NORMEN

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

Versjon 3.0

Juni 2023

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen,etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til å at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på www.normen.no.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

Innhold

1 Innledning

1.1 Bakgrunn

Digitale tjenester flyttes i økende grad fra lokale driftende systemer og over i skybaserte tjenester. Driverne for dette er blant annet lavere kostnader for virksomhetene og enklere drift. Overgangen til skytjenester er også en villet utvikling, sett fra myndighetenes og virksomhetenes side.

Selv om skytjenester for mange virksomheter vil ha flere fordeler enn ulemper, er ikke bruk av skytjenester uten risiko. Når man ikke har full kontroll på hvor og hvordan virksomhetenes helse- og personopplysninger blir behandlet, blir det enda viktigere å gjøre gode vurderinger av informasjonssikkerhet, personvern og pasientsikkerhet.

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

1.2 Tema for veilederen

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

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

1.3 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
- Dataansvarlig
- Leverandører/databehandler
- IKT-ansvarlig
- Sikkerhetsleder/sikkerhetskoordinator

- Personvernombud
- Bestiller / innkjøpsfunksjon
- Systemeier. Dette vil ofte være en definert rolle og kan være en bestemt person, eller lagt til IT-avdelingen.
- Forskningsansvarlig og prosjektleder forskning
- Ansatte

1.4 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Forskrift for ledelse og kvalitetsforbedring i helse- og omsorgstjenesten skal bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves. Dette skal blant annet gjøres ved at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter i tråd med forskriften, og at medarbeiderne i virksomheten medvirker til dette. Styringssystemet skal tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold og ha det omfang som er nødvendig, og det beskrives en rekke relevante plikter i § 6-9 av denne forskriften.

Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) beskriver virksomheters plikter ved behandling av helseopplysninger, og § 23 Internkontroll beskriver at dataansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med lovgivningen, og at tiltakene skal dokumenteres og være tilgjengelig både for medarbeidere og tilsynsmyndighetene.

Det er flere bestemmelser fra lov om behandling av personopplysninger (personopplysningsloven) som er relevante for kravene som dekkes av denne veilederen. Loven gjennomfører personvernforordningen (GDPR) i Norge. Et av personvernprinsippene som beskrives i forordningens artikkel 5 er at den dataansvarlige er ansvarlig for og skal kunne påvise at virksomheten behandler opplysninger i samsvar med de andre prinsippene. For mer veiledning, se Normens faktaark om personvernprinsippene.

Personvernforordningen artikkel 32 fremhever at virksomheten skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad, for å gjennomføre egnede tekniske og organisatoriske tiltak. Videre beskrives at ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til omstendighetene og risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. Se også pasientjournalloven § 22 og helseregisterloven § 21 om informasjonssikkerhet.

Forordningens artikkel 24 beskriver dataansvarliges ansvar. Artikkelen fremhever at virksomheten skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad, for å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med kravene i forordningen.

Dersom skytjenestene inngår som (en del av) grunnleggende nasjonale funksjoner, må virksomheten blant annet følge sikkerhetslovens krav til sikkerhetsgraderte anskaffelser (kap.

9), forebyggende sikkerhetsarbeid (kap. 4) og informasjonssikkerhet (kap. 5).[1] For mer informasjon om etterlevelsen av sikkerhetsloven, henvises det til Nasjonal sikkerhetsmyndighet.

Det europeiske personvernrådet (EDPB) har mer veiledning om temaer offentlig sektor må følge opp ved bruk av skytjenester.[2]

Se for øvrig Oversikt over Normens krav med samlet oversikt over alle Normens krav og lovhjemmel for disse.

1.5 Avgrensninger

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 etter helselovgivningen og personvernforordningen
- 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

1.6 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.

