# Vedlegg 2

## Tentativ kravspesifikasjon

(Ikke-funksjonelle krav)

### Generelt

| Nr. | Kundens behov |
|---|---|
| | Løsningen skal vedlikeholdes, videreutvikles og oppdateres kontinuerlig. |
| | Leverandøren skal beskrive rutiner for oppgradering, feilretting og vedlikehold og hvordan Oppdragsgiver informeres om dette eksempelvis ved større endringer som får konsekvenser for Oppdragsgivers brukere. Besvarelse på krav vil der aktuelt tas inn som en del av SLA (Service level agreement) ved signering av avtale. Minimumskrav til SLA vil fremkomme i endelig kravspesifikasjon |
| | Leverandør bør beskrive sin plan for avvikling av Løsningen. Dette er beskrevet i SSA-L bilag X, Avtalens punkt X Avslutning av avtalen. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |

### Lover standarder og normer

| Nr. | Kundens behov |
|---|---|
| | Løsningen skal være i tråd med enhver tid gjeldende lover og forskrifter. Det gjelder blant annet:<br><br>• Helse- og omsorgstjenesteloven<br>• Kommuneloven med tilhørende forskrifter<br>• Arbeidsmiljøloven<br>• Offentlighetsloven med tilhørende forskrift<br>• Forvaltningsloven med tilhørende forskrift<br>• Personopplysningsloven med tilhørende forskrift, herunder Personvernforordningen, GDPR, som er inkorporert i loven.<br>• Sikkerhetsloven med tilhørende forskrift<br>• Arkivloven med tilhørende forskrifter<br>• Folketrygdloven med tilhørende forskrifter<br>• Normen (Normen er en bransjenorm for informasjonssikkerhet og personvern og utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren.)<br>• Helsepersonelloven<br>• Pasientjournalloven<br>• Forskrift om pasientjournal<br>• Pasient og brukerrettighetsloven<br>• Fastlegeforskriften<br>• Helseregisterloven<br>• Legemiddelforskriften<br>• Forskrift om pseudonymt register for individbasert helse- og omsorgsstatistikk<br>• Forskrift om IT-standarder i offentlig forvaltning<br><br>Opplistingen er ikke uttømmende. |

| | |
|---|---|
| | Løsningen, med tilhørende nettsteder og apper bør til enhver tid følge gjeldende krav i forskriften om universell utforming.<br>WAD \| WCAG \| Tilsynet for universell utforming av ikt (uutilsynet.no)<br><br>Beskriv hvordan løsningen ivaretar krav om universell utforming. |
| | Nettsteder, applikasjoner og kommunikasjon som er rettet mot innbygger skal til enhver tid tilfredsstille krav i forskrift om universell utforming<br>WAD \| WCAG \| Tilsynet for universell utforming av ikt (uutilsynet.no) |
| | Løsningen bør følge grunnleggende standarder for elektronisk samhandling som angitt i Referansekatalogen for e-helse. Dette inkluderer krav til interoperabilitet, sikkerhet og informasjonsutveksling, slik at løsningen kan integreres effektivt med andre systemer i helse- og omsorgstjenesten. Leverandøren bes beskrive hvordan de sikrer at løsningen kontinuerlig er i samsvar med gjeldende nasjonale retningslinjer. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen skal ha mulighet for arkivuttrekk for langtidsbevaring i henhold til Helsedirektoratets EPJ-standard del 5 - Arkivuttrekk. |
| | Løsningen bør enten inneholde en godkjent arkivkjerne (NOARK 5) for emnebasert dokumentasjon med mulighet for uttrekk av arkiv til avlevering i Oppdragsgivers depot, eller kunne integreres med Oppdragsgivers valgte godkjente arkivkjerne (frittstående eller del av Oppdragsgivers sak- og arkivsystem) for å sikre ivaretakelse av det emnebaserte arkivet.<br><br>Løsningen bør kunne arkivere dokumenter som hører hjemme i et emnebasert arkiv på minst én av følgende måter:<br>- Ved bruk av kommunal standard, for tiden KS FIKS-Arkiv.<br>- Gjennom API levert av arkivleverandøren.<br>- Via API fra EPJ-leverandøren som muliggjør at arkivleverandøren kan tilby et integrasjonsadapter for å hente dokumenter og metadata.<br><br>Leverandøren bes beskrive hvordan Løsningen muliggjør avlevering til Kundens depot. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør benytte nasjonale og internasjonale standarder for kodeverk og terminologi som er anbefalt av Helsedirektoratet og eventuelt andre myndigheter for å kunne sammenstille og dele helseinformasjon. Hensikten er å sikre interoperabilitet, datakvalitet og presis informasjonsutveksling mellom helsetjenester. Det finnes flere typer av kodeverk:<br>- Administrative kodeverk (kjønn, adresse, yrke, etc.).<br>- Tekniske kodeverk for kommunikasjon (meldingstype, adresseringsinformasjon, etc.).<br>- Helsefaglige kodeverk (diagnoser, tiltak, undersøkelser, etc.).<br><br>Leverandøren bes beskrive hvordan Løsningen muliggjør sammenstilling og deling av informasjon gjennom bruk av kodeverk og terminologier. Beskrivelsen bør omfatte:<br>- Hvilke kodeverk som løsningen støtter i dag. Dette omfatter både administrative, tekniske og helsefaglige kodeverk, inkludert nasjonalt laboratoriekodeverk. Oppdragsgiver vektlegger bruk av HL7-FHIR og ICNP. Eksempler på andre kodeverk er ICD- 10/11, Snowmed CT, Open EHR.<br>- Hvordan leverandøren sikrer at oppdateringer av standardene implementeres kontinuerlig i samsvar med retningslinjene fra Helsedirektoratet. Eksempler på standarder er ICPC-2, ICD-10/11 og SNOMED CT. |

