI i offentlig sektor".

2. Kryptering av kanalen for overføring

Nettverkskommunikasjonen skal sikres med minst to uavhengige, tekniske virkemidler (jf. Normen kap. 5.5.2).

Sikring av kanaler kan f.eks. løses ved:
- Bruk av VPN[6] (Virtual Private Network)
- Kombinasjon av VPN og prinsipper for VLAN[7] (Virtual LAN (Local Area Network))

Om overføringskanalen er etablert over Internett skal virksomheten etablere tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles.

Mer hjelp til sikkerhetsarkitektur og datakommunikasjon fins i Kommunikasjon over åpne nett (faktaark 24).

3. Kryptering av data som lagres

Data som lagres hos leverandøren kan sikres med kryptering. Dette er en metode som kan benyttes for data som er i transitt mellom datasentre på ulike lokasjoner.

Ved bruk av kryptering av lagrede data bør en undersøke om løsningen er tilfredsstillende iht. krav til kryptering.

4.4 Konfigurasjonskontroll

Det er en forutsetning at virksomheten har oversikt over og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger slik at konfidensialitet, integritet og tilgjengelighet blir ivaretatt.

---

[5] Se for eksempel dokumentet «NSM Cryptographic Requirements Version 3.1» og Level Moderate, https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

[6] Om VPN: http://no.wikipedia.org/wiki/Virtual_private_network

[7] Om VLAN: http://en.wikipedia.org/wiki/Virtual_LAN

Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

- Risikovurdering som viser at nivå for akseptabel risiko er oppnådd.
- Test som sikrer at forventede funksjoner er ivaretatt.
- Implementering som sikrer mot uforutsette hendelser.
- Ny konfigurasjon er dokumentert.
- Konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger.

Leverandøren av skytjenesten plikter å dokumentere alle konfigurasjoner i et konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen. Konfigurasjonskartet skal vise leverandørens datasenter(e) (lokasjon(er)) og eventuelle underleverandørers lokasjon.

Konfigurasjonskontroll skal avtales i databehandleravtalen (jf. kap. 3.5).

4.5 Pasientens rettigheter og personvern

Virksomheten må sikre at det er mulig å ivareta den registres rettigheter ved bruk av skytjenester.

Det bør avtales i databehandleravtalen at det skal finnes prosedyrer som sikrer at:

- Pasienten/brukeren sikres innsyn i alle opplysninger i behandlingsrettet helseregister. Dette gjelder også lydlogger, røntgenbilder, videoopptak etc.
- Pasientens/brukerens rettigheter til retting/sletting av helse- og personopplysninger ivaretas
- Pasienten eller brukeren har rett til å motsette seg at opplysninger utleveres eller tilgjengeliggjøres. Dette kan gjelde overføring eller tilgjengeliggjøring av opplysninger både til pasienten selv, til verger og /eller til helsepersonell

Innsyn i logger skal som et minimum sikre at den registrerte får informasjon om minimum:

- Identitet og organisatorisk tilhørighet til den som har hentet fram helseopplysninger
- Grunnlaget for tilgjengeliggjøringen
- Tidsperioden for tilgjengeliggjøringen.

5 Vedlegg

5.1 Mapping Cloud Controls Matrix og Normen 6.0

Kryssreferanse mellom Normen 6.0 og kontrollområdene i Cloud Controls Matrix:
https://ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen

5.2 Referanser

- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)
- Datatilsynets nettsted for skytjenester
- Markedsplassen for skytjenester
- Interdepartemental arbeidsgrupperapport: Kartlegging av hindringer i regelverk for bruk av skytjenester
- NISTs nettsted for skytjenester
- NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0
- Cloud Controls Matrix
- Kravspesifikasjon for PKI i offentlig sektor
- Bruk av databehandler (faktaark 10)
- Logging og innsyn i logg (faktaark 15)
- Personopplysningsloven (personvernforordningen - GDPR)
- Pasientjournalloven
- Helseregisterloven
- Helsepersonelloven
- Pasient- og brukerrettighetsloven

Besøksadresse
Direktoratet for e-helse
Verkstedveien 1
0277 Oslo

Kontakt
sikkerhetsnormen@ehelse.no