---

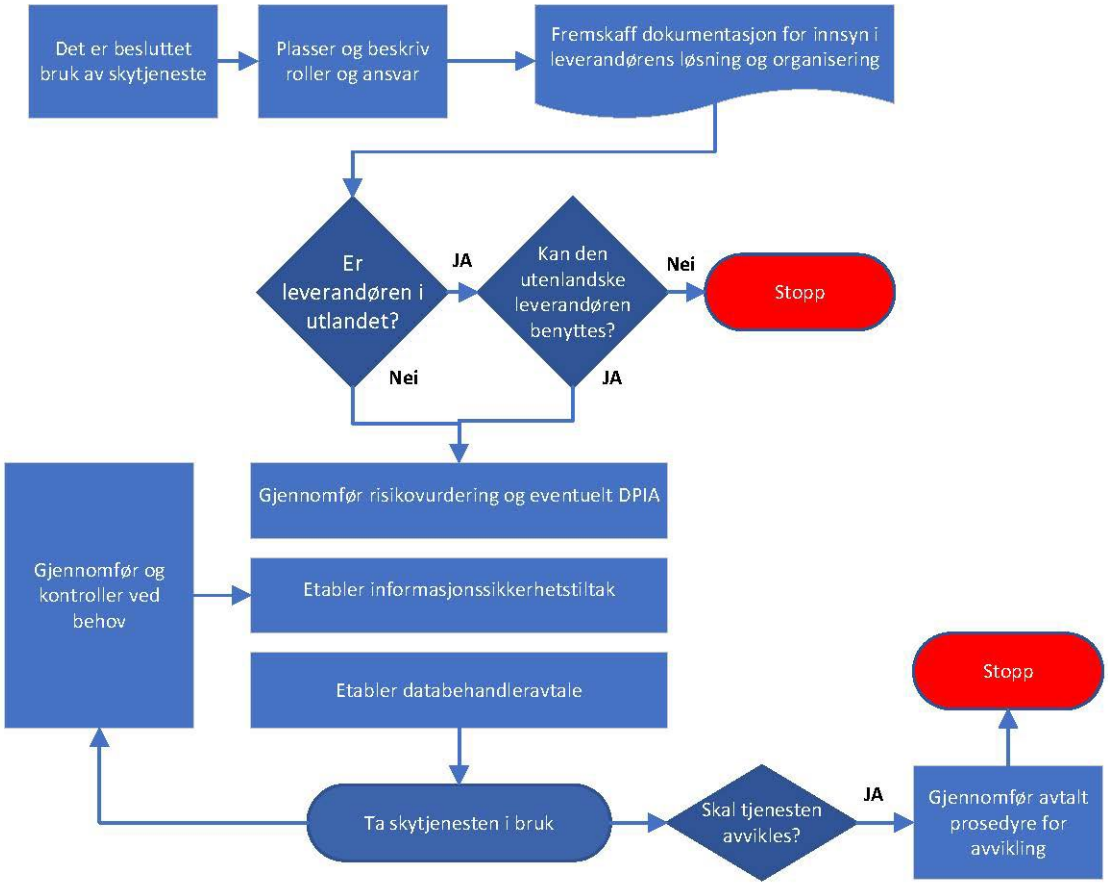
1 Lov om nasjonal sikkerhet (sikkerhetsloven)

2 2022 Coordinated Enforcement Action. Use of cloud-based services by the public sector.

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.

1.7 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.



2 Om skytjenester

2.1 Innledning

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

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.

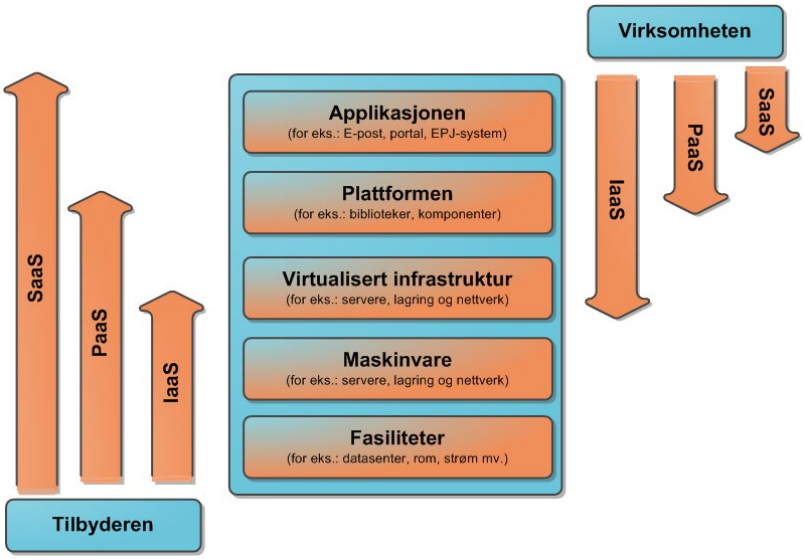
Flere av tjeneste- og leveransemodellene for skytjenester er en form for tjenesteutsetting (outsourcing). Tjenesteutsetting er i bruk i stor grad i helse- og omsorgssektoren. En tradisjonell databehandler for drift av applikasjoner er et slikt eksempel på tjenesteutsetting.

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. Virksomhetene må likevel må kompetanse (enten internt eller innleie) for kravstilling, vurdering, oppfølging og kontroll av løsning/leverandør.

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[3] nedenfor viser graden av kontroll sett i lys av de ulike tjenestemodellene. Reelt handler dette om ansvarsfordeling og hva dataansvarlig og leverandør har ansvar for.

[3] 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, og nettverk. Virksomheten kan installere sine applikasjoner på leverandørens infrastruktur. Virksomheten kontrollerer ikke den underliggende infrastrukturen, men vil ha ansvar for operativsystemer, lagring, applikasjoner som er tatt i bruk og kontroll på utvalgte nettverkskomponenter (f.eks. brannmurer som er dedikert til virksomheten).

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.

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.

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.

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.

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.

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. Det kan også innebære at deler av virksomhetenes løsninger driftes on-premise, og resterende driftes i en skyløsning. 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.

2.2.3 Kort om Zero trust og skytjenester

Ved bruk av skytjenester kan ansatte få tilgang til helse- og personopplysninger fra hvor som helst og fra mange ulike typer enheter, i motsetning til en sikker sone hvor kun en eller flere klientmaskiner har tilgang. For et slikt digitalt landskap kan virksomheten vurdere å ta i bruk Zero Trust-modellen i sitt sikkerhetsarbeid.

Zero Trust-modellen innebærer at ingen brukerkontoer, IT-utstyr og IT-systemer automatisk kan stole på andre, uavhengig av deres tilknytning til en virksomhet.