| | |
|---|---|
| | - Hvordan leverandøren i samarbeid med Oppdragsgiver legger til rette for at nye kodeverk kan implementeres og tas i bruk.<br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |

## Drift, Innovasjon og utvikling

| Nr. | Oppdragsgivers krav |
|---|---|
| | Leverandøren bør beskrive sin tilnærming til bruk av innovasjonsfond og kick-back, og sin kompetanse og kapasitet til å gjennomføre innovasjonsprosesser. Leverandøren vurderes utfra tilnærming til løsning av kravet. |
| | Løsningen bør utvikles fortløpende i henhold til nasjonale felleskomponenter og tjenester. Leverandør bes beskrive hvordan dette blir ivaretatt i Løsningen. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør tilrettelegge for å ta i bruk «Pasientens journaldokumenter» som kilde. Leverandøren bes beskrive sin utviklingsplan for dette.<br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør tilpasses endrede myndighetskrav til rapportering, eksempelvis rapportering til pasientregistre eller andre nasjonale registre. Dette bør utvikles i Løsningen uten ekstra kostnad. Leverandør bes beskrive hvilken prosess og metodikk som brukes. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør utvikles ved bruk av kunstig intelligens i funksjonalitet der det gir nytte for Oppdragsgiver. Dersom Løsningen benytter elementer av kunstig intelligens (KI) bes Leverandøren beskrive forutsetninger, funksjonalitet og muligheter i Løsningen. Leverandør bes beskrive KI-modellen, hvilke data KI-modellen er trent på, hvordan den fungerer mv. Leverandøren bes beskrive hvilke behandlinger som benytter kunstig intelligens eller eventuelt der Leverandør planlegger å benytte kunstig intelligens, hvilke data KI-modellen er testet på og hvordan KI-modellen fungerer, samt eventuelle risikoer Leverandøren ser knyttet til bruken. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Leverandør bør legge til rette for at Oppdragsgiver beslutter hvorvidt kunstig intelligens tas i bruk (“opt-in”) på Oppdragsgivers data. Leverandøren bes beskrive hvordan dette løses. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør ha talegjenkjenning som konverterer tale til tekst i sanntid, og genererer forslag til dokumentasjon som bør godkjennes av helsepersonellet. Leverandør bes beskrive fremtidig utvikling og fremdriftsplan for dette. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør ha integrasjon med tjenestene Påkobla og DigiHOT som KS Digital leverer. Leverandør bes beskrive fremtidig utvikling og fremdriftsplan for dette.<br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør tilrettelegge for nye integrasjon mot fremtidige tredjeparter.<br>Leverandør bes beskrive hvordan ytterligere tredjeparter kan kobles på fortløpende.<br><br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |

## Datadeling

| Nr. | Oppdragsgivers krav |
|---|---|
| | Løsningen bør kunne forenkle arbeidsprosesser ved å unngå dobbeltregistrering. Eksempelvis skal det unngå flere registreringer av samme type opplysning, eks. Cave eller diagnoser. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Leverandør skal tilby API tilgjengelige for integrasjon med tredjeparter. API skal være sikret med HelseID og blant annet følge HL7 FHIR standard for REST API. |
| | Leverandør skal dokumentere APIer som inngår i Løsningen. Leverandør skal tilby dokumentasjon for alle integrasjonspunkter. For API skal det benyttes standard dokumentasjonsformat slik som OpenAPI. |
| | Løsningens API-dokumentasjon skal være tilgjengelig og til enhver tid oppdatert for Oppdragsgiver. |
| | Løsningen bør tilby overvåkning av integrasjoner og varsling til brukere hvis en integrasjon ikke fungerer eller er utilgjengelig. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør ha funksjonalitet for å eksportere data og ta fysisk utskrift dersom behov. Leverandør bes beskrive hvilke filformater man kan eksportere data i. Leverandør vil bli vurdert ut fra tilnærming til løsningen av kravet. |
| | Løsningen bør ha integrasjon med KS digital: SvarInn/SvarUt-tjenesten på KS FIKS-plattformen - se nærmere beskrivelse i kapittel 3.1 i Bilag 1.2 - Integrasjoner. Leverandøren bes beskrive hvordan Løsningen støtter integrasjon med KS FIKS-plattformen, inkludert funksjonalitet for SvarUt og SvarInn, samt eventuelle begrensninger i funksjonalitet og hvordan disse kan adresseres gjennom videreutvikling. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør støtte integrasjon mot grunndata hos Norsk helsenett, inkludert:<br>- Adresseregisteret (AR)<br>- Fastlegeregisteret (FLR)<br>- Helsepersonellregisteret (HPR)<br>- Persontjenesten (tidligere Personregisteret)<br><br>Leverandøren bes beskrive hvordan tilbudt Løsning støtter integrasjon mot grunndata. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør ha støtte for HelseID og nasjonalt tillitsrammeverk ved integrasjon mot API som tilgjengeliggjøres fra Norsk Helsenett. Leverandøren bes beskrive hvordan de løser å ta i bruk disse tjenestene ved integrasjon til eksisterende og nye API'er. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør integreres med etablerte tjenester fra Norsk helsenett for å sikre sikker og effektiv tilgang til pasienters helseopplysninger. Dette inkluderer:<br>- Kjernejournal og Kritisk informasjon<br>- Pasientens journaldokumenter |

| | |
|---|---|
| | - Pasientens prøvesvar<br>Leverandøren bes beskrive hvordan foreslått løsning ivaretar disse integrasjonene. Dersom funksjonaliteten er under utvikling ber vi Leverandøren beskrive tidsperspektivet for ferdigstillelse. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør støtte integrasjon med nasjonale systemer for medikamenthåndtering, inkludert:<br>- Sentral forskrivningsmodul (SFM): For forskrivning av legemidler og medisinske hjelpemidler, inkludert beslutningsstøtte for trygg og korrekt legemiddelbehandling.<br>- E-reseptkjeden: For elektronisk ordinering, håndtering og overføring av resepter, samt tilgjengeliggjøring for helsepersonell.<br>- Pasientens legemiddel liste<br><br>Leverandøren bes beskrive hvordan foreslått løsning ivaretar disse integrasjonene. Leverandøren bes også beskrive om foreslått løsning vil ha egen legemiddelmodul eller benytte seg av SFM Fullversjon. Dersom funksjonaliteten er under utvikling, ber vi Leverandøren beskrive tidsperspektivet for ferdigstillelse. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør støtte integrasjon med nasjonale løsninger for kommunikasjon og meldingsutveksling, inkludert:<br>- Meldingsutveksling: Elektronisk utveksling av meldinger i henhold til nasjonale standarder, inkludert støtte for EDI 1.0 (SMTP), EDI 2.0 og AMQP.<br>- Helsenorge: Tilrettelegging for digital dialog med pasienter og avlevering av tilgangslogger for å sikre transparens og sikkerhet.<br><br>Leverandøren bes beskrive hvordan foreslått løsning ivaretar nasjonale løsninger som beskrevet over. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør støtte elektronisk innrapportering til relevante nasjonale registre, inkludert:<br>- Kommunalt pasientregister (KPR)<br>- SYSVAK (nasjonalt vaksineregister)<br>- MSIS<br>- Dødsmelding<br><br>Innrapporteringen skal følge gjeldende lover, forskrifter og nasjonale standarder for sikkerhet, personvern og datakvalitet.<br>Leverandøren bes beskrive hvordan Løsningen ivaretar innrapportering til nasjonale register. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør kunne ta imot og avgi data gjennom integrasjoner med Oppdragsgivers øvrige relevante fagsystemer på en god måte. Leverandøren bør dokumentere de integrasjonene Leverandøren har utviklet ferdig og hvilke integrasjoner som er under utvikling. |
| | Løsningen skal tilby integrasjon mot velferdsteknologiske løsninger via Velferdsteknologisk knutepunkt (VKP). |
| | Løsningen bør ha integrasjoner mot VKP (NHN) innenfor følgende teknologier ved oppstart:<br><br>- Medisineringsstøtte<br>- E-lås<br>- Samhandlingstavler<br>- Pasient- og ansatte varsling |

