

Problemstilling

Sendt inn av avdeling for medisinsk genetikk OUS, v/ Dag Undlien.

Flere og flere IKT-verktøy for PM-diagnostikk kjører i skyen. Erfaringene hittil er at det er krevende å få tillatelse til å benytte skyløsninger. Det er vanskelig for ikke[1]jurister og ikke-informatikere å skjønne hva som er begrensningene her og hva som gjør at dette er så krevende. Uklart for meg om dette primært er et juridisk tolkningsproblem eller om det er andre forhold som spiller inn, men ville uansett vært nyttig å få en tydeligere juridisk forklaring for legfolk om hva som skal til for at slike løsninger kan benyttes.

Bruk av skytjenester i helsetjenesten og helseforskning

Innledning

Bruk av skytjenester i helsesektoren er mulig, men det stilles strenge krav til informasjonssikkerhet og personvern. I tillegg er det en rekke krav i helselovgivningen som også skal oppfylles.

Vi vil innledningsvis påpeke at hvert helseforetak er selvstendige dataansvarlige og at interne prosedyrer og retningslinjer vil kunne være ulike fra helseforetak til helseforetak, selv om vi ser en økende grad av harmonisering og mer sammenfallende vurderinger innad i de ulike helseregionene.

Dataansvaret etter personvernregelverket vil alltid ligge hos helseforetaket, også når dataene teknisk sett håndteres av en ekstern leverandør.

Det kan oppleves krevende å få godkjenning til å bruke skyløsninger, det skyldes ikke nødvendigvis at regelverket i seg selv forbyr skybruk, men at det krever grundige juridiske, tekniske og organisatoriske vurderinger for å sikre at alle lovpålagte krav er oppfylt.

Generelt om skytjenester og forvaltningsmodellen

Skytjenester innebærer en annen forvaltnings- og driftsmodell enn helseforetakene tradisjonelt har brukt. Ansvar for drift, infrastruktur og tekniske løsninger ligger i større grad hos leverandøren, og det kan være en lang og kompleks leverandørkjede.

Skytjenester leveres vanligvis i tre tjenestemodeller:

- **IaaS (Infrastructure as a Service)** – leie av infrastruktur, som servere og lagring
- **PaaS (Platform as a Service)** – leie av en plattform for utvikling og drift av applikasjoner
- **SaaS (Software as a Service)** – ferdige applikasjoner levert over nettet

Skytjenester kan tilbys gjennom ulike leveransemodeller:

- **Public cloud** – delt infrastruktur levert av en ekstern leverandør
- **Private cloud** – dedikert infrastruktur for én organisasjon
- **Community cloud** – felles løsning for flere virksomheter med like behov
- **Hybrid cloud** – kombinasjon av ulike modeller

Skytjenester benyttes allerede i varierende grad i alle helseregioner. Det benyttes ulike tjenestemodeller og leveransemodeller, og bruk av skytjenester og skyteknologi er blant annet en del av Helse Sør-Østs strategiske satsing.

Juridiske krav og personvern

All behandling av personopplysninger i spesialisthelsetjenesten må følge personvernregelverket. Helseopplysninger er en *særlig kategori* personopplysninger (GDPR art. 9), og derfor stilles det ekstra strenge krav til behandlingen av slike opplysninger.

Når data behandles i skyløsninger, kan de lagres eller prosesseres på servere utenfor Norge, og i mange tilfeller også utenfor Europa. Det må da vurderes om dette er forenlig med personvernforordningens krav til overføring av personopplysninger til tredjeland (land utenfor EU/EØS). Overføring krever et gyldig rettslig grunnlag, for eksempel EU-standardklausuler eller adekvansbeslutninger, og det må foreligge en risikovurdering av mottakerlandets regelverk og beskyttelsesnivå.

Kort sagt handler de juridiske hindringene først og fremst om å sikre at data behandles i samsvar med regelverket, og at det er tilstrekkelig kontroll og beskyttelse rundt helseopplysninger som lagres og behandles i skyen.

Året 2025 har vært preget av stor usikkerhet rundt overføring av personopplysninger til USA. Ettersom mange av skytjenestene som er aktuelle for helsetjenesten eies av amerikanske selskaper, mener vi det er relevant å trekke frem dette her.