Modellen er verken en rendyrket programvare- eller maskinvareløsning, men utgjør summen av en rekke tiltak som overvåkning, deteksjon og andre kontrolltiltak som skal ivareta sikkerheten til virksomhetens infrastruktur.

Modellen tilegner alle brukerkontoer, enheter og systemer hver sin unike identitet. I stedet for å stole på at identitetene er legitime, så gjør Zero Trust-modellen det mulig å verifisere og autentisere alle forespørsler og aktiviteter som skjer innenfor den digitale infrastrukturen fortløpende. Dette kontrolleres ved at virksomheten overvåker trafikk og utstyrsbruk for å avdekke unormal atferd fra en bruker, enhet eller et system.

Zero Trust-modellen kan bidra til å redusere risikoen for lekkasjer eller uautorisert tilgang, og gir flere sikkerhetsbarrierer. En ytterligere konsekvens ved å ha flere sikkerhetsbarrierer er at man på sikt blir et mindre attraktivt angrepsmål.

Les mer om Zero Trust i Normens fagartikkel Zero Trust-modellen – et paradigmeskifte innen digital sikkerhet?

2.3 Potensielle gevinster og utfordringer ved bruk av skytjenester

Det er flere mulige gevinster for sikkerhet og personvern ved bruk av skytjenester. Det er også andre fordeler med skytjenester som ikke direkte vil ha betydning for personvernet og informasjonssikkerheten. Videre er det også noen utfordringer ved bruk av skytjenester. Noen av utfordringene som virksomheten må ta stilling til er beskrevet under i kap. 2.3.2.

2.3.1 Potensielle gevinster

Det er ikke automatikk i at gevinstene 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 registrerte 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.

2.3.2 Utfordringer

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

- Bruk av skytjenester forutsetter en annen type forvaltning enn når man drifter selv. Dette medfører at det kan være behov man ikke ser ved avtaleinngåelsen (f.eks. sikkerhetstjenester) som kan påvirke ressursbruk og kostnader.
- 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 kunnskap hvordan tjenesten er sikret og forvaltet
- Leverandøren kan ha standardbetingelser som er vanskelige å forstå omfanget av eller endre
- 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
- Sikkerhetsutfordringer knyttet til sikker konfigurasjon og bruk av skytjenester

Bruk av skytjenester kan også gi dataansvarlig støtte i å etterleve krav til informasjonssikkerhet.

2.4 Pasientens rettigheter

Virksomheten må sikre at det er mulig å ivareta den registres rettigheter ved bruk av skytjenester. Virksomheten må i anskaffelsesprosessen stille krav til skyleverandøren som skal gjøre den i stand til å oppfylle både pasientrettigheter etter helselovgivingen og personvernrettighetene som følger av personvernforordningen.

Det må blant annet sikres 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

- Dersom krav om retting/sletting skjer manuelt av leverandøren eller på forespørsel fra dataansvarlig, må det avklares på forhånd hvem hos dataansvarlig som kan gi slik instruks, og hvordan det skal gjøres i praksis.
- Den registrerte kan få innsyn i den faktiske identiteten til mottakere(virksomheter) av deres personopplysninger, inkludert underleverandører. Den dataansvarlige har en plikt til å gi den registrerte, på forespørsel, den faktiske identiteten til mottakere av personopplysninger. Det er bare der det (ennå) ikke er mulig å identifisere disse mottakerne at dataansvarlig kan nøye seg med å angi hvilke kategorier av mottakere det gjelder. Et annet unntak er når anmodningen «åpenbart er grunnløs eller overdreven, jf. EU-domstolens dom C-154/21.

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

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

For mer veiledning om rettigheter, se Veileder for rettigheter ved behandling av helse og personopplysninger.

3 Anskaffelse

Før virksomheten setter i gang med å anskaffe og ta i bruk en skytjeneste som behandler helse- og personopplysninger, må virksomheten blant annet ta stilling til om formålet ved behandlingen kan oppnås ved bruk av en skytjeneste og om virksomheten er organisert og utstyrt for å håndtere den. Man må identifisere og forstå fordelene, risikoen og fallgruvene som er knyttet til skyløsningen.

Har virksomhetene kompetanse til å planlegge og implementere skyløsningen? Vet man som vil skje med hensyn til personvern og informasjonssikkerhet? Har du de riktige sikkerhetstiltakene på plass? Å svare på disse spørsmålene på forhånd er viktig for en vellykket overgang til skyen. Det er viktig å sette seg inn i skyleverandørens standardbetingelser i forbindelse med gjennomføringen av anskaffelsen for å se om det er avvik mellom kravene som settes til sikkerhet og de aktuelle standardbetingelsene.

Kravstilling og nødvendige sikkerhetstiltak ved bruk av leverandører skal bygge på en risikovurdering. Risikovurderingen skal alltid omfatte scenarioer som omfatter leverandørens autoriserte og ev. uautoriserte tilgang til helse- og personopplysninger og annen taushetsbelagt informasjon. I forbindelse med anskaffelsesprosessen, kan oppdragsgiver benytte en prosessform der det er mulig å gå i dialog med leverandøren for å oppnå enighet om hvordan risikoen skal håndteres i avtalen.