| | |
|---|---|
| | - Trygghetsalarm<br>- Digital hjemmeoppfølging<br><br>Leverandør bes oppgi og beskrive hvilke integrasjoner de har innenfor hver teknologi, og evt. Planer for nye. |
| | Løsningen bør tilby direkte integrasjon mot tredjepart:<br>- VAR Healthcare<br>- Felleskatalogen<br>- DIPS Interactor<br>-NAV (elektronisk sending av sykemelding)<br><br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør tilby støtte for elektronisk rekvirering/henvisning av radiologiske undersøkelser.<br><br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Leverandøren bør ha løsningen integrert og oppdatert i henhold til relevante og tilgjengelige tjenester på kommunal samhandlingsplattform (NHN), senest 6 mnd. etter at en ny tjeneste er publisert.<br><br>Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet |

## Sikkerhet og personvern

Oppdragsgiver har behov for en elektronisk pasientjournalløsning (EPJ) som ivaretar sikkerhet og personvern i samsvar med gjeldende lover og forskrifter, inkludert, men ikke begrenset til Personopplysningsloven og GDPR, Helse- og omsorgstjenesteloven, Pasientjournalloven, Helsepersonelloven og Normen. Løsningen må sikre de grunnleggende prinsippene for informasjons- og datasikkerhet; konfidensialitet, integritet, tilgjengelighet og robusthet for sensitive pasientdata gjennom dokumenterte tekniske og organisatoriske sikkerhetstiltak.

Oppdragsgiver har en variert brukergruppe der noen benytter personlig Windows-klient, andre bytter mellom ulike fellesklienter gjennom en arbeidsdag, og enkelte kun benytter administrerte mobiltelefoner og nettbrett for å nå EPJ-løsningen. Felles for alle disse klientene er at de administreres og forvaltes sentralt via MDM (Mobile Device Management). Variasjonene i bruksmønster og arbeidsflater må tas høyde for av leverandøren, slik at det sikrer Løsningen godt nok uten å skape utfordringer i den praktiske arbeidshverdagen.

Løsningen må støtte, men ikke være begrenset til:

- **Moderne automatisert og dynamisk tilgangsstyring** med sikker flerfaktorautentisering (nivå 4), rollebasert tilgang og funksjonalitet for automatisk utlogging, som sikrer at helsepersonell identifiseres korrekt og kun gis autorisert tilgang til det de har tjenstlig behov for (Zero Trust).
- **Sikker kommunikasjon** internt gjennom sterk ende-til-ende-kryptering og sikre protokoller for trafikkflyt internt og eksternt.
- **Logging og overvåking** av aktivitet i tråd med Normen, inkludert rutiner for hendelseshåndtering og analyse som bidrar til tidlig oppdagelse av brudd.

- **Trygg lagring** av data i ro, i trafikk og i bruk, og en isolering av disse mot eventuelle andre kunder i leverandørens portefølje.
- **Høy tilgjengelighet** gjennom redundans, failover, regelmessig sikkerhetstesting og gode gjenopprettingsrutiner.
- **Risikostyring** og trusselvurdering basert på ISO-standarder eller tilsvarende rammeverk, som tar høyde for den kommende Digitalsikkerhetsforskriften.

