

Helseanalyseplattformens data- og analyseplattform

Kravspesifikasjon v0.5

Versjon: 0.5

Dato: 21.05.2019

|  |
| --- |
|  |



Innhold

[1 Introduksjon 4](#_Toc9328548)

[2 Bakgrunn og målbilde 5](#_Toc9328549)

[Overordnet målbilde Helseanalyseplattformen 5](#_Toc9328550)

[Etablering av et økosystem 7](#_Toc9328551)

[Personvern og informasjonssikkerhet 8](#_Toc9328552)

[3 Kundens overordnede plan for implementering 9](#_Toc9328553)

[Stegvis etablering av Helseanalyseplattformen 9](#_Toc9328554)

[Stegvis etablering av Helsedataservice 9](#_Toc9328555)

[Forslag til overordnet nedbrytningsstruktur knyttet til anskaffelsen 11](#_Toc9328556)

[4 Funksjonelle krav (EPOS) 14](#_Toc9328557)

[Data- og analysetjenester 14](#_Toc9328558)

[4.1.1 Analyserom 14](#_Toc9328559)

[4.1.2 Brukerflater 17](#_Toc9328560)

[4.1.3 Åpne data 19](#_Toc9328561)

[4.1.4 Kohortutforsker 20](#_Toc9328562)

[4.1.5 Anonymisert analyse 21](#_Toc9328563)

[4.1.6 Syntetiske data 22](#_Toc9328564)

[4.1.7 Tilgjengeliggjøring av data 24](#_Toc9328565)

[Helseregister på Helseanalyseplattformen 26](#_Toc9328566)

[4.1.8 Helseregister som en tjeneste 26](#_Toc9328567)

[4.1.9 Registerforvalters forkammer 27](#_Toc9328568)

[Innbyggertjenester 27](#_Toc9328569)

[4.1.10 Innsyn og tilbakemelding 27](#_Toc9328570)

[4.1.11 Dialog mellom forsker og innbygger 28](#_Toc9328571)

[5 Utforming av Helseanalyseplattformen 30](#_Toc9328572)

[Dataplattform 30](#_Toc9328573)

[Integrasjon av datakilder inn på dataplattformen 32](#_Toc9328574)

[Integrasjon mot andre løsninger og grensesnitt 33](#_Toc9328575)

[Antatt nødvendige tekniske kapabiliteter 35](#_Toc9328576)

[5.1.1 Dataforvaltning 36](#_Toc9328577)

[5.1.2 Sikkerhet 37](#_Toc9328578)

[5.1.3 Analyseverktøy 38](#_Toc9328579)

[5.1.4 Integrasjon 39](#_Toc9328580)

[5.1.5 Administrasjonsverktøy 40](#_Toc9328581)

[5.1.6 Infrastruktur 42](#_Toc9328582)

[5.1.7 Utviklerverktøy 43](#_Toc9328583)

[6 Kvalitetskrav 44](#_Toc9328584)

[6.1.1 Ytelse 44](#_Toc9328585)

[6.1.2 Kompabilitet 45](#_Toc9328586)

[6.1.3 Brukskvalitet 46](#_Toc9328587)

[6.1.4 Robusthet 48](#_Toc9328588)

[6.1.5 Sikkerhet 50](#_Toc9328589)

[6.1.6 Vedlikeholdbarhet 57](#_Toc9328590)

[6.1.7 Portabilitet 59](#_Toc9328591)

# Introduksjon

Dette dokumentet inneholder det foreløpige utkastet til kravspesifikasjonen som Direktoratet for e-helse har tenkt å benytte i utlysningen av data- og analysetjenester for Helseanalyseplattformen. Vi velger å publisere dette utkastet åpent for å gi potensielle leverandører og andre interessenter en mulighet til å gi innspill på kravspesifikasjonen, samt dele informasjon om hvor vi står i arbeidet. I tillegg ønsker vi med dette å gi leverandørene bedre tid til å utforme løsninger for Helseanalyseplattformen. Tidspunkt for publisering av selve anskaffelsen er ikke besluttet, men vi legger opp til at fristen for søknad om deltakelse i konkurransen vil være ila Q3 2019.

I forbindelse med utkastet til krav til Helseanalyseplattformen er vi spesielt ute etter innspill knyttet til

* Er det områder i kravspesifikasjon som er dårlig beskrevet og som gjør det krevende å forstå hva vi ønsker å oppnå?
* Er det krav eller brukerhistorier leverandørene mener vi har glemt og som vi bør inkludere som en del av anskaffelsen?
* Er det krav eller brukerhistorier som leverandørene mener undergraver konseptet som skal realiseres?
* Er det krav eller brukerhistorier som peker seg ut som svært krevende og lite kostnadseffektivt å implementere?
* Bør vi gjøre fundamentale endringer i vårt forslag til overordnet nedbrytningsstruktur (arbeidsstrømmer) av realiseringen av Helseanalyseplattformen?
* Har leverandørene innspill til hvordan vi bør evaluere tilbudene?

Ut over dette tar vi gjerne imot alle typer innspill som leverandørene, eller andre måtte ha til kravspesifikasjonen.

Tilbakemeldinger og innspill kan gjerne gjøres ved å kommentere direkte i dette dokumentet og/eller oppsummere innspillene i et eget dokument. Tilbakemeldinger kan sendes til [helsedataprogrammet-anskaffelser@ehelse.no](mailto:helsedataprogrammet-anskaffelser@ehelse.no) innen 04.06.2019. Vi har dessverre ikke kapasitet til å gjennomføre 1-1 møter med alle leverandører i denne fasen og ber om forståelse for det. Hvis det imidlertid er innspill vi får i de skriftlige tilbakemeldingene som gjør at vi mener det er nødvendig med et møte for ytterligere detaljer så åpner vi for dette.

# Bakgrunn og målbilde

## Overordnet målbilde Helseanalyseplattformen

I April 2018 leverte Direktoratet for e-helse en konseptvalgutredning[[1]](#footnote-2) der konsept 7 – Analyseøkosystem ble anbefalt. Dette konseptet ble besluttet gjennomført av Regjeringen i Desember 2018. Konseptvalgutredningen beskriver på et overordnet nivå målbildet for Helseanalyseplattformen.

Konseptet går ut på å etablere et økosystem for helseanalyse. For å utnytte potensialet i helsedataene og tilrettelegge for økt sekundærbruk skal programmet realisere et økosystem, med en nasjonal Helseanalyseplattform som en del av kjernen. Den tekniske og organisatoriske utviklingsretningen som er staket ut de neste årene er basert på en helhetlig vurdering av samfunnsøkonomisk lønnsomhet, personvernkonsekvenser, risiko- og sårbarhetsvurdering, i kombinasjon med innspill fra aktørene og erfaringene som er bygget i programmets første to år.

Programmet skal også etablere et forvaltnings- og finansieringsregime rundt Helseanalyseplattformen for å forenkle tilgangen til og styrke arbeidet med norske helsedata. Helseanalyseplattformen skal gjennom tilgjengeliggjøring av helsedata og etablering av avansert analysefunksjonalitet bidra til bedre helseforskning og mer innovasjon og næringsutvikling basert på bruk av helsedata. Bedre bruk av helsedata til styring og administrasjon vil føre til mer kunnskapsbaserte helsetjenester og riktigere ressursbruk i helsetjenesten.

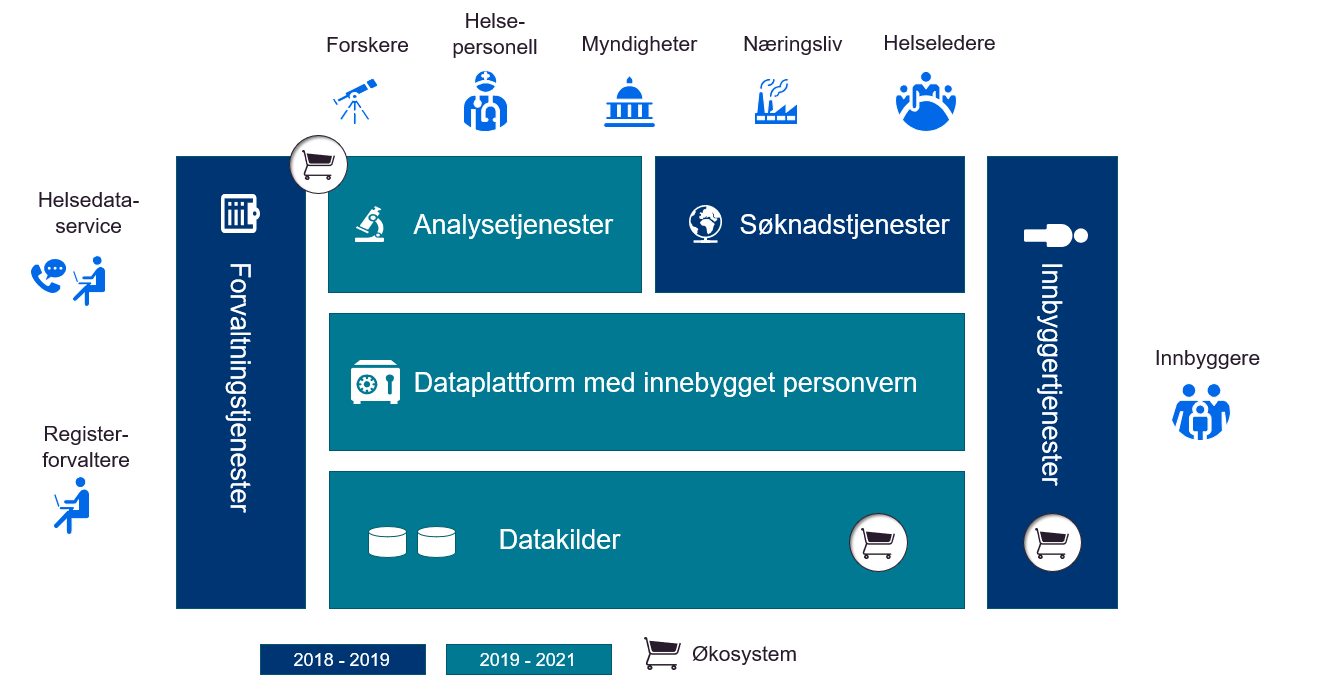
Helsedataprogrammet skal også bidra til å etablere fellestjenester for bruk av helseregistrene og andre relevante datakilder, slik at de ikke trenger å utvikle, forvalte og drifte denne funksjonaliteten selv. Bruk av fellestjenester skal bidra til å heve datakvaliteten og automatisere forvaltningen, samtidig som at investeringer i fellestjenestene gjøres én gang i fellesskap fremfor at registrene tar denne kostnaden hver for seg. Helsedataprogrammet har i tillegg en koordinerende rolle for å drive frem kodeverk, terminologi og tekniske standarder som brukes i helseregistrene og de andre datakildene som skal ligge til grunn for helseanalyser.

Vi definerer et analyseøkosystem som kombinasjonen av et juridisk grunnlag, et bredt samarbeid mellom offentlige virksomheter, tekniske løsninger og standarder, et sikkerhetsregime og et merkantilt rammeverk. I dette økosystemet er eier av plattformen, tjenesteleverandører og brukere avhengig av hverandre. Økosystemer setter scenen for innovasjon ved at private/offentlige selskaper får mange nye forretningsmuligheter, gjennom utnyttelse av nettverkseffekter som økosystemet skaper.