Dersom tjenestene inngår som (en del av) grunnleggende nasjonale funksjoner, må virksomheten blant annet følge sikkerhetslovens krav til sikkerhetsgraderte anskaffelser (kap. 9), forebyggende sikkerhetsarbeid (kap. 4) og informasjonssikkerhet (kap. 5).

Virksomheten skal sikre at relevante sikkerhetskrav inngår i alle anskaffelser. Virksomheten skal sørge for at den har tilstrekkelig bestillerkompetanse tilgjengelig. Det vil være nødvendig med riktig kompetanse for kravstilling, vurdering, oppfølging og kontroll av løsning/leverandør. Dette vil blant annet inkludere teknisk, juridisk, merkantil, helsefaglig og innkjøpskompetanse.

For ressurser om anskaffelse av skytjenester, se Markedsplassen for skytjenester.

Anskaffelsesprosessen legger grunnlaget for hele avtaleforholdet med skyleverandøren, herunder hvordan avtaleforholdet skal følges opp, kontrolleres og eventuelt evalueres. For å gjøre leverandøroppfølgingen så effektiv som mulig, må dette legges til rette for. Krav og spørsmål dataansvarlig kan stille til skyleverandøren finnes i kap. 5.

Les mer om dette i Normens veileder for anskaffelse og leverandøroppfølging

3.1 Normens krav ved anskaffelse av skytjenester

Det er viktig at anskaffende virksomhet gjør en konkret vurdering av hvilke krav i Normen som er relevante for den aktuelle anskaffelsen av skytjenester. Det er lite hensiktsmessig å angi at skyleverandøren skal «oppfylle kravene i Normen» eller lignende. Dette kan imidlertid være vanskelig å evaluere for oppdragsgiver og skape et dårlig grunnlag for en kontrakt. For å kunne evaluere dette på en god måte og danne det beste grunnlaget for kontrakten, er det viktig at både leverandør og oppdragsgiver har god kommunikasjon og kjennskap til kravene

i Normen. Dette bidrar til å sikre at begge parter har en felles forståelse og forventninger til hva som kreves, og det øker sannsynligheten for en vellykket kontrakt og et godt samarbeid mellom partene.

Det finnes flere eksempler på krav i Normen som ikke er direkte rettet mot leverandører, som derfor må vurderes konkret i den enkelte anskaffelse,

Mange av Normens krav seg mot dataansvarlig virksomhet (altså den som anskaffer) og ikke databehandler/leverandør, for eksempel krav til internkontroll og risikostyring. På en annen side vil også leverandøren ofte bli pålagt via databehandleravtale eller på annen må å ha fungerende internkontroll.

Videre er det en rekke krav som er rettet mot behandlingsrettede helseregistre, og som ikke vil være relevante hvis man for eksempel skal kjøpe IaaS eller programvare som ikke skal være et behandlingsrettet helseregister.

Dokumentet «Hvordan bruke Normens krav i anskaffelser» er utarbeidet i Excel og kan sees som en plukkliste med krav som gir støtte i arbeidet med konkurransegrunnlag, utarbeidelse av kvalifikasjonskrav og kravspesifikasjoner. Det er utarbeidet egen veiledning i bruk av dokumentet. Dokumentet inneholder også mapping av alle Normens krav mot krav i NS-EN ISO/IEC 27001:2017og NS-EN ISO/IEC 27002:2017. Det er også utarbeidet en kort beskrivelse av oppbygging av dokumentet og veiledning i hvordan det kan brukes i forbindelse med anskaffelser.

Cloud Security Alliance Norway har mappet Normens krav til Cloud Controls Matrix (CCM). I tillegg er det utarbeidet en kryssreferanse fra CCM til kapitlene i Normen. CCM-rammeverket gjør det enklere for både kunder og leverandører å snakke samme språk når sikkerheten i en skyløsning skal vurderes.

3.2 Databehandleravtale

Dersom en annen virksomhet behandler personopplysninger på "vegne av dataansvarlig" skal det skal inngås en databehandleravtale. En skyleverandør vil være databehandler dersom det behandles helse- og personopplysninger i løsningen deres.

Databehandleravtalen etablerer den dataansvarliges instruksjonsmyndighet overfor databehandler. Instruksjoner som dataansvarlig setter rammene for hvordan databehandler skal behandle personopplysninger på vegne av behandlingsansvarlig. Virksomhetens ledelse har ansvaret for å inngå en databehandleravtale med databehandler.

Personvernforordningen artikkel 28 nr. 3 stiller krav til databehandleravtalens innhold. Dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med lovbestemte krav og Normens krav. Det er viktig å presisere i kontrakten med skyleverandøren at databehandleravtalen skal gå foran leverandørens standardbetingelser. Dersom det benyttes en standardavtale, for eksempel SSA-L, bør man ta inn en klausul som regulerer rangeringen. En databehandleravtale kan gjerne inngå som et vedlegg i andre avtaler. Hva som reguleres i databehandleravtalen utover kravene til innhold som følger av personvernforordningen, vil avhenge av tjenestemodellen for skytjenesten.

Minimumskravene til en databehandleravtale finnes i Faktaark 10 – Bruk av databehandler.

Direktoratet for e-helse har utarbeidet en mal for databehandleravtale med veileder som kan benyttes. Malen finnes både på norsk og engelsk.