EPJ-løsningen må kunne dokumentere overholdelse av regelverk og opprettholde akseptabel risiko for oppdragsgiver, samtidig som den legger til rette for effektiv og trygg pasientbehandling.

| Nr | Kundens behov |
|---|---|
| | **Dokumentasjonskrav:** |
| | systemets informasjonssikkerhet og innebygde personvern som viser hvordan dette er ivaretatt i alle faser av produktutviklingen. |
| | systemets datasikkerhet og de tekniske og organisatoriske sikkerhetstiltakene i Løsningen, inkludert isolering og sikring av oppdragsgivers data fysisk eller logisk, samt en rapport som evaluerer potensielle interne og eksterne angrep. |
| | systemets robusthet og tilgjengelighet i form av redundans, failover, gjenopprettingsrutiner og prosedyrer. Dette inkluderer dokumentasjon på prosesser som verifiserer at sikkerhetskopier er fullstendige, intakte og pålitelige for gjenoppretting, og at disse prosedyrene regelmessig gjennomføres og testes. |
| | beredskapsplaner, nylig gjennomførte beredskapsøvelser og evalueringen av disse i form av tiltak og forbedringspunkter. |
| | risikostyring og trusselvurdering basert på ISO-standarder eller tilsvarende rammeverk, som inkluderer årlige vurderinger og gjennomganger av hendelser, trusler og tiltak. |
| | Hendelseshåndtering (IRP) som inkluderer kritiske underleverandører og sårbarhetskartlegging av løsningskomponenter. Videre ønskes en prosedyre for regelmessig sikkerhetstesting basert på anerkjente rammeverk. |
| | high-level-design (HLD) og detailed-design (DLD). |
| | åpne kildekode- eller tredjepartskomponenter som benyttes, inkludert en eventuell juridisk og økonomisk vurdering av implikasjoner. |
| | teknisk arkitektur og meldingsflyt i Løsningen. Denne skal vise alle komponenter, kommunikasjonslenker med detaljer om kryptering, protokoller, ansvar og lokasjon, og tydelig markere når kommunikasjon går over internett. Oversikten bør være på et nivå som gjør at drifts- og sikkerhetspersonell hos oppdragsgiver forstår informasjonsflyten. |
| | dokumentasjon av test- og produksjonsmiljø, inkludert beskrivelse av eksterne integrasjoner for hvert enkelt miljø. |
| | Leverandøren skal helhetlig dokumentere prosedyre og strategi for overvåkning av kritiske tjenester og retningslinjer for behandling av tilhørende data i hele verdikjeden. |

| | |
|---|---|
| | |
| | Leverandøren skal loggføre aktivitet knyttet til bruk og innsyn i pasientinformasjon både på infrastrukturnivå og i informasjonssystemer, og gi oppdragsgiver tilgang til loggene. Dette inkluderer, men er ikke begrenset til:<br><br>Ordinære brukere og systemadministratorers autoriserte aktivitet.<br>Konfigurasjons- eller programvareendringer.<br>Bruk av selvautorisering eller forsøk på uautorisert bruk av system eller infrastruktur. |
| | Leverandøren skal fremvise rutiner for analyse av logger i henhold til Normen, for tidlig oppdagelse av hendelser og eventuelle databrudd, og prosedyre for varsling av oppdragsgiver. |
| | Leverandøren skal ha rutiner, organisatoriske tiltak og systemtekniske sikkerhetstiltak for å oppdage, håndtere og varsle om hendelser, brudd og avvik som får konsekvenser for informasjonssikkerhet eller personvern. Med mindre brudd og avvik er av ubetydelig karakter, skal det meldes til kunden uten ugrunnet opphold. Leverandøren skal i tillegg ha rutiner for øving på håndtering av hendelser, og vise dokumentasjon på gjennomføring av øvelser ved forespørsel fra Kunden. |
| | Leverandøren bør gi Kunden mulighet til å overvåke og bekrefte tjenestens tilgjengelighet, som inkluderer en mekanisme for overvåkning og rapportering av eventuell nedetid eller tilgjengelighetsproblemer |
| | Leverandøren skal sikre at uvedkommende ikke får tilgang til infrastruktur og sørge for at lagringsmedia slettes sikkert etter bruk. |
| | Løsningen bør la flere brukere arbeide på samme pasient samtidig uten noen form for låsing, og uten tap av data. |
| | Leverandøren skal kryptere kommunikasjon og lagrede helse- og personopplysninger med sterke kryptomekanismer i henhold til NSMs anbefalinger for kryptografi. Leverandøren skal risikovurdere all ukryptert kommunikasjon og lagring av annen informasjon og data. |
| | Leverandøren skal autorisere all tilgang til helse- og personopplysninger. Løsningen skal ha granulær tilgangskontroll med bruk av roller og rettigheter. Konfigurasjon og tilpasning av roller og rettighetsstyring skal være tilgjengelig for Kunden.<br><br>Løsningen skal ivareta at brukere jobber ved ulike avdelinger og har ulike roller. Leverandøren skal beskrive hvordan autorisasjon, tilgangskontroll, konfigurasjon av roller og rettigheter fungerer i Løsningen. Løsningen skal være i henhold til Normens krav til tilgangsstyring og veileder for tilgang til helse- og personopplysninger. |
| | Løsningen bør støtte provisjonering av brukere og roller via EntraID, og bruke Azure AD sikkerhetsgrupper eller Azure applikasjonsroller. Det er en fordel med standard API i samsvar med SCIM-standarden, men dersom dette ikke støttes bør Løsningen støtte synkronisering basert på søkefilter eller sikkerhetsgrupper.<br><br>Synkronisering bør være dokumentert med oversikt over hvilke attributter som synkroniseres. Leverandør bes beskrive hvordan dette ivaretas. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| | Løsningen bør gi mulighet til innlogging ved bruk av ID-porten for tjenestemottakere og pårørende. |