Analyseøkosystemet skal forsterke personvernet gjennom redusert eksponering av data om individet, og øke den enkeltes kontroll over hvordan personopplysninger brukes.

Målbildet for analyseøkosystemet omfatter digitale tjenester og etablering av nye offentlige tjenester med helseforskere, myndigheter, helsepersonell, næringslivet, innbyggere og helseledere som målgrupper. Disse brukergruppene har ulike behov som i stor grad kan betjenes av de samme tekniske løsningene og organisatoriske funksjonene.

De tekniske komponentene som skal etableres skal i hovedsak legge til rette for innbyggertjenester, data- og analysetjenester, søknads- og veiledningstjenester, samt forvaltningstjenester. Det skal i tillegg etableres en ny servicefunksjon for brukere av helsedata i henhold til Helsedatautvalgets[[2]](#footnote-3) anbefaling om å etablere en sentral tilgangsforvalter (heretter beskrevet som Helsedataservice). Helsedataservice vil bestå av en sentral organisasjon med vedtaksmyndighet og baseres på et nettverkssamarbeid mellom dagens registerforvaltere og andre myndigheter.



Figur 1: Overordnet illustrasjon av Helseanalyseplattformens målbilde

Direktoratet for e-helse har lagt noen sentrale prinsipper til grunn for realisering av analyseøkosystemet:

1. Helseanalyseplattformen skal realiseres stegvis både når det gjelder funksjonalitet og datakilder
2. Brukergruppen forsker har prioritet i første versjon av Helseanalyseplattformen
3. De store, komplekse løftene knyttet til etablering av Helseanalyseplattformen må tas i programperioden
4. Det må etableres et fundament i form av en dataplattform før analyseøkosystemet kan realiseres
5. Nye søknadstjenester må dekke et bredt spekter av datakilder selv om Helseanalyseplattformen ikke inkluderer alle disse datakildene i en tidlig versjon
6. Helsedataprogrammet skal som prinsipp ikke bygge ferdig innsikt- og analyseprodukter, men legge til rette for at dette skal kunne gjøres enklere gjennom enklere tilgang på data- og analyseinfrastruktur
7. Helseanalyseplattformen skal kunne realiseres gjennom bruk av skytjenester
8. Helseanalyseplattformen skal, der det er hensiktsmessig, gjenbruke tjenester og infrastrukturer som allerede finnes

## Etablering av et økosystem

Plattformbegrepet knyttes ofte til moderne løsninger som for eksempel Google og Apple. Disse kjennetegnes ved at det er tre hovedaktører på en og samme tekniske plattform;

* Plattformeier
* Leverandører
* Brukere

Alle aktørene har en sterk interesse i og nytte av at plattformen utvikles videre.

Et analyseøkosystem har de samme egenskapene som plattformene nevnt over. Det må være en sentral eier og forvalter, en rekke tilbydere av data, analyseverktøy og -tjenester i et "marked" på plattformen og brukere bestående av forskere i offentlig og privat sektor, myndighetsaktører, ledere i helsesektoren osv. I tillegg vil det også i analyseøkosystem være tjenesteleverandører og utviklere som utvikler løsninger og tjenester basert på plattformen.

Fra vårt ståsted er økosystembegrepet knyttet til flere dimensjoner:

1. Økosystem av analyseverktøy: Vi ønsker å etablere en teknisk løsning der mange ulike aktører kan tilby sine analyseverktøy og analysetjenester gjennom Helseanalyseplattformen.
2. Økosystem av aktører som driver med helseanalyse: Vi ønsker å etablere en infrastruktur der mange ulike aktører, både offentlige og private, kan etablere helseanalyseløsninger.
3. Økosystem av dataleverandører: Vi ønsker å etablere et økosystem av dataleverandører slik at data fra mange ulike virksomheter kan tilgjengeliggjøres gjennom Helseanalyseplattformen
4. Økosystem mot andre økosystem: Analyseøkosystemet må også sees i sammenheng med andre nasjonale og internasjonale økosystemer.

## Personvern og informasjonssikkerhet

Personvern handler om retten til privatliv og retten til å bestemme og ha kontroll over egne personopplysninger. Helsedataprogrammet har utviklet seks prinsipper for å ivareta innbyggers personvern. Ved etablering av Helseanalyseplattformen skal innbygger alltid kunne være trygg på at disse prinsippene blir ivaretatt.

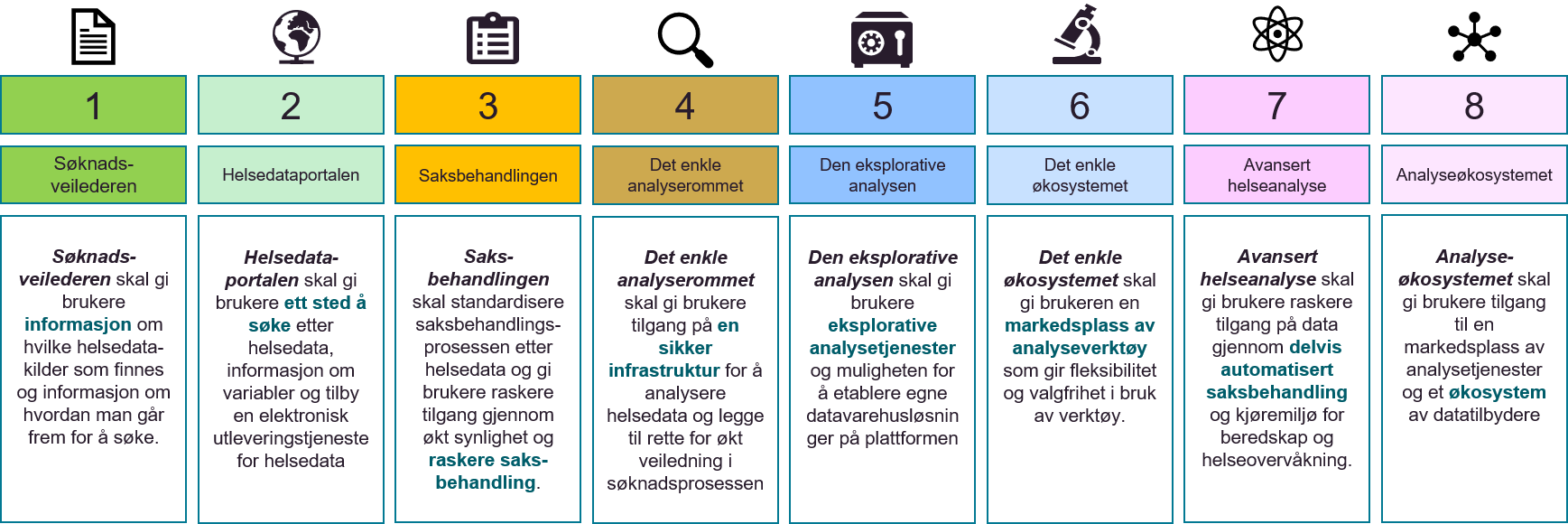
1. Behandling av mine personopplysninger skal alltid være lovlig og rettferdig
2. Jeg skal raskt og enkelt kunne se hvilke personopplysninger som er lagret om meg
3. Jeg skal raskt og enkelt kunne få vite hvordan opplysninger om meg behandles, og hvem som har tilgang
4. Jeg skal umiddelbart få beskjed dersom det er brudd på sikkerheten ved behandling av personopplysninger om meg
5. Jeg skal kunne samtykke til og reserverer meg mot enkelte typer behandling av personopplysninger om meg
6. Mine personopplysninger skal alltid være riktige, og jeg skal kunne bidra til å rette opp feil

Etablering av Helseanalyseplattformen vil medføre at det behandles et stort antall særlig kategorier av personopplysninger (sensitive personopplysninger). Med særlig kategorier av personopplysninger menes en rekke kategorier av opplysninger som har et særskilt vern, jf. personvernforordningen (GDPR) artikkel 9. Dette er opplysningskategorier slik som rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, fagforeningsmedlemskap, samt helseopplysninger. For Helseanalyseplattformen vil det i hovedsak behandles helseopplysninger. I det følgende vil sensitive personopplysninger blir brukt som betegnelse.

I Helseanalyseplattformen vil det bli behandlet store mengder sensitive personopplysninger og konsolidering og integrasjon av ulike datakilder medfører at de potensielle konsekvensene av brudd på personvernet og informasjonssikkerhet er store. Det er på denne bakgrunn behov for mekanismer som gir tillit til at alle aspekter ved personvernet og informasjonssikkerhet er tilfredsstillende ivaretatt. Det vil bli stilt strenge krav til utvikling og etablering av Helseanalyseplattformen og det er en forutsetning at enhver tid gjeldende regelverk for informasjonssikkerhet og behandling av personopplysninger etterleves.

# Kundens overordnede plan for implementering

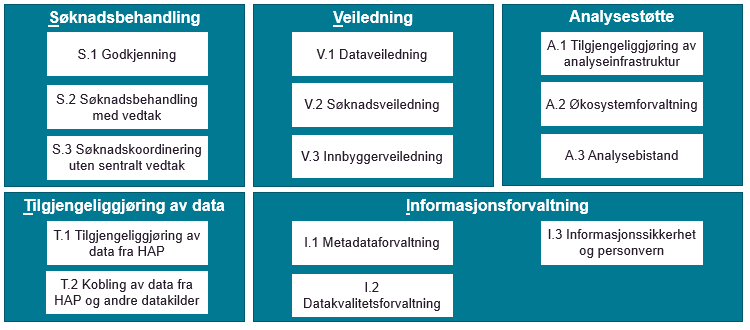
## Stegvis etablering av Helseanalyseplattformen

Figur 1 illustrerer på overordnet nivå den anbefalte stegvise etableringen av Helseanalyseplattformen som kunden bruker som overordnet veikart på utvikling av plattformen. Denne anskaffelsen omfatter store deler av steg 4-8. Her må imidlertid noen løsninger også sees i sammenheng med løsninger som er omfattet av anskaffelsen på søknad- og saksbehandling. I tillegg vil også andre leverandører og partnere etter planen levere analysetjenester og -verktøy knyttet til økosystemet. 