Virksomheten bør vurdere om punktene nedenfor skal innarbeides i databehandleravtalen:

- 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 (restore) 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.
- 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.

3.3 Krav til overføringsgrunnlag ved bruk av databehandler utenfor EU/EØS

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

Alle landene innenfor EU/EØS-området har innført personvernforordningen og slik sikret at personopplysninger behandles forsvarlig. EU-kommisjonen har i tillegg anerkjent at noen land utenfor EU/EØS har et tilstrekkelig nivå for vern av personopplysninger. Denne beslutningen kalles en adekvansbeslutning. Dermed kan personopplysninger overføres til disse statene som om de lå innenfor EU/EØS. Dette forutsetter at personopplysningslovens øvrige vilkår er oppfylt.

Dersom det skal benyttes leverandører eller tjenester etablert utenfor EU/EØS som ikke omfattes av en adekvansbeslutning, kan man ikke legge til grunn at disse er underlagt nasjonal lovgiving som sikrer et tilsvarende beskyttelsesnivå som i EU/EØS. Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området som ikke er anerkjent av EU-kommisjonen, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene i forordningen.

Virksomhetene er selv ansvarlig for å finne ut hvilket overføringsgrunnlag i personvernforordningen artikkel 46 som er best egnet for deres overføring. Det mest brukte overføringsgrunnlaget er standard personvernbestemmelser (Standard Contractual Clauses

eller SCCs) vedtatt av EU-kommisjonen (jf. personvernforordningen artikkel 46 nr. 2 bokstav c)).

Selv om virksomheten bruker standard personvernbestemmelser for å overføre helse- og personopplysninger til tredjeland, påligger det en plikt til å sørge for at personopplysningene har et tilstrekkelig vern. Dette må være en konkret helhetsvurdering, basert på grundig risikovurdering og innføring av adekvate tiltak. Vurderingen må dokumenteres. Helhetsvurderingen må blant annet omfatte informasjonssikkerhet, personvern, pasientsikkerhet og formålet som søkes oppnådd med skytjenesten. Virksomheten har ansvar for å kontrollere at det faktiske beskyttelsesnivået til opplysningene er i samsvar med de standard personvernbestemmelsene og personvernforordningen for øvrig.

Overføring til tredjeland krever at virksomheten gjør komplekse vurderinger, og det er derfor viktig å ha tilstrekkelig kompetanse tilgjengelig for å gjennomføre dette i tråd med relevante krav.

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

Status for overføring til USA per 9. juni:
EU-kommisjonen har lagt frem utkast til adekvansbeslutning. Det Europeiske personvernrådet (EDPB) har lagt frem en rådgivende uttalelse om utkastet til EU-kommisjonen. Utkastet er nå til vurdering hos en komité bestående av representanter for nasjonene i EU.
En eventuell godkjenning av utkastet og en vedtatt adekvansvurdering kan ventes i løpet av 2023.

4 Risikostyring og sikkerhetstiltak ved bruk av skytjenester

For å kunne vurdere om et system skal tas i bruk, må risikoområdene, som informasjonssikkerhet, personvern og pasientsikkerhet, vurderes opp mot hverandre. Det er ledelsens ansvar i hver enkelt virksomhet å vurdere om risikoene ved å implementere et system er akseptable eller ikke. En grundig risikovurdering vil kunne bidra til en bedre forståelse av disse risikoene og styrke beslutningsgrunnlaget for ledelsen.

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 skytjenester, endres raskt og kan gi nye eller endrede trusler som kan innebære risiko. Det er ulike aktører som utgir oppdaterte situasjons- og risikorapporter, for eksempel lokalt i de ulike helseforetakene og Nasjonal Sikkerhetsmyndighet, og fra organisasjoner som Cloud Security Alliance og OWASP.

For generell veiledning om risikostyring og gjennomføring av risikovurderinger, se Veileder i risikostyring i informasjonssikkerhet og personvern.

4.1 Generelle risikoområder

Skytjenester 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.). Leverandøren kan ha underleverandører som tilbyr support på ulike lokasjoner, herunder utenfor EU/EØS.

Dette kan gi et komplekst bilde med både juridiske og sikkerhetsmessige utfordringer. 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.

Siden leveransen av tjenesten skjer fra ulike steder og man «ikke ser» leverandøren, kan også forståelsen av ansvaret være mer utfordrende. Virksomheten kan for eksempel ha en oppfatning av at alt som bygges eller lagres på en skyplattform er tilstrekkelig sikret, uten å ha forstått at skyleverandøren i hovedsak sikrer den underliggende skyplattformen og at data- og applikasjonsansvaret forblir hos virksomheten.

I de forskjellige tjeneste- og leveransemodellene kan det være ulike grader av sikkerhetsutfordringer. Se kap.3.3 for mer om overføring av personopplysninger utenfor EU/EØS.

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.
- Sikkerhetsrisiko knyttet til tredjeparter og underleverandører (andre deler av leveransekjeden). Dette kan for eksempel være partnere, sårbarheter i programvarebiblioteker, underleverandører, konkurs, osv.
- Løsepengevirus, etterretningsoperasjoner (Advanced persistence threat - APT), DDOS (tjenestenekt) og datatyveri og salg av informasjon på det mørke nettet.
- 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 har standard avtaletekster som ikke er i samsvar med 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. For å unngå innlåsing er det viktig å tenke på en evakueringsplan når kontrakten inngås.
- Avhengighet mot leveranser fra annen skyleverandør (f.eks. lisenser på produkter)

4.2 Risikoområder for tjeneste- og leveransemodellene

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

Tjeneste-modell	**Risikoscenarier** (**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 opplysninger og konfigurasjoner

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

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

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

4.3 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 særlige kategorier 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. I forbindelse med en anskaffelsesprosess kan det være lurt å vurdere hvorvidt en foreløpig risikovurdering eller en full risikovurdering, bør gjennomføres før kontrakten signeres.
- 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.

For mer veiledning om praktisk gjennomføring av risikovurderinger, se Veileder i risikostyring i informasjonssikkerhet og personvern.

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

- Tilgangsstyring
    - (Brukerkontoer og roller er iht. tjenstlige behov

    - Autentiseringsmetode)
- Logging
    - Logger i tilknytning til helse- og personopplysninger
    - Logger for infrastruktur
- Kryptering
    - Mellom bruker (klienten), leverandøren, internt hos leverandøren og eventuelle underleverandører
- Konfigurasjonskontroll
    - Separering mellom kunder
    - Bevissthet rundt hvor data ligger i leverandørens ulike datasenter, i ulike land
- Pasientrettigheter og personvern
    - 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
    - Virksomheten har ikke tilgjengelig riktige verktøy for å behandle helse- og personopplysninger som er tilbakelevert etter evakuering/avvikling av skytjenesten.

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.

4.4 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 kap. 4.2 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.
- Det er utfordringer knyttet stabil tilgang til internett og eller 4G/5G-nett.
- 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[4] 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.
- Det vil ofte være en sikkerhetsrisiko knyttet til pasientens digitale enheter, for eksempel router, nettbrett, smarttelefon eller PC.

4.5 Personvernkonsekvensvurdering

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.

Personvernkonsekvensvurderingen må gjennomføres før behandlingen av helse- og personopplysninger kan starte, og skal omhandle den spesifikke behandlingen som vurderes gjennomført. Det er med andre ord ikke til strekkelig å gjennomføre en generell vurdering av personvernkonsekvensener ved behandling av helse- og personopplysninger ved bruk av skytjenester. Dersom det er mulig å identifisere risiko i forbindelse med anskaffelsen, kan virksomheten gjennomføre en DPIA før kontrakten signeres, slik at dette er gjennomført før skytjenesten tas i bruk etter signering. Alternativt kan virksomheten få kontraktregulert at det skal gjennomføres en personvernkonsekvensvurdering før leverandøren/skytjenesteleverandøren kan gi tilgang til skytjenesten.

Dersom en eksisterende behandlingsaktivitet flyttes over til en skytjeneneste, må virksomheten vurdere om personvernkonsekvensvurderingen skal revideres. I mange skytjenesters natur ligger det også at de stadig videreutvikles, det vil si det kommer ny funksjonalitet og konfigurasjonsmuligheter. Mange av disse vil ikke dataansvarlig ha kontroll over. Noen slike endringer kan utgjøre en så stor forskjell i behandlingen av helse- og personopplysninger eller sikkerhetstiltak at de alene kan utløse behov for å revidere personvernkonsekvensvurderingen.

Det er ikke tilstrekkelig å legge til grunn vurderinger som skyleverandøren har gjort av sine egne tjenester, virksomheten må alltid vurdere om personvernrisikoen er høy og om det er nødvendig å innføre risikoreduserende tiltak før behandlingen kan starte.

Direktoratet for e-helse har laget veiledning og Mal for personvernkonsekvensvurdering med tilhørende veileder for utfylling finnes her.

[4] 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.

Se også 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.

4.6 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.

Egnede sikkerhetstiltak skal velges på bakgrunn av en risikovurdering.

4.6.1 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.

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. 3.2).

4.6.2 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 Normens veileder om tilgang.

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

For administrasjonskontoer gjelder Normens krav:

- Bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver, og
- 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.

Se også Veileder for tilgang til helse- og personopplysninger

For veiledning om å etablere tilgangsstyring, se Faktaark 14 - Tilgangsstyring.

4.6.3 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. Ved bruk og konfigurasjon av skytjenester som kan være flyktig (dvs. tjenester kan oppstå og avvikles på kort tid), kan man være nødt til å oppbevare loggene etter at den tekniske tjenesten er avviklet for å sikre sporbarhet.
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.

Faktaark 15 - Logging og oppfølging av logger – gir mer hjelp.

4.6.4 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.

For mer informasjon om kryptering, se for eksempel NSM Cryptographic Recommendations versjon 1.0.

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. 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". Se også Normens faktaark 49 om Krav ved bruk av PKI ved ekstern kommunikasjon.

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 (Virtual Private Network)
- Kombinasjon av VPN og prinsipper for VLAN (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 Faktaark 24 - Kommunikasjon over åpne nett.

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.

4.7 Tiltak ved migrering til sky

Det er vanlig at virksomheter flytter tjenester og systemer som tidligere ble driftet lokalt til en skytjeneste. Dette kan forenkle driften av tjenesten, men reiser også noen nye problemstillinger som virksomheten må ta stilling til for å sikre en vellykket overgang til skyen. For å sikre at prosessen ikke medfører unødige risikoer, er det viktig at det gjennomføres en risikovurdering.

Flytting av tjenester over til skyen kan innebære en overgang fra sonebasert tilgang (åpen og sikker sone) til «åpen sky»/en sone. Før skytjenesten tas i bruk må virksomheten derfor ta stilling til hvordan tilgangsstyring og strukturering av helse- og personopplysninger skal skje for å sikre at opplysningene er tilstrekkelig sikret og at kun personell med tjenstlig behov har adgang.

Før løsningen flyttes over i skytjenesten, må virksomheten blant annet undersøke:

- Er det i forbindelsen med gjennomføring av anskaffelsen tatt høyde for en migreringsplan i kontrakten? Inneholder denne planen nødvendige forutsetninger - eksempelvis må datamigrering skje i et uavhengig system, er det nødvendig å kryptere data under konvertering osv.
- Fungerer integrasjoner med andre systemer som de skal etter migrasjon, eller må disse konfigureres på nytt?
- Beholder løsningen all tidligere funksjonalitet? Dette kan for eksempel være påloggings- og autentifiseringsløsninger.

For veiledning om anbefalte tiltak i forbindelse med etablering av nye systemer og oppgradering/migrering av eksisterende systemer, se Normens veileder for anskaffelser og leverandøroppfølging.

5 Leverandøroppfølging

5.1 Kontroll med leverandør og underleverandører

I utgangspunktet har dataansvarlig virksomhet full valgfrihet med hensyn til utvelgelse av skyleverandør. Valgfriheten er begrenset av at leverandøren må være i stand til å ivareta kravene dataansvarlig er underlagt.

Dette innebærer at før skyleverandøren kan starte behandling av helse- og personopplysninger på dine vegne, må virksomheten vurdere om skyleverandøren er i stand til å levere et sikkerhetsnivå for opplysningene som er egnet for virksomheten, og om den setter virksomheten i stand til å oppfylle sine forpliktelser etter personvernregelverket og andre relevante regelverk, for eksempel helselovgivningen.

For å kunne sikre at databehandleren har et sikkerhetsnivå som er akseptabelt i henhold til avtalen som inngås mellom parternen, må dataansvarlig få dokumentasjon på dette. Slik dokumentasjon vil være avgjørende for at dataansvarlig skal kunne gjennomføre en reell risikovurdering av skytjenesten. 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.

Dokumentasjonen fra leverandør bør demonstrere og dokumentere etterlevelse av relevant regelverk og krav, herunder tilfredsstillende internkontroll, risikostyring og sikkerhetstiltak. Relevante sertifiseringer kan bidra til å demonstrere etterlevelse.

5.1.1 Aktuelle kontrollspørsmål til skyleverandøren

Skyleverandøren bør kunne besvare spørsmålene nedenfor, enten via dialog eller ved å levere annen form for dokumentasjon. Disse spørsmålene er relevante å besvare både ved an anskaffelse og når dataansvarlig skal kontrollere skyleverandørens etterlevelse senere i avtaleforholdet.

- Har leverandøren forpliktet seg, via databehandleravtale eller på annen måte, til å kun behandle helse- og personopplysninger på dataansvarlig sin instruks, eller forbeholder leverandøren seg retten til å behandle opplysninger til egne formål? (for eksempel «business purposes» eller lignende.)? Dersom leverandøren oppgir å bruke opplysninger til egne formål, er det viktig å identifisere hva denne behandlingen går ut på.
- Har leverandøren rutiner som sikrer at ansatte er pålagt taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon? ,jf. Normen 5.7.1
- Har leverandøren etablert et sikkerhetsnivå som er egnet i henhold til den risikoen som behandlingen av helse- og personopplysninger utgjør, og som samsvarer med ansvarsfordelingen mellom dataansvarlig og leverandør?
- Har leverandøren rutiner for å kontrollere at deres underleverandører er i stand til å opprettholde et tilsvarende sikkerhetsnivå som er pålagt leverandøren?

- Kan leverandøren sikre at underleverandører ikke engasjeres uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den dataansvarlige?
- Gjenspeiler avtalen mellom skyleverandøren og underleverandøren de krav som er pålagt skyleverandøren av dataansvarlig?
- Har skyleverandøren en fullstendig oversikt over hvilke underleverandører som benyttes til behandling av opplysningene som behandles på dine vegne? Dersom underleverandøren befinner seg utenfor EU/EØS, har leverandøren av skytjenester et overføringsgrunnlag for overføringen?
- Hvor lagres data geografisk? 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).
- Har leverandøren rutiner som sikrer at dataansvarlig får bistand til ivaretakelse av de registrertes rettigheter og dersom relevant, pasientrettigheter som følger av helselovgivningen?
- Har leverandøren rutiner for å håndtere brudd på personopplysningssikkerheten, herunder rutiner for å melde avvik til Datatilsynet innen 72 timer?
- Kan leverandøren slette eller tilbakelevere opplysningene når behandlingsaktiviteten opphører?
- Har leverandøren rutiner for å bistå ved revisjon av tjenesten, eller ved gjennomføring av revisjon av en uavhengig tredjepart?

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.

Tjenesteutsetting 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 ligger i skytjenestens egenskaper at oppgaver delegeres til leverandøren for den delen av behandlingen skytjenesten dekker. Omfanget vil avhenge av hvilken tjeneste- og leveransemodell skytjenesten er basert på.

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.

Leverandøren av skytjenesten har et selvstendig ansvar til å oppfylle kravene i Normen når disse stilles i databehandleravtalen. Om leverandøren benytter en eller flere

underleverandører, har leverandøren et selvstendig ansvar for å påse at Normen etterleves hos underleverandørene.

5.1.2 Revisjon underveis i avtaleforholdet

Dataansvarlig har plikt til å kontrollere at skyleverandøren oppfyller kravene som er nedfelt i personvernforordningen og i databehandleravtalen mellom partene.

Behovet for revisjon av skyleverandøren vil påvirkes av flere faktorer, for eksempel omfanget av helse- og personopplysninger, om det er særlige kategorier av opplysninger eller annen sensitiv informasjon og hvor inngripende behandlingen er for de registrerte.

Behovet og hyppigheten for revisjon vil bero på hvor høy risiko som er forbundet med behandlingen.

Det kan for eksempel være nødvendig å gjennomføre revisjon oftere dersom:
- Databehandleren tidligere har hatt problemer med å oppfylle avtalen
- Databehandleren har hatt flere alvorlige sikkerhetsbrudd, eller nylig har opplevd et sikkerhetsbrudd
- Leverandøren skifter underleverandører oftere
- Leverandøren ofte skifter eiere eller gjennomgår andre store endringer

Lavere frekvens kan argumenteres for dersom man har lang erfaring med databehandleren 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. Spørsmålene til leverandørene som er listet opp i kap. 5.1.1 vil også være aktuelle å følge opp.

Leverandøren har som nevnt et selvstendig ansvar for å påse at eventuelle underleverandører etterlever kravene i Normen. Det er derfor viktig at de relevante kravene stilles via databehandleravtalen med skyleverandøren.

Nedenfor er eksempler på dokumentasjon virksomheten kan benytte for å kontrollere om databehandler etterlever Normens krav:

- Rapporter fra avvikshåndtering. Se veileder for internkontroll.
- Resultat fra sikkerhetsrevisjon. Se Faktaark 6 - Sikkerhetsrevisjon
- Analyser fra logger. Se Faktaark 15 - Logging og oppfølging av logger
- Resultat fra risikovurderinger. Se Veileder for risikostyring
- Resultater/rapporter fra internkontroll og etterlevelse av avtaler. Se Veileder for internkontroll
- Innsyn i konfigurasjonskart og dokumentasjon av teknisk løsning

5.1.3 Bruk av standarder for kontroll

Enkelte virksomheter følger og er sertifisert etter ulike standarder for informasjonssikkerhet. En av disse er ISO 27001.

Virksomheten må gjøre egne vurderinger selv om leverandøren har gjennomført sertifiseringer. Leverandørens sertifisering (sertifikat) med 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. Dersom ikke SOA ikke er tilgjengelig bør leverandør bekrefte og redegjøre for at sertifiseringen gjelder for den delen av leveransen der kundens data behandles.

Det er videre viktig å vurdere om sertifiseringens omfang er relevant for ivaretakelse av informasjonssikkerhet i behandlingen av helse- og personopplysninger som skjer på vegne av dataansvarlig.

Mapping mellom ISO 27001 og Normen finnes i dokumentet «Hvordan bruke Normen i anskaffelser». Kravene i Normen og kravene i ISO 27001.

6 Tiltak ved avvikling og evakuering av tjenesten

6.1 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. Merk at en strategi for avslutning av tjenesten bør diskuteres i forbindelse med gjennomføringen av anskaffelsen, slik at strategien er på plass i det kontrakten signeres.

Statens standardavtaler for IKT, eksempelvis SSA-Lille sky har allerede noen minimumskrav til avslutning, men det må vurderes om dette er tilstrekkelig og om det må suppleres med de kravene som fremgår her.

Det er et grunnleggende krav at leverandøren plikter å levere tilbake alle opplysninger, inkludert helse- og personopplysninger, herunder sikkerhetskopier til virksomheten. Opplysninger skal tilbakeleveres på avtalt eller universelt format. 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.

6.2 Evakuering av tjenesten

Det anbefales at det etableres nødprosedyrer for alternativ drift om avvikling skjer brått. Mer om nødprosedyrer finnes i Faktaark 11 - Nødprosedyrer.

Virksomheten bør påse at slike nødprosedyrer også inntas i avtalen med skyleverandøren. Det er også viktig å være klar over at standardbetingelsene til skytjenesten har bestemmelser om avslutning. Disse kan innebære umiddelbart opphør av tjenesten dersom Virksomheten misligholder avtalen. I anskaffelsesprosessen viktig å se hvilke rettigheter kunden i slike tilfeller har for å få sine data tilbakeført, og eventuelt forsøke å forhandle på en

utsatt frist for hevingsvirkningen slik at data kan tilbakeføres til kunden før tjenesten stoppes av skytjenesteleverandøren.

Besøksadresse
Direktoratet for e-helse
Verkstedveien 1
0277 Oslo

Kontakt
sikkerhetsnormen@ehelse.no