| | |
|---|---|
| | Løsningen bør ha en ikke-overskrivbar backup. Backup av data i løsningen bør lagres i et annet datasenter enn det den kjøres i.<br><br>Leverandør bes beskrive backup-løsningen og prosedyren for sikkerhetskopiering inkludert detaljer om metoder, frekvens, og lagringsmetoder for sikkerhetskopiene. |
| | Løsningen bør støtte sammenstilling og bruk av attest fra nasjonalt felles tillitsrammeverk. Løsningen bør støtte sikring av eget API med HelseID.<br><br>Det er ønskelig med støtte for autorisasjon ved bruk av token-claim tilhørende felles tillitsrammeverk.<br>Løsningen bør støtte bruk av HelseID Selvbetjenings-API via delegerte rettigheter fra Kunde. |
| | Dersom løsningen leveres som en applikasjon til mobile enheter, skal den distribueres via Apple og Google sine offisielle butikker, Apple AppStore og Google Play Store. |
| | Leverandøren skal levere en liste over eventuelle minimumskrav til hardware som skal benytte Løsningen. Videre bør leverandøren kunne levere en oversikt over godkjente enheter og programvare som kan brukes i leveransen, som inneholder detaljer om funksjoner og prosedyrer som sikrer at kun sikker og godkjent programvare og utstyr brukes. |
| | Leverandør bør tilby et testmiljø for all funksjonalitet i Løsningen som Kunden har tilgang til. Testmiljøet skal inneholde representativ syntetisk data og være integrert med alle relevante nasjonale og lokale tjenester og applikasjoner. Det bør være mulig for Kunden å enkelt legge til eller endre på testdata via API. Testmiljøet skal brukes til for eksempel testing av funksjoner, integrasjoner, opplæring og feilsøking. Leverandør bes beskrive hvordan dette ivaretas. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |

## Eierskap

| Nr. | Kundens krav |
|---|---|
| 1 | Alle data som lagres i tilbudt løsning er oppdragsgivers eiendom, også etter endt avtaleforhold.<br><br>Tilbyder har ikke under noen omstendighet rett til å utøve tilbakeholdsrett i kundens data. |
| 2 | Kunden skal ha tilgang til alle kundegenererte data som lagres i løsningen i et digitalt format, eksempelvis via API eller som XML-eksport. Dette inkluderer tilgang ved avslutning og migrering til annen eller ny løsning, og en eventuell kostnad ved datauttrekk skal beskrives i prisskjemaet. |
| 3 | Løsningen bør gjøre data automatisk tilgjengelig for sekundærbruk både til rapporterings- og styringsdata og i kommunens dataplattform/datasjø. Leverandør bes beskrive tilnærming og metodikk for håndtering av dette. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |
| 4 | Løsningen bør dele data med eksisterende analyseverktøy i kommunen og/eller analyseverktøy fra leverandør, eksempelvis Power BI. Leverandør vil bli vurdert ut fra tilnærming til løsning av kravet. |