Figur 2: Illustrasjon av stegvis utvikling av Helseanalyseplattformen

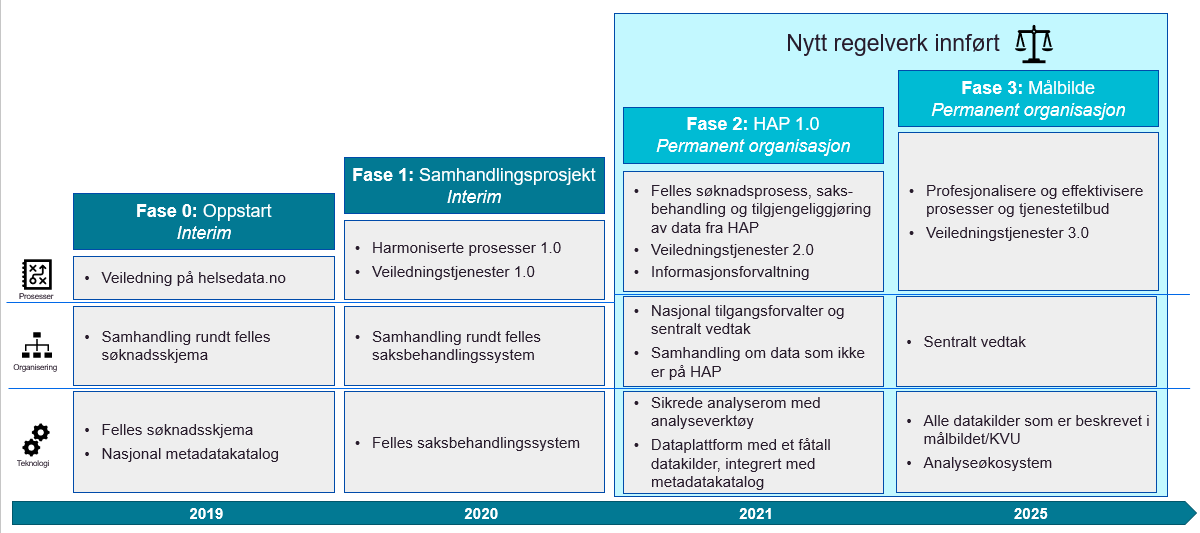
## Stegvis etablering av Helsedataservice

Helsedataservice er navnet på den nye tjenesteorganisasjonen som skal være ansvarlig for Helseanalyseplattformen. Målbildet for Helsedataservices forretningsarkitektur inkluderer forretningskapabiliteter innenfor Søknadsbehandling, Veiledning, Tilgjengeliggjøring av data, Analysestøtte og Informasjonsforvaltning. Dette er illustrert i Figur 2: Kjernekapabiliteter for Helsedataservice. Forretningsarkitekturen vil realiseres stegvis i takt med den teknologiske utviklingen av Helseanalyseplattformen, samt regelverksutviklingen som drives av Helse- og omsorgsdepartementet (HOD).



Figur 3: Kjernekapabiliteter for Helsedataservice

Tilsvarende den stegvise utviklingen av den tekniske plattformen, har vi også definert en stegvis utvikling for Helsedataservice. Denne utviklingen er beskrevet gjennom fire steg og illustrert i Figur 3.



Figur 4: Helsedataservice vil utvikles i faser i samsvar med teknisk og juridisk utvikling

**Helsedataservice fase 0**, "**Oppstart interim",** er planlagt startet høsten 2019 rundt samme tid som innføringen av et felles søknadsskjema. Helsedataservice vil i denne fasen ikke ha ansvar for saksbehandling, vedtak og tilgjengeliggjøring av data, men vil ha en koordinerende rolle innenfor søknadsbehandling og etablering av metadata for registervariabler. Helsedataservice vil også tilby enkle veiledningstjenester, hovedsakelig gjennom nettstedet helsedata.no og felles søknadsskjema, samt gjennom 1.linje brukerstøtte.

**Helsedataservice fase 1, "Samhandlingsprosjekt interim",** starter når felles saksbehandlingssystem innføres i registerforvaltningen. Organisasjonen vil her fortsette å jobbe med å harmonisere prosesser for søknads- og saksbehandling, samt å forbedre veiledningstjenestene. I tillegg vil Nasjonal metadatakatalog utvides med metadata fra flere helseregistre, og arbeidet med å harmonisere variabler kan begynne.

**Helsedataservice fase 2, "HAP 1.0 permanent organisasjon",** starter når et nytt regelverk innføres. Dette vil etter planen medføre at Helsedataservice får hjemmel for å etablere en dataplattform med helseregisterdata, samt vedtaksmyndighet for tilgjengeliggjøring av data. Fra og med denne fasen vil derfor resterende forretningsfunksjoner innenfor søknadsbehandling, tilgjengeliggjøring av data, analysestøtte og informasjonsforvaltning, realiseres. Det vil i starten av denne fasen kun være et fåtall datakilder på dataplattformen på HAP slik at behovet for samhandling om data som ikke er på HAP, vil være stort.

Hvis regelverksutviklingen blir forsinket eller hvis det ikke blir vedtatt nytt regelverk, vil det få konsekvenser for Helsedataservice ved at man forblir i fase 1.

Overgangen mellom **Helsedataservice** **fase 2** og **Helsedataservice fase 3, "Målbilde permanent organisasjon",** vil skje gradvis ved at tjenestene som tilbys videreutvikles i tråd med den stegvise realiseringen av Helseanalyseplattformen. I fase 3 vil dataplattformen være implementert med de planlagte datakildene og analyseøkosystemet vil være etablert med tjenesteprodusenter og -konsumenter.

## Forslag til overordnet nedbrytningsstruktur knyttet til anskaffelsen

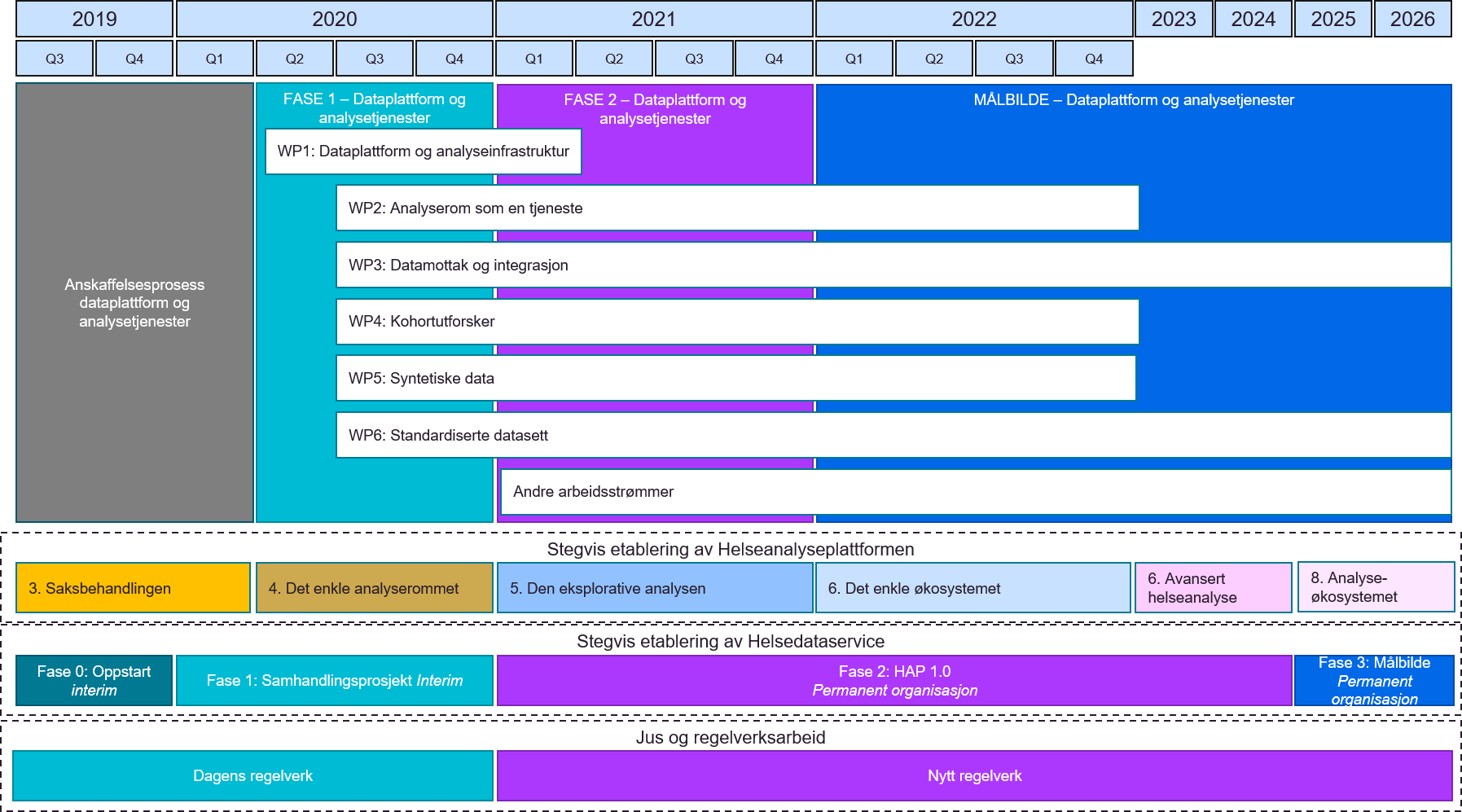
På grunn av eksterne rammebetingelser, vil det være løsninger og tjenester som ikke kan etableres umiddelbart. Noen viktige rammebetingelser som leverandørene bør være oppmerksomme på er:

* Behandlingsgrunnlaget for data på Helseanalyseplattformen avhenger av regelverk- og forskriftsarbeidet som ledes fra Helse- og omsorgsdepartementet (HOD). Planen som ligger til grunn fra HOD sin side er at nytt regelverk vil tidligst være gjeldende 01.01.2021
* Integrasjonsarbeid mot andre virksomheter (for eksempel registerforvaltere) avhenger av tett samarbeid i både planlegging og gjennomføring sammen med eksterne virksomheter.
* Helsedataprogrammets finansiering er i stor grad basert på årlige tilskudd over statsbudsjettet. Dette vil påvirke realiseringshastighet.
* Helsedataprogrammet vil etter planen gå ut 2020, men det vurderes hvorvidt programperioden bør utvides med ett år.

Figur 4 illustrerer sammenhengen mellom programmets stegvise realiseringsstrategi av hhv Helseanalyseplattformen og Helsedataservice opp imot rammebetingelsen rundt regelverksutvikling, samt forslag til arbeidsstrømmer knyttet til denne anskaffelsen som skal realisere løsninger og tjenester på Helseanalyseplattformen.

Vi ser for oss en fasebasert tilnærming, der fase 1 har en direkte sammenheng med regelverksutviklingen på den måten at alt som realiseres av tjenester i denne fasen, er mulig å realisere i henhold til gjeldende regelverk. Fase 2 på sin side er basert på en antakelse om at nytt regelverk må være tredd i kraft.

*Hvis Leverandøren har forslag til en annen nedbrytningsstruktur som er mer hensiktsmessig, eller mener at løsninger i målbildet enkelt kan, og bør inkluderes som en del av fase 1 ønsker vi å vite om dette og ber om at dette beskrives.*



Figur 5: Kundens forslag til faseinndeling og arbeidsstrømmer for anskaffelsen

Vår foreslåtte tilnærming til fase 1 er at det først må etableres et "fundament" i form av en data- og analyseplattform der sensitive personopplysninger kan behandles og sluttbrukertjenester kan bygges/tilbys. En viktig del av denne jobben er å etablere mekanismer og prosesser som håndterer informasjonssikkerhet og personvern.

Når dette er etablert kan man begynne jobben med å etablere data- og analysetjenester som kan tilbys til sluttbrukere. For fase 1 ønsker vi å etablere flere "minimumsprodukter" (MVPer) slik at løsningene kan testes mot sluttbrukere og man i senere faser kan gjøre endringer i henhold til konkrete brukerbehov.

Vi foreslår derfor en nedbrytning i følgende arbeidsstrømmer for fase 1.

* WP1: Dataplattform og analyseinfrastruktur
* WP2: Analyserom som en tjeneste
* WP3: Datamottak og integrasjon
* WP4: Kohortutforsker
* WP5: Syntetiske data
* WP6: Standardiserte datasett

Vi ser for oss at mange av disse arbeidsstrømmene vil fortsette i fase 2 🡪.

**WP1: Etablering av dataplattform og analyseinfrastruktur**

Formålet med denne arbeidspakken er å etablere den sentrale infrastrukturen som gjør det mulig å lagre og forvalte helsedata på en sikker måte, samt etablere utviklingsplattformen som må på plass for at prosjektet skal kunne etablere digitale tjenester til sluttbrukere. Infrastrukturen må knyttes til helsenettet.

**WP2: Analyserom som en tjeneste**

Formålet med denne arbeidspakken er å kunne tilby analyserom som en tjeneste til sluttbrukere. På sikt vil det tilbys ulike typer analyserom med ulike kapabiliteter til ulike brukere, men for fase 1 ser vi for oss at man etablerer "det enkle analyserommet". I dette legger vi et sikkert sandkassemiljø med open source analyseverktøy der sluttbrukere kan håndtere og analysere sensitive personopplysninger.

**WP3: Datamottak og integrasjon**

Formålet med denne arbeidspakken er å knytte helseregistre og andre datakilder til plattformen. Dette vil være en arbeidspakke med mange leveranser og vil gå utover fase 1 slik den er definert. I fase 1 vil det i utgangspunktet ikke etableres fullstendige kopier av registre på plattformen, men det er nødvendig å jobbe aktivt også i fase 1 for at dette skal skje. Her vil det derfor være nødvendig å opprette gode testdata.

**WP4: Kohortutforsker**

Formålet med denne arbeidspakken er å etablere første versjonen av en kohortutforsker. Dette er en løsning rettet mot forskere der de kan filtrere på reelle helsedata gjennom definerte inklusjon- og eksklusjonskriterier for å identifisere den potensielle størrelsen av en kohort/utvalg. Resultatet vil være anonymt. Nivået og kompleksiteten av kohortutforskeren i fase 1 vil være direkte knyttet til dagens regelverk rundt hvilken databehandling som kan gjøres.

**WP5: Syntetiske data**

Formålet med denne arbeidspakken er å etablere verktøy og metoder for generering av syntetiske data slik at disse kan benyttes forskningsformål. En viktig egenskap ved syntetiske data er at de har tilsvarende statistiske egenskaper som reelle data, samtidig som det ikke skal være mulig å identifisere enkelt individer.

**WP6 Standardiserte datasett**

Formålet med denne arbeidspakken er å etablere standardiserte datasett som går på tvers av registre og legge opp til en søknadsprosess som i stor grad er automatisert. I fase 1 ser vi for oss at hovedfokuset vil være å definere en informasjonsmodell som vil danne grunnlaget for en hensiktsmessig måte å håndtere og tilgjengeliggjøre data på. Informasjonsmodellen vil danne basis for kvalitetssikrede, standardiserte datasett på tvers av helseregistre og vil være sentral for ulike tilgjengeliggjøringer av data, blant annet APIer. Dagens helseregistre er hendelsesbaserte og hendelsene er knyttet til personer. Mange hendelser vil være relaterte og knyttet til forløp. For mange formål det derfor være veldig interessant å kunne se hendelser sammen som forløp, men det er svært utfordrende å gjøre dette på en generisk måte.

# Funksjonelle krav (EPOS)

Vi har valgt å beskrive mange av de funksjonelle kravene som brukerhistorier fordi vi ønsker å gi leverandørene mest mulig spillerom i design av løsning. Brukerhistoriene beskriver hvilket problem en bestemt sluttbruker ønsker løst, og hvorfor sluttbrukeren ønsker dette løst, ikke hvordan.

I tillegg til brukerhistoriene vil det også stilles mer tradisjonelle funksjonelle krav samt kvalitetskrav.

Brukerhistoriene i dette dokumentet **står ikke i prioritert rekkefølge**. Prioritering vil komme på et senere tidspunkt.

## Data- og analysetjenester

### Analyserom

|  |
| --- |
| **Tittel: Analyserom** |
| **EPOS**  Som bruker ønsker jeg tilgang til helsedata og en sikker og skalerbar data- og analyseinfrastruktur slik at jeg kan analysere data på en rask, effektiv og sikker måte. |
| **Beskrivelse**  Forskere har behov for en sikker, men fleksibel analyseinfrastruktur som tilbyr et bredt spekter med analyseverktøy, samt funksjonalitet for å lagre data, validere data og sammenstille data. Forskere har også behov for å kunne importere egne data inn i analyserommet slik at data som forsker har samlet inn på egen hånd eller fått utlevert fra andre steder kan sammenstilles med helsedata fra HAP. Dataleveranser fra Helsedataservice vil hovedsakelig være ad-hoc leveranser i etterkant av søknader om bruk av data. Forskere har også behov for at data og analyser arkiveres i etterkant av prosjektet slik at resultatene fra forskningsprosjektet er etterprøvbare. Selve analyseinfrastrukturen må være fleksibel hva gjelder lagring og prosessering og forsker må på en enkel måte kunne øke, eller redusere kapasitet ettersom behovet i prosjektet endres.  Myndighetsaktører har behov for en sikker, men fleksibel analyseinfrastruktur på mange måter likt det som er beskrevet i avsnittet over. I tillegg til behovet for avanserte analyseverktøy tilsvarende det forskere har behov for, har også myndighetsaktører behov for tilgang til mer tradisjonelle visualisering/business intelligence (BI) verktøy for å bygge og publisere statistikk og rapporter, samt mulighet for å bygge og operasjonalisere algoritmer. Myndighetsaktører har også behov for funksjonalitet for å lagre data, validere data og sammenstille data. Videre har enkelte myndighetsaktører behov for å etablere permanente sammenstillinger av data på plattformen.  Næringslivsaktører har behov som er sammenfallende med både forskere og myndighetsaktører. Næringslivsaktører vil for eksempel ha behov for å monitorere innføring av nye legemidler i forbindelse med bivirkningsovervåkning eller for å overvåke bruk og effekt. I denne sammenhengen trenger de den sammen typen funksjonalitet som myndighetsaktører, beskrevet over. Næringslivet bedriver også forskning og forskningsliknende aktivitet, og har i den sammenheng de samme behovene som forskere, beskrevet over.  Brukerhistoriene under er beskrevet for følgende aktører:   * **Bruker av analyserom** – Dette kan være forskere, myndighetsaktører, næringslivsaktører eller andre med gyldig tilgang til å bruke et analyserom. Der behovene er spesifikke for en av disse gruppene vil det være spesifisert. * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. * **Myndighetsaktør** – Denne aktøren er en samlebetegnelse for personer involvert i å analysere data, enten på oppdrag for egen virksomhet eller for andre. * **Dataansvarlig for analyserommet** – Denne aktøren er en betegnelse for personen i forskningsprosjektet som har dataansvar for data som ligger i analyserommet. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling og fatte vedtak om tilgang til helsedata samt være en tjenestetilbyder for enkelte tjenester på Helseanalyseplattformen. Helsedataservice antas å være plattformeier for Helseanalyseplattformen. * **Avtaleansvarlig i virksomhet** - Denne aktøren i en privat eller offentlig, norsk eller internasjonal virksomhet er ansvarlig for avtaleforholdet med Helsedataservice. * **Leverandør av analysetjenester til økosystemet** – Denne aktøren tilbyr analysetjenester og -verktøy på gjennom analyseøkosystemet på Helseanalyseplattformen * **Produsent av innsiktstjenester** – Denne aktøren kan levere innsikt og analyser basert på helsedata. Det kan være en offentlig eller privat aktør som benytter analyserommet. Se også EPOS – Konsument av innsiktsjenester. |
| **Brukerhistorier**   1. Som bruker av analyserom må jeg kunne ta med egne data inn i analyserommet, slik at jeg kan analysere disse sammen med andre sensitive personopplysninger 2. Som bruker av analyserom må jeg kunne lagre sensitive personopplysninger i analyserommet på en sikker måte, slik at jeg er sikker på at data jeg er ansvarlig for ikke kommer på avveie 3. Som bruker av analyserom må jeg kunne hente ut resultater fra analyser (som statistikk, grafer, tabeller osv), slik at jeg kan dele resultatene med andre uten at sensitive personopplysninger kommer på avveie 4. Som bruker av analyserom ønsker jeg tilgang til et bredt utvalg med analyseverktøy i analyserommet slik at jeg kan analysere data med de verktøyene som er riktig for meg 5. Som bruker av analyserom ønsker jeg muligheten til å ta med egne verktøy, analysepakker eller containere inn i mitt analyserom slik at jeg har full fleksibilitet hva gjelder funksjonalitet 6. Som bruker av analyserom ønsker jeg enkle grensesnitt for å kunne bestille analyserom slik at det er raskt og lett å komme i gang med analyser 7. Som bruker av analyserom ønsker jeg gode grensesnitt for å kunne endre eksisterende analyserom (for eksempel øke og redusere kapasitet på lagring og prosessering eller legge til nye verktøy) slik at jeg er kan reagere på endringer i behov 8. Som bruker av analyserom ønsker jeg å enkelt kunne avslutte bruken av analyserom slik at kostnader ikke løper utover det jeg trenger 9. Som bruker av analyserom ønsker jeg en totaloversikt over alle medgåtte kostnader knyttet til analyserom som min institusjon kjører til enhver tid slik at man på virksomhetsnivå kan drive effektiv kostnadskontroll 10. Som bruker av analyserom av innsikt ønsker jeg forutsigbare kostnader for bruk av Helseanalyseplattformen, slik at jeg kan estimere hvor store utgifter som vil påløpe 11. Som bruker av analyserom ønsker jeg en totaloversikt over alle medgåtte kostnader knyttet til analyserom som min virksomhet kjører til enhver tid slik at man på virksomhetsnivå kan drive effektiv kostnadskontroll 12. Som forsker ønsker jeg at data fra helseanalyseplattformen kan tilgjengeliggjøres direkte inn i eksterne analyseinfrastruktur slik at jeg har fleksibilitet i valg av infrastruktur og løsninger. 13. Som bruker av analyserom ønsker jeg å kunne aksessere analyserom fra alle lokasjoner, slik at jeg har full fleksibilitet rundt hvor jeg jobber fra. 14. Som bruker av analyserom ønsker jeg å kunne operasjonalisere algoritmene mine slik at de kan gi innsikt på nye, usette data 15. Som bruker av analyserom ønsker jeg kunne sette opp data pipelines mot produksjonssatte algoritmer slik at jeg skaper ny innsikt. 16. Som forsker må jeg kunne arkivere data fra analyserommet på sikker måte slik at resultatene fra forskningen er etterprøvbare på en sikker måte 17. Som forsker ønsker jeg å enkelt kunne innhente ytterligere opplysninger fra innbyggere direkte inn i mitt analyserom slik at jeg sikrer at disse dataene kan lagres på en sikker måte 18. Som produsent av innsiktstjenester ønsker jeg en enkel måte å tilgjengeliggjøre disse til konsumenter på, slik at kunnskapen kommer til de som trenger det i tide 19. Som produsent av innsiktstjenester ønsker jeg en sikker og god måte å tilgangsstyre rapporter på slik at jeg kan sikre at ingen som ikke skal ha tilgang får tilgang 20. Som produsent av innsiktstjenester ønsker jeg en enkel og sikker måte å publisere resultater slik at kunnskap blir tilgjengelig for konsumenter raskt 21. Som produsent av innsiktstjenester ønsker jeg gode visualiseringsverktøy for å bygge gode dashbord og rapporter til mine brukere slik at de kan konsumere kunnskapen på en enkel måte 22. Som produsent av innsiktstjenester ønsker jeg å kunne tilgjengeliggjøre data til fagsystemer slik at mine sluttbrukere kan konsumere kunnskapen på en enkel måte 23. Som produsent av innsiktstjenester ønsker jeg verktøy for å kvalitetssikre, koble og transformere data fra ulike kilder slik at resultatet ut til konsumentene er av høy kvalitet 24. Som produsent av innsiktstjenester ønsker jeg å kunne bygge egne data pipelines mot andre datakilder enn kilder som ligger på Helseanalyseplattformen slik at jeg kan sette sammen det nødvendige datagrunnlaget for min problemstilling 25. Som produsent av innsiktstjenester ønsker jeg å kunne lagre sensitive data i analyserommet på en sikker måte, slik at jeg er sikker på at data jeg er ansvarlig for ikke kommer på avveie 26. Som produsent av innsiktstjenester trenger jeg oversikt over hva som finnes av tilgjengelige data, slik at jeg finne ut av hva jeg kan produsere. 27. Som dataansvarlig for analyserommet ønsker jeg gode mekanismer for å sikre hvilke data som forlater analyserommet, slik at jeg kan sikre at jeg har kontroll på sensitive personopplysninger 28. Som dataansvarlig for analyserommet ønsker jeg selv å kunne håndtere tilgangsstyring av analyserommet slik at jeg til enhver tid har kontroll på hvem som har tilgang til data og at det er enkelt å legge til nye brukere 29. Som dataansvarlig for analyserommet ønsker jeg å enkelt kunne se hvilke databehandlingsaktiviteter som er gjort i analyserommet slik at jeg kan etterprøve at bruken er i samsvar med personvernregelverket, herunder blant annet at bruken er lovlig og ihht. formål. 30. Som dataansvarlig for analyserommet ønsker jeg at alle logger behandles på en slik måte at de ikke kan manipuleres av noen og ivaretar personvernet. 31. Som dataansvarlig for analyserommet ønsker jeg mekanismer som oppdager uvanlig bruk slik at jeg kan gjøre nødvendig tiltak for å hindre at slike ting skjer. 32. Som dataansvarlig for analyserommet ønsker jeg å sikre at data etter endt prosjekt slettes slik at prosjektet oppfyller krav til personvernforordningen. 33. Som Helsedataservice ønsker jeg å automatisk provisjonere opp nye analyserom basert på bestilling, slik at forvaltningskostnadene mine er lave 34. Som Helsedataservice ønsker jeg oppdatert faktureringsgrunnlag av analyserommene slik at jeg kan fakturere sluttbrukere på en riktig måte 35. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data fra dataplattform til analyserommet basert på godkjent bruk på en rask og sikker måte slik at sluttbruker får rask tilgang til data 36. Som Helsedataservice (plattformeier for Helseanalyseplattformen) ønsker jeg å gjøre det mulig for leverandører til analyseøkosystemet å levere tjenester gjennom plattformen slik at brukere får størst grad av fleksibilitet og et bredest mulig tilbud 37. Som Helsedataservice (plattformeier for Helseanalyseplattformen) ønsker jeg å gjøre det enkelt for leverandører til analyseøkosystemet å etablere seg som leverandør på plattformen slik at prosessen er mest mulig smidig 38. Som leverandør av analysetjenester til økosystemet ønsker jeg å tilby mine analysetjenester og -verktøy gjennom plattformen slik at jeg kan bruke analyseøkosystemet som en markedsplass |

### Brukerflater

|  |
| --- |
| **Tittel: Konsument av innsiktstjenester** |
| **EPOS**  Som konsument av innsiktstjenester trenger jeg lett tilgjengelige nøkkelindikatorer og analyser tilpasset mitt behov, slik at jeg enkelt kan bruke helsedata som støtte i mitt arbeid. |
| **Beskrivelse**  Helsepersonell, helseledere og myndighetsaktører har alle behov for innsikt og analyser basert på helsedata. De har delvis overlappende behov, og ofte vil innsiktsløsninger kunne brukes av alle.  Forskjellene ligger blant annet i hva slags data som brukes og hvordan de blir presentert. Eksempelvis vil helsepersonell trenge innsiktstjenester i EPJ i forbindelse med pasientbehandling, mens myndighetsaktører vil ha tilgang til analyser i andre brukerflater.  Myndighetsaktører har behov for tilgang til nøkkelindikatorer og analyser av disse for å kunne følge med på, og følge opp helsetjenesten.  Myndighetsaktører vil kunne være både produsent av innsikt og konsument av innsikt. Myndighetsaktører vil kunne konsumere innsikt produsert av egen virksomhet, andre myndighetsaktører og andre aktører.  Helsepersonell har behov for å bruke helsedata til beslutningstøtte i behandling og for eget kvalitetsarbeid.  Helsepersonell har behov for å kunne sammenlikne egne data fra EPJ.  Helseledere har behov for enkle måter å konsumere data slik at data kan brukes for kvalitetsforbedring, styring og som beslutningsstøtte.   * **Myndighetsaktør** – Denne aktøren er en samlebetegnelse for personer involvert i å analysere data, enten på oppdrag for egen virksomhet eller for andre. * **Helseleder** – Med helseleder menes her alle som er involvert i ledelse i helsetjenesten, både på avdelings- og RHF-nivå. * **Helsepersonell** – Med helsepersonell menes her alle som er involvert i behandling av pasienter i helsetjenesten, både i primær og spesialisthelsetjenesten. |
| Brukerhistorier   1. Som konsument av innsikt ønsker jeg en enkel måte å få tilgang til innsynstjenester slik at jeg effektiv kan bruke disse i mitt arbeid. 2. Som konsument av innsikt ønsker jeg stor fleksibilitet rundt hvilke kanaler data leveres til meg, slik at jeg lett kan få tak i riktige data når jeg trenger det. 3. Som konsument av innsikt ønsker jeg god informasjon om potensielle produsenter av innsikt og hva de kan levere, slik at jeg kan ha et godt beslutningsgrunnlag for å velge produsent. 4. Som konsument av innsikt ønsker jeg å kunne se data fra egen virksomhet i sammenheng med ande datakilder, slik at jeg kan sammenlikne egne resultater med andres, og se om det er områder med mulighet for kvalitetsforbedring. 5. Som konsument av innsikt ønsker jeg å kunne tilpasse rapporter og analysemoduler, slik at det best mulig kan svare til mine behov. 6. Som konsument av innsikt ønsker jeg å vite hva som er tilgjengelig av data og av hvilken kvalitet, slik at jeg effektivt kan bruke det som er tilgjengelig av informasjon. 7. Som konsument av innsikt har jeg behov for å vite at analyser er kvalitetssikret og av høy kvalitet, slik at jeg trygt kan bruke dem som grunnlag for beslutninger. 8. Som konsument av innsikt har jeg behov for analyser med data i nær sanntid, slik at jeg kan overvåke smittsomme sykdommer, pandemier o.a. 9. Som myndighetsaktør har jeg behov for oversiktlige kvalitetsindikatorer, slik at jeg kan følge med på, og følge opp helsetjenesten i mitt ansvarsområde. 10. Som myndighetsaktør eller helseleder ønsker jeg en enkel måte å få tilgang til analyser på slik at jeg effektivt kan bruke data til styring 11. Som helsepersonell har jeg behov for å sammenlikne egne pasienter med andre liknende pasienter og caser for å kunne ta best mulig beslutninger sammen med pasientene mine. 12. Som helsepersonell ønsker jeg at data fra mine pasienter skal automatisk sammenliknes med eksisterende data og se etter sammenhenger, slik at jeg kan få forslag til tiltak og varsler hvis det er faresignaler i forbindelse med behandlingen. 13. Som helsepersonell har jeg behov for tilgang på innsikt i min vanlige brukerflate slik at jeg har det enkelt tilgjengelig. 14. Som helsepersonell ønsker jeg å kunne sammenlikne egen praksis med andres, slik at jeg kan se om det er områder jeg bør forbedre meg på. |

### Åpne data

|  |
| --- |
| **Tittel: Åpne data** |
| **EPOS**  Som forsker ønsker jeg en enkel og god oversikt over åpne, anonyme helsedata slik at jeg raskt kan finne frem til eksisterende kunnskap og data. |
| **Beskrivelse**  I dag finnes det mange åpne statistikkbanker og resultatportaler der aggregerte helsedata presenteres til sluttbrukere. Eksempler på dette er Helseatlas[[3]](#footnote-4) og Kreftregisterets statistikkbank[[4]](#footnote-5).  I fremtiden vil også slike aggregerte data og statistikker kunne bygges gjennom analyserom på Helseanalyseplattformen. Det er nødvendig både å lage en god løsning slik at sluttbrukere får en enkel oversikt over hvilke åpne data som finnes slik at åpen kunnskap blir mer tilgjengelig, og gjøre det enkelt for produsenter av innsikt på Helseanalyseplattformen å kunne publisere åpne data.  Brukerhistoriene under er beskrevet for følgende aktører:   * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. * **Produsent av innsikt** – Denne aktøren er en fellesbetegnelse på aktører i økosystemet som produserer innsikt gjennom analyse på data. I denne sammenheng er også Helsedataservice inkludert som en mulig produsent av innsikt. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling og fatte vedtak om tilgang til helsedata samt er en tjenestetilbyder for enkelte tjenester på Helseanalyseplattformen. |
| **Brukerhistorier**   1. Som forsker ønsker jeg en oversikt over åpne data, grensesnitt og statistikker som ikke er laget på Helseanalyseplattformen, slik at jeg raskt kan finne frem til eksisterende kunnskap og data[[5]](#footnote-6) 2. Som forsker ønsker jeg en oversikt over åpne data, grensesnitt og statistikker som er laget på Helseanalyseplattformen, slik at jeg raskt kan finne frem til eksisterende kunnskap og data. 3. Som produsent av innsikt ønsker jeg kunne publisere og tilgjengeliggjøre åpne data, grensesnitt og statistikker, slik at disse blir tilgjengelig for flest mulig |

### Kohortutforsker

|  |
| --- |
| **Tittel: Kohortutforsker** |
| **EPOS**  Som forsker ønsker jeg på en enkel måte å kunne identifisere den potensielle kohortstørrelsen for en problemstilling, slik at jeg raskt kan avgjøre om problemstillingen har forskningspotensiale. |
| **Beskrivelse**  Forskere har behov for en kohortutforsker som er en åpen løsning de kan sette definerte inklusjon- og eksklusjonskriterier for å identifisere den potensielle størrelsen av en kohort/utvalg for en gitt problemstilling tidlig i et forskningsprosjekt. Forsker vil ikke kunne se identifiserbare helsedata, men vil få returnert et antall/eller et intervall som matcher kriteriene. Denne tjenesten forutsetter direkte tilgang/oppslag mot skarpe data.  Tjenesten bør som et minimum gjøre det mulig å filtrere på demografiske data og diagnose- og prosedyrekoder, og på sikt er det tenkt at tjenesten vil utvides med andre variabler som for eksempel legemiddeldata og data om biologisk materiale.  Det er også tenkt at det skal være mulig å søke om registerdata om kohorten man velger fra løsningen. Her er det tenkt at selve saksbehandlingen vil håndteres gjennom løsning som er under anskaffelse, men at selve tilgjengeliggjøring av data vil gjøres fra dataplattformen.  Brukerhistoriene under er beskrevet for følgende aktører:   * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling og fatte vedtak om tilgang til helsedata samt er en tjenestetilbyder for enkelte tjenester på Helseanalyseplattformen. |
| **Brukerhistorier**   1. Som forsker ønsker jeg å kunne benytte inklusjon- og eksklusjonskriterier på gitte variabler slik at jeg raskt får svar på hvor stort det potensielle befolkningsgrunnlaget til problemstillingen min er. 2. Som forsker ønsker jeg å kunne søke om, og få tilgjengeliggjort data fra min valgte kohort, slik at jeg får rask tilgang på helsedata og kan starte forskningsarbeidet raskt. 3. Som forsker ønsker jeg en tjeneste for å innhente samtykke og ytterligere opplysninger fra personene i min valgte kohort anonymt, slik at jeg kan innhente et rikere datagrunnlag for min forskning. 4. Som Helsedataservice ønsker jeg å forsikre meg om at det ikke er mulig å identifisere enkeltpersoner fra kohortutforskeren slik at jeg kan være compliant med gjeldende regelverk. |

### Anonymisert analyse

|  |
| --- |
| **Tittel: Anonymisert analyse** |
| **EPOS**  Som forsker ønsker jeg å kunne lete eksplorativt etter sammenhenger i store, koblede, anonymiserte datasett, slik at jeg kan få umiddelbar tilgang til disse uten å måtte gå via en søknadsprosess. |
| **Beskrivelse**  Anonymisert analyse er analysetjenester der sluttbrukere fritt kan analysere data fra HAP sin dataplattform uten at personopplysninger eksponeres. Hensikten er at en forsker kan få umiddelbar tilgang til data, uten å gå via en søknadsprosess. Data må være tilrettelagt på en slik måte at de ikke kan spores tilbake til enkelt individer. SSBs microdata.no er et eksempel på en slik tjeneste. |
| **Brukerhistorier**   1. Som forsker ønsker jeg rask tilgang til et anonymisert datasett med mulighet til å utforske ulike spørsmål og problemstillinger slik at jeg kan lage nye hypoteser eller adressere nye problemstillinger som ikke er jobbet med tidligere, uten å gå via en tidkrevende søknadsprosess. 2. Som forsker ønsker jeg tilgang til en oversikt over hvilke variabler med tilhørende metadata som er tilgjengelig for anonymisert analyse, slik at det er enkelt for meg å plukke ut de dataene jeg har behov for. 3. Som forsker ønsker jeg mulighet til å hente ut resultater fra analysen i form av statistikk, tabeller, grafikk o.l., slik at det er enkelt for meg å presentere anonyme data fra HAP i mitt videre arbeide. 4. Som dataansvarlig for anonymisert analysetjeneste ønsker jeg at resultatet fra alle analysene er fult ut anonyme, slik at det ikke er mulig å spore data tilbake til enkeltindivider. 5. Som forsker ønsker jeg å kunne aksessere anonymiserte analyse fra alle lokasjoner, slik at jeg har full fleksibilitet rundt hvor jeg jobber fra. 6. Som dataansvarlig for anonymiserte analyse tjenesten ønsker jeg å enkelt kunne se hvilke databehandlingsaktiviteter som er gjort i analyserommet slik at jeg kan etterprøve at bruken er korrekt og ihht formål. 7. Som dataansvarlig for anonymisert analyse tjenesten ønsker jeg mekanismer som oppdater uvanlig bruk slik at jeg kan gjøre nødvendig tiltak for å hindre at slike ting skjer. 8. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data fra dataplattform til anonymisert analyse tjenesten basert på godkjent bruk på en rask og sikker måte slik at sluttbruker får rask tilgang til data |

### Syntetiske data

|  |
| --- |
| **Tittel: Syntetiske data** |
| **EPOS**  Som plattformeier av helseanalyse plattformen ønsker jeg mulighet for å kunne etablere representative syntetiske data basert på skarpe data, hvor personopplysninger ikke på noen som helst måte er mulig å gjenskape, slik at aktører kan bruke disse i forbindelse med utvikling av eksempelvis integrasjoner, rapporter og analyser. |
| **Beskrivelse**  Syntetisk data er genererte data med tilsvarende statistiske/matematiske egenskaper, struktur og relasjoner som skarpe data. For Helseanalyseplattformen er det et mål å kunne tilby syntetiske data hvor personopplysningene fra det originale datasettet er fullt ut anonymisert og ikke på noen måte er mulig å gjenskape. Syntetiske data kan dermed brukes til å skjerme skarpe data mot uønsket bruk. På Helseanalyseplattformen kan syntetiske data ha følgende bruksområde:   * Mulighet for registerforvalter til å generere representative testdata til det enkelte register * Kunne generere realistiske testdata til utvikling av tjenester på helseanalyseplattformen * Tilgang til representativ data for metode- og verktøysutvikling for forskere * Tilgjengeliggjøring av representativ data for innovasjon i næringsliv og akademia   Behovet for gode testdata vil alltid være til stede både før, under og etter utvikling av en helseanalyseplattform. Syntetiske data vil være viktig for automatisk å kunne generere gode testdata for flere bruksformål, fra systemtesting i Helseanalyseplattformen til hypotesegenerering og oppsett av dataanalyser for alle systemer som håndterer helsedata.  For å ivareta gode personvernprinsipper er en svært viktig egenskap til syntetiske data i kontekst av helseanalyseplattformen, at det ikke må være mulig å spore de tilbake til reelle individer med tilhørende data. Denne egenskapen er viktigere enn at syntetiske data har like statistiske egenskaper som skarpe data. |
| **Brukerhistorier**   1. Som registerforvalter ønsker jeg å kunne etablere ett syntetisk datasett på mine data slik at andre aktører kan bruke disse til å teste mot våre tjenester, som for eksempel datautlevering, innbyggertjenester og integrasjon mot helseanalyseplattformen, samtidig som gode personvernprinsipper ivaretas. 2. Som utvikler av analysetjenester på helseanalyseplattformen ønsker jeg tilgang på ett syntetisk datasett fra helseanalyseplattformen for alle tilgjengelige data, slik at jeg kan benytte disse til å utvikle og teste analysetjenester og maskinlæringsalgoritmer, samtidig som gode personvernprinsipper ivaretas. 3. Som forsker ønsker å jeg å kunne få tilgang til ett mest mulig representativt syntetisk datasett med variabler fra helseanalyseplattformen, basert på utvalgskriterier, som er relevante for meg og mitt prosjekt, slik at jeg kan benytte data til å utvikle hypoteser, metoder og verktøy til forskningen min, uten å måtte vente på å få utlevert reelle data. 4. Som forsker ønsker jeg åpen tilgang til representative, syntetiske datasett for de ulike datakildene på Helseanalyseplattformen slik at jeg kan utforske variabler og datasett, lære meg om dataen, utvikle hypoteser og se muligheter ved bruk av dataen 5. Som forvalter av helseanalyseplattformen ønsker jeg å kunne etablere ett syntetisk datasett på alle sammenstilte data fra ulike kilder, slik at andre aktører kan bruke disse til å teste mot våre tjenester, som for eksempel datautlevering, kohort utforsker, statistikk, analysetjenester, innbyggertjenester, samtidig som gode personvernprinsipper ivaretas. 6. Som kommersiell tilbyder av tjenester ønsker jeg rask tilgang på syntetiske test data fra HAP på variabler som er relevante for meg, slik at jeg kan utvikle og teste tjenester på mest mulig representativ, samtidig som gode personvernprinsipper ivaretas. |

### Tilgjengeliggjøring av data

|  |
| --- |
| **Tittel: Tilgjengeliggjøring av data** |
| **EPOS**  Som Helsedataservice ønsker jeg gode mekanismer for å tilgjengeliggjøre helsedata på en sikker og effektiv måte, slik at både personvernet og at sluttbrukernes legitime behov om rask tilgang til helsedata ivaretas. |
| **Beskrivelse**  Helsedataservice skal tilgjengeliggjøre data fra Helseanalyseplattformen som en sluttbruker har fått innvilget tilgang til via søknad, samt kunne trekke tilbake tilgang til data når godkjenning av tilgang ikke er gyldig lenger. I tillegg vil det være aktuelt å tilgjengeliggjør datasett som er anonyme, dvs. data på ett aggregert nivå og hvor det ikke er mulig å identifisere enkeltpersoner.  Helsedataservice bør ha mulighet for å tilgjengeliggjøre data på ulike måter og til ulike plattformer:   * Utlevering til sluttbrukers eget analyserom på Helseanalyseplattformen * Utlevering til andre nasjonale og internasjonale sikre analyseinfrastrukturer, slik som Tjenester for Sensitive Data (TSD) fra Universitetet i Oslo, eller NTNU sin HUNT Cloud tjeneste. Det bør legges opp til en mest mulig automatisert utleveringsprosess for analyseinfrastrukturer som er mye brukt * Direkte utleveringer til sluttbrukers egen infrastruktur, for eksempel vha filoverføringer * Mulighet for at sluttbruker kan gjøre API oppslag mot åpne data, eller data denne har fått godkjent tilgang til   For all utlevering gjelder det at sluttbruker må ha en hjemmel for tilgang til data. Det er viktig at det etableres gode mekanismer for samhandling med Helseanalyseplattformen og prosesser for søknad om tilgang på data, slik at man sikrer at det kun gis tilgang til de data som søknaden har gitt hjemmel for, samt at det er rask og effektiv å utlevere data når søknaden er godkjent av Helsedataservice.  Brukerhistorier under merket med \* er også beskrevet under andre EPOS, men er tatt med her for å synliggjøre helheten knyttet til tilgjengeliggjøring av data.  Alle disse brukerhistoriene er tett knyttet til anskaffelsen om søknads- og saksbehandlingstjenester. En løsning vil derfor måtte forholde seg til løsninger som etableres gjennom "anskaffelse søknad- og saksbehandlingstjenester"  Brukerhistoriene under er beskrevet for følgende aktører:   * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling og fatte vedtak om tilgang til helsedata samt er en tjenestetilbyder for enkelte tjenester på Helseanalyseplattformen. * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. * **Innbygger** - Denne aktøren er innbygger i Norge. Data på Helseanalyseplattformen vil være hentet fra innbygger, eller person innbygger handler på vegne av, for eksempel egne barn. |
| **Brukerhistorier**   1. \*Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data fra dataplattform til ulike analyserom basert på godkjent bruk på en rask og sikker måte slik at sluttbruker får rask tilgang til data 2. Som Helsedataservice ønsker jeg å kunne trekke tilbake tilgang til data som er tilgjengeliggjort til ulike analyserom, slik at jeg kan sikre at sluttbrukere som ikke lenger har gyldig tilgang ikke får tilgang til data 3. \*Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data fra dataplattform til ulike analyserom på fast basis basert på godkjent bruk på en rask og sikker måte slik at konsumenter får rask tilgang til oppdaterte data 4. \*Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre åpne data på helsedata.no, slik at disse blir tilgjengelig for flest mulig. 5. Som Helsedataservice ønsker jeg å kunne forvalte og utlevere data fra standardiserte og ferdigkoblede datasett, slik at jeg kan tilgjengeliggjør disse til sluttbruker på en rask og sikker måte 6. Som Forsker ønsker jeg å kunne søke om tilgang på og få utlevert ett brukerdefinert datasett, slik at jeg selv kan spesifisere i min søknad hvilke data fra de ulike dataleverandørene som er relevante for meg i min forskning 7. Som Forsker ønsker jeg rask tilgang til data etter at søknaden min om tilgang på data er godkjent, slik at jeg kan komme i gang med forskningsarbeidet mitt 8. Som Forsker ønsker mulighet for å koble data fra ulike dataleverandører, slik at jeg kan forske på problemstillinger på tvers av ulike medisinske registre 9. Som forsker ønsker jeg mulighet til å motta løpende oppdaterte data fra underliggende dataleverandører på data som jeg allerede har fått tilgang til, slik at data jeg benytter i min forskning er mest mulig oppdatert 10. Som Helsedataservice ønsker jeg mulighet for at data som utleveres pseudonymiseres, slik at gode prinsipper for personvern ivaretas 11. Som Helsedataservice ønsker jeg å tilby en tjeneste for nøkkelforvaltning av unike koblingsnøkler for prosjekter slik at det skal bli enklere å koble data fra flere dataleverandører på en måte som fremmer personvernet. 12. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre og tilgangsstyre data som oppslagstjenester gjennom definerte APIer, slik at sluttbrukere med hjemmelsgrunnlag selv kan gjøre oppslag mot registerdata. 13. Som Forsker ønsker jeg å få data tilgjengeliggjort direkte til eksterne nasjonale og internasjonale analyseinfrastrukturer, slik at jeg benytte disse til min forskning og kan få overlevert data på en rask og sikker måte 14. Som innbygger ønsker jeg en enkel oversikt over hvilke opplysninger om meg som er tilgjengeliggjort, til hvem og til hvilket formål slik at jeg får oversikt over hva mine opplysninger brukes til. 15. Som innbygger vil jeg ha mulighet til å reservere meg mot at mine data utleveres til gitte formål, slik at jeg har eierskap og kontroll på mine data 16. Som Helsedataservice ønsker jeg fullstendig oversikt over alle tilgjengeliggjøringer av data som er gjort, slik at jeg kan sikre compliance med gjeldende regelverk. 17. Som Forsker ønsker jeg mulighet for å få data ulevert direkte til meg, slik at jeg kan benytte min egen infrastruktur til å analysere data 18. Som registerforvalter ønsker jeg å motta løpende oppdaterte grunndata fra Helseanalyseplattformen, slik at jeg har en kilde til visse typer grunndata som jeg kan knytte mine data mot |

## Helseregister på Helseanalyseplattformen

### Helseregister som en tjeneste

|  |
| --- |
| **Tittel: Helseregister som en tjeneste** |
| **EPOS**  Som registerforvalter ønsker jeg en enkel og rimelig registerløsning slik at jeg slipper å tilrettelegge for dette selv. |
| **Beskrivelse**  Sluttrapporten om referansearkitektur for helseregistre[[6]](#footnote-7) fra 2016 beskrev anbefalt referansearkitektur for helseregistre. Det bør være mulig for en registerforvalter å opprette og drifte et helseregister på infrastrukturen til Helseanalyseplattformen, med dette ligger bruk av fellestjenester som beskrevet i referansearkitekturrapporten, teknisk drift og forvaltning av register (inkl fagapplikasjoner) og integrasjon mot datakilder/innrapportering. Som en del av dette vil "best practice" for etablering av registre være sentralt. |
| **Brukerhistorier**  *<Detaljerte brukerhistorier for dette EPOS vil skrives senere>* |

### Registerforvalters forkammer

|  |
| --- |
| **Tittel: Registerforvalters forkammer** |
| **EPOS**  Som registerforvalter ønsker jeg tilgang til en infrastruktur slik at jeg kan drive datakvalitetsforbedringsarbeid av mitt register på en god måte. |
| **Beskrivelse**  For helseregistre som ligger utenfor Helseanalyseplattformen bør Helseanalyseplattformen tilby en infrastruktur som gjør at registerforvalter av registeret kan drive datakvalitetsarbeid for sitt register på Helseanalyseplattformen. På mange måter kan dette sees på som en variant av et analyserom. Den største forskjellen er at data fra registerforvalters forkammer vil leveres til den sentrale dataplattformen. |
| **Brukerhistorier**  *<Detaljerte brukerhistorier for dette EPOS vil skrives senere, men mange av de samme brukerhistoriene for analyserom vil også være relevante her>* |

## Innbyggertjenester

### Innsyn og tilbakemelding

|  |
| --- |
| **Tittel: Innsyn og tilbakemelding** |
| **EPOS**  Som innbygger ønsker jeg innsyn i hvilke data som finnes om meg på helseanalyseplattformen, og hva de er brukt til, slik at jeg har kontroll på egne helseopplysninger |
| **Beskrivelse**  Innbyggere har ønske om, og krav på innsyn i data om seg selv. Dette gjelder både hva som er registrert, hvor det er registrert og hva det brukes til. Innbyggere skal også kunne få oversikt over hvilke samtykker de har gitt i forskjellige sammenhenger. Innsyn i egne helseopplysninger vil også kunne øke kvaliteten ved at feilregistreringer oppdages. Det skal være mulig å gi tilbakemelding om retting og sletting og å trekke samtykker som er gitt.  Innbygger skal ha innsyn og mulighet for tilbakemeldinger på helsenorge.no   * **Innbygger** - Denne aktøren er innbygger i Norge. Data på Helseanalyseplattformen vil være hentet fra innbygger, eller person innbygger handler på vegne av, for eksempel egne barn. * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. |
| **Brukerhistorier**   1. Som innbygger ønsker jeg innsyn i hvilke data som finnes om meg på helseanalyseplattformen, og hva de er brukt til, slik at jeg har kontroll på egne helseopplysninger 2. Som innbygger ønsker jeg innsyn i hvilke samtykker jeg har gjort til forskjellige registre og forskningsprosjekter, slik at jeg har kontroll på hva mine helsedata kan bli brukt til. 3. Som innbygger ønsker jeg å kunne gi tilbakemelding om feilregistreringer, slik at jeg kan få rettet opp feil i data om meg selv. 4. Som innbygger ønsker jeg å kunne få slettet data som er feil eller jeg ikke ønsker at skal være registrert, der jeg har krav på det, slik at jeg har bedre kontroll på egne helseopplysninger. 5. Som forsker som har med egne data inn på helseanalyseplattformen trenger jeg mekanismer for å gi innbygger innsyn, slik at jeg kan overholde mine forpliktelser ovenfor innbygger |

### Dialog mellom forsker og innbygger

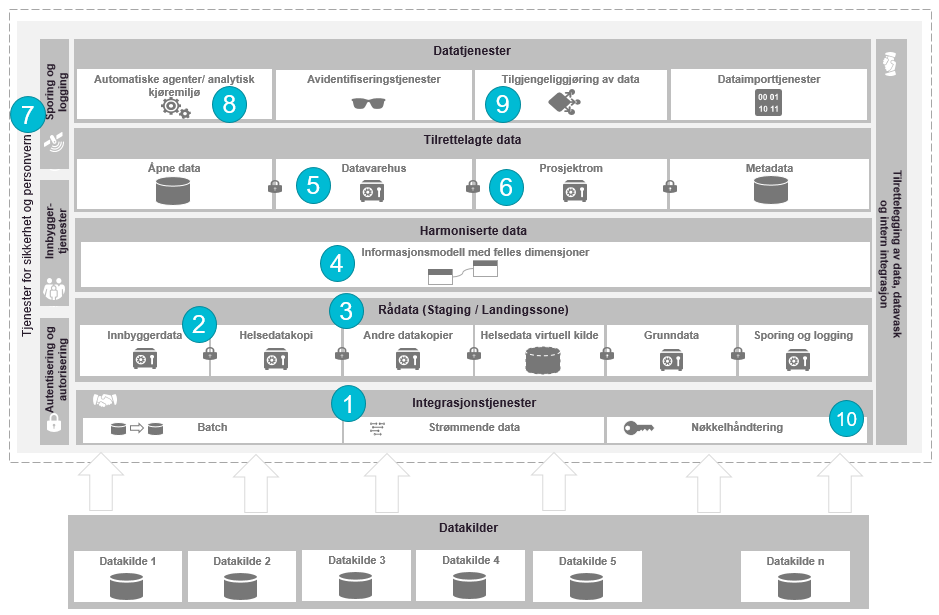
|  |
| --- |
| **Tittel: Dialog mellom forsker og innbygger** |
| **EPOS**  Som forsker ønsker jeg å kunne ha dialog med innbyggere for å få samtykke til bruk av opplysninger og innhente nye data. |
| **Beskrivelse**  Forskere har behov for å ha dialog med innbyggere i flere sammenhenger. Det vil være med forskjellig grad av anonymitet avhengig av hva det dreier seg om. Eksempelvis bør samtykkeforespørsler kunne sendes ut til et utvalg innbyggere uten at de er identifisert for forskeren. I tilfeller der innbygger allerede er identifisert, for eksempel som deltager i en klinisk studie vil det kunne være aktuelt med direkte identifisert dialog.  Det er også behov for å kunne håndtere samtykker som både gis og trekkes.   * **Innbygger** - Denne aktøren er innbygger i Norge. Data på Helseanalyseplattformen vil være hentet fra innbygger, eller person innbygger handler på vegne av, for eksempel egne barn. * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. |
| **Brukerhistorier**   1. Som forsker ønsker jeg å kunne sende samtykkeforespørsler til et utvalg innbyggere for å kunne gjenbruke helsedata som allerede er samlet inn. 2. Som forsker ønsker jeg å kunne sende forespørsler til et utvalg av innbyggere om deltagelse i forskningsprosjekter (kliniske studier, helseundersøkelser o.a.), slik at jeg kan rekruttere deltagere. 3. Som forsker ønsker jeg å kunne sende ut undersøkelser til et utvalg av innbyggere og få responsene på helseanalyseplattformen, slik at jeg har en enkel og sikker måte å få inn data på. 4. Som forsker ønsker jeg å ha dialog med forskningsdeltagere slik at jeg kan innhente kompletterende opplysninger og informere om resultater. 5. Som forsker ønsker jeg gode verktøy til å håndtere samtykker, slik at jeg har oversikt over hvem som er med i studien min og til enhver tid har data fra de deltagerne som har samtykket. |

# Utforming av Helseanalyseplattformen

## Dataplattform

For at Helsedataservice skal kunne levere ett godt tilbud av data- og analysetjenester slik at data enkelt og trygt kan tilgjengeliggjøre for godkjente formål, vil det å etablere en dataplattform med innebygget personvern stå sentralt. Denne vil danne fundamentet for å kunne realisere sluttbrukertjenester på Helseanalyseplattformen da sikker håndtering av helsedata er en kritisk suksessfaktor. Dataplattformen kan sees på som forvaltningssonen der Helsedataservice er dataansvarlig og som benyttes for å tilgjengeliggjøre data på en sikker måte til godkjente formål.

En viktig del av dataplattformen er grensesnitt mot registre og andre datakilder slik at kopier av registerdata kan tilgjengeliggjøres gjennom Helseanalyseplattformen. En slik dataplattform danner også grunnlaget for at nye datakilder enkelt skal kunne integreres inn og for at nye tjenester som benytter helsedata skal kunne etableres på toppen. Under er en illustrasjon på hvordan en slik dataplattform kan utformes:



Figur 6: Illustrasjon fra konseptvalgutredningen til Helseanalyseplattformen som illustrerer egenskaper ved dataplattformen.

Dataplattformen må inneholde integrasjonstjenester, både i form av batchintegrasjoner, men også i form av strømmende data (nær-sanntidsintegrasjoner) (1). Det legges opp til at innbyggere selv på sikt skal kunne laste opp, forvalte og tilgjengeliggjøre egne data på plattformen (2) i en sonebasert lagringsmodell med vanntette skott mellom datakildene (3). Det er støtte for ulike metoder for hvordan man lagrer data på plattformen, og ulike aktører skal kunne forvalte sine egne data på plattformen. Data fra ulike helseregistre er koblet på fast basis gjennom en informasjonsmodell med felles dimensjoner (4). Konseptet inneholder tilrettelagte datavarehus (5) som mottar data på fast basis og midlertidige analyserom (6) der brukere får tilrettelagte data og kan ta med egne data gjennom datatjenestelaget. Tjenester for sikkerhet og personvern omslutter hele dataplattformen (7). Konseptet inkluderer et kjøremiljø der automatiske agenter analyserer data ettersom nye data kommer inn (8). I tillegg må plattformen støtte tilgjengeliggjøring av data inn i andre sertifiserte analyseplattformer, samt tilgjengeliggjøring av åpne og aggregerte data som APIer (9). Dataplattformen må ha et regime for forvaltning av krypteringsnøkler (10), slik at person­opplysninger som er kryptert på ulike måter av de ulike datakildene, kan kobles på en sikker måte. I tillegg må ulike aktører kunne forvalte sine nøkler på en god måte.

Dataplattformen bør også ha mulighet til å tilby helseregistre som en tjeneste. I kombinasjon med flere tekniske fellestjenester som utvikles utenfor Helseanalyseplattformen kan dette muliggjøre billigere og sikrere etablering av nye registre med enkle datastrukturer og forvaltningsbehov.

## Integrasjon av datakilder inn på dataplattformen

*<Det utarbeides et eget dokument som beskriver as-is arkitekturen der kildesystemene beskrives i mer detalj. Dette er ikke med i dette dokumentet. Vi tar gjerne mot innspill på hva leverandøren mener det er viktig blir dokumentert som en del av dette arbeidet. Dette dokumentet vil støttes av en tabell som illustrert under>*

Tabell 1: Beskrivelse av datakilder som Helseanalyseplattformen skal integreres mot.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Datakilde | Eier | Type innhold | Juridisk grunnlag | Frekvens | Volum | Størrelse | Historikk | Endringstakt | Datakvalitet | Integrasjonsmuligheter | Utvekslingsformat | Kjøremiljø | Kryptering | Prioritet |
| Dødsårsaksregistret | FHI | Informasjon om dødsårsak. | Helseregisterloven §11 | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> | <kommer> |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

HL7 FHIR anses som en viktig standard for datadeling i helse- og omsorgsektoren. HL7 FHIR (Fast Healthcare Interoperability Resources) er en fritt tilgjengelig standard fra HL7 International. FHIR ble utarbeidet for å møte krav til mer effektiv og fleksibel utveksling av helsedata, og er også en anbefalt standard fra Direktoratet for e-helse. For tjenester basert på datadeling vil bruk av FHIR standarden stå sentralt, for overføring av hele datasett vil det måtte vurderes om bruk av informasjonsmodellen i FHIR kan være aktuelt. For mer informasjon se anbefaling om bruk av HL7 FHIR for datadeling[[7]](#footnote-8).

## Integrasjon mot andre løsninger og grensesnitt

*<Her vil en beskrivelse av andre løsninger og grensesnitt som Helseanalyseplattformen vil forholde seg mot komme. Listen under er ikke komplett og vil utvides. Leverandøren må gjerne kommentere hvorvidt det er ytterligere informasjon som kreves>*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Løsning | Eier | Beskrivelse | Grensesnitt/protokoll | Forretningsmessig kontekst | Forventet tid for integrasjon |
| HelseID | Norsk Helsenett | <kommer> | OpenID-Connect/SAML | <kommer> | <kommer> |
| Nextcloud Files | Norsk Helsenett | <kommer> | Ikke besluttet (WebDAV API et alternativ) | Nextcloud Files skal etter planen benyttes som elektronisk datautleveringsmekanisme mellom registerforvaltere, fra registerforvalter til forsker, samt deling av filer fra forsker til registerforvalter. Tjenesten vil bli tilgjengeliggjort gjennom helsedata.no. | <kommer> |
| HealthTerm | Direktoratet for e-helse | <kommer> | REST API | HealthTerm skal etter planen inneholde metadata om variabler i registrene. Dette vil være kilde for variabelutforskeren på helsedata.no og er planlagt implementert ila våren 2019. | <kommer> |
| Saksbehandlings-løsning for helsedata | Direktoratet for e-helse | <kommer> | <kommer> | <kommer> | <kommer> |
| Helsedata.no | Direktoratet for e-helse | <kommer> | <kommer> | <kommer> | <kommer> |
| Helsenorge.no | Direktoratet for e-helse | <kommer> | <kommer> | <kommer> | <kommer> |

Tabell 2: Beskrivelse over eksterne løsninger og grensesnitt som Helseanalyseplattformen etter planen vil integreres mot



Figur 7: Application communication diagram (v0.3) på nivå 1 for Helseanalyseplattformen

## Antatt nødvendige tekniske kapabiliteter

For å kunne realisere dataplattformen med tilhørende analysetjenester er det etablert ett forslag til tekniske kapabiliteter som Helsedataprogrammet tror er nødvendige for å realisere Helseanalyseplattformen. Under er en illustrasjon på disse:



Figur 8: Illustrasjon over forslag til tekniske kapabiliteter for Helseanalyseplattformens dataplattform og analyseinfrastruktur

Hvis Leverandøren mener det er ytterligere eller alternative tekniske kapabiliteter som kreves for å løse de funksjonelle kravene til løsningen oppfordrer vi på det sterkeste til at dette beskrives som en del av løsningsforslaget.

Vi har valgt å gruppere de tekniske kapabilitetene inn i følgende grupper:

* Dataforvaltning
* Sikkerhet
* Analyseverktøy
* Integrasjon
* Infrastruktur
* Administrasjonsverktøy
* Utviklerverktøy

Disse er videre beskrevet i kapitlene under.

### Dataforvaltning

Med tekniske kapabiliteter knyttet til dataforvaltning menes de egenskapene plattformen bør ha knyttet til å lagre og forvalte data på en god måte.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |

|  |  |  |
| --- | --- | --- |
|  | Lagring av strukturerte data | Den tekniske plattformen må inneholde kapabiliteter for lagring av strukturerte data i form av relasjonsdatabaser. |
|  | Lagring av ustrukturerte data | Den tekniske plattformen må inneholde kapabiliteter for lagring av ustrukturerte data. |
|  | Informasjonsmodelleringsverktøy | Den tekniske plattformen bør inneholde informasjonsmodelleringsverktøy som kan benyttes for å etablere og forvalte informasjonsmodeller som Helsedataservice er ansvarlig for. Det bør være mulig å knytte register variabler mot en eller flere informasjonsmodeller. |
|  | Datavirtualisering | Den tekniske plattformen bør inneholde kapabiliteter for datavirtualisering/federering som gjør det mulig for Helsedataservice å koble registre og andre kilder på et logisk nivå uten nødvendigvis sitte på lokale kopier av data. |
|  | Data lineage | Den tekniske plattformen må inneholde kapabiliteter som gjør det mulig å spore data tilbake til opprinnelse og hvordan data har blitt flyttet og behandlet over tid fram til endepunkt. |
|  | Metadataforvaltningsverktøy | Den tekniske plattformen bør inneholde verktøy for forvaltning av metadata. Denne bør kunne samspille med HealthTerm- verktøyet, som sektoren har valgt som standard løsning for å dokumentere og beskrive kodeverk, terminologi og metadata knyttet til helseregister variabler.  Det må også legge til rette for at operasjonelle data på HAP kan kobles med metadata. |
|  | Arkivere data | Den tekniske plattformen må ha mulighet til å arkivere og gjenfinne data som ikke lenger er i aktiv bruk. Data må lagres på en slik måte at det er enkelt å gjenfinne data ved behov. |
|  | Versjonere data | Den tekniske plattformen må ha mulighet for å kunne håndtere ulike versjoner av datasett. Ulike sluttbrukere kan ha fått utlevert ulike versjoner av datasett fra dataleverandør, løsningen må kunne håndtere dette. |

### Sikkerhet

Med tekniske kapabiliteter knyttet til sikkerhet menes de egenskapene plattformen bør ha for å kunne forvalte data på en trygg måte slik at man ivaretar gode personvernprinsipper.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Sporing og logging | Den tekniske løsningen må tilby detaljerte sporingsmuligheter og logging for all bruk av plattformen. |
|  | Autentisering og autorisasjon | Den tekniske plattformen må ha mulighet for å skille mellom ulike brukergrupper, bør støtte integrasjon med Helse-ID, og bør kunne integrere med andre, eksterne autentiseringsmekanismer basert på standarder som eksempelvis SAML og OAuth2.  Tilgangsrettigheter må kunne modelleres slik at tilgang kun gis for de som skal ha tilgang, uavhengig av autentiseringsmetode. |
|  | Sertifikat- og nøkkelhåndtering | Den tekniske løsningen må tilrettelegge for sikker administrasjon/håndtering av sertifikater og krypteringsnøkler. |
|  | Kryptering av data | Det må være mulig å kryptere data i alle stadier: Data som transporteres, data som lagres på disk, samt data som prosesseres. Krypteringsalgoritmer som legges til grunn må kunne byttes ut. |
|  | Segmentering og soneinndeling | Den tekniske plattformen bør støtte muligheter til å dele systemer og ressurser inn i segmenter/soner, basert på kriterier som klassifisering, brukergrupper og trafikk mellom segmentene må kunne sperres/filtreres og logges. |

### Analyseverktøy

Med tekniske kapabiliteter knyttet til