USA har, siden juli 2023, hatt en adekvansbeslutning vedtatt av EU-kommisjonen. Adekvansbeslutningen omfatter bare virksomheter som er sertifisert etter EU-U.S. Data Privacy Framework. Det er kun EU-kommisjonen og EU-domstolen som kan oppheve adekvansbeslutningen, og frem til det eventuelt skulle skje, er overføringer til USA lovlige. Urolighetene som oppstod etter presidentvalget i USA har imidlertid hatt stor påvirkning på hvordan amerikanske leverandører opererer i det europeiske markedet. Flere sentrale amerikanske selskap leverer nå tjenester utelukkende fra EU, slik som «EU-Sovereign cloud» og «EU data boundary», som skal gjøre det enklere for dataansvarlige i EU (og EØS) å ta i bruk tjenestene.

Databehandleravtaler og avtaleforhold

Når helseforetaket benytter en skyløsning, innebærer det at data behandles av en ekstern leverandør på helseforetakets vegne. Da skal det inngås en databehandleravtale i henhold til personvernforordningens artikkel 28. I de fleste tilfeller er IKT-leverandøren i regionen

helseforetakets primære databehandler, og IKT-leverandøren inngår merkantile og databehandleravtaler med underleverandører, som blir underdatabehandlere.

Databehandlervtaler skal blant annet:

- klargjøre hvordan og til hvilke formål opplysningene behandles
- regulere hvem som har tilgang til data
- stille krav til sikkerhet, konfidensialitet og avvikshåndtering
- sikre at helseforetaket beholder faktisk kontroll over opplysningene

Ettersom mange skyleverandører benytter underleverandører, må hele leverandørkjeden omfattes av de samme kravene.

Tekniske krav og informasjonssikkerhet

Fra et teknisk perspektiv må skyløsninger oppfylle kravene i både sektorspesifikk lovgivning, personvernforordningen artikkel 32 og [Norm for informasjonssikkerhet i helse- og omsorgssektoren \("Normen"\)](#). Det er utarbeidet en [egen veileder for bruk av skytjenester til behandling av helse og personopplysninger](#), som gir god veiledning i hvordan man kan ta i bruk skytjenester i helsesektoren.

Leverandøren må kunne dokumentere at sikkerhetsnivået tilfredsstiller helseforetakets krav, og helseforetaket må gjennomføre risikovurdering og eventuelt personvernkonsekvensvurdering (DPIA) før løsningen tas i bruk.

Hvorfor kan det oppleves som krevende å ta i bruk skytjenester?

Opplevelsen av at det er krevende å få tillatelse til bruk av skyløsninger kan ha flere årsaker:

- ulik modenhet og interne retningslinjer i de enkelte helseforetakene og regionene
- varierende grad av teknisk dokumentasjon fra leverandørene
- Varierende grad av reell påvirkningsmulighet for helseforetakene når det gjelder innretningen av skyløsninger og bruk av underleverandører mv.
- usikkerhet knyttet til lagring i tredjeland og tolkning av overføringsreglene
- behov for samordning mellom juridisk, teknisk og faglig vurdering

Dette er derfor ikke bare et juridisk tolkningsproblem, men like mye et spørsmål om praktisk implementering og risikohåndtering.

Hva skal til for å kunne bruke skyen?

For at et helseforetak eller et forskningsprosjekt skal kunne ta i bruk en skyløsning må følgende punkter være oppfylt:

1. Det må finnes et gyldig behandlingsgrunnlag – hjemmel i lov, samtykke eller dispensasjon fra taushetsplikt.
2. Databehandleravtale – inngått mellom helseforetaket og leverandøren, eventuelt mellom regionens IKT-selskap og underleverandøren, som regulerer behandling av data.
3. ROS (risiko- og sårbarhetsvurdering) – inkludert vurdering av hvor data lagres og hvem som kan få tilgang.
4. DPIA (personvernkonsekvensvurdering) – dersom behandlingen innebærer høy risiko.
5. Forankring i virksomhetens styringssystem – bruk av sky må inngå i internkontroll og sikkerhetsstyring.
6. Vurdering av dataflyt og overføringsgrunnlag – særlig dersom data overføres utenfor EØS.

For å sikre at kravene blir oppfylt bør helseforetaket involvere både fagressurser, juridisk kompetanse og sikkerhetsressurser i vurderingene.

Kort oppsummert

Skybruk i helsesektoren er mulig, men krevende. Juridiske, tekniske og organisatoriske krav må være dokumentert og oppfylt. OG til sist; et godt samarbeid mellom fagressurser, teknologer, sikkerhetsressurser og jurister er helt nødvendig for å ta valget om å gå i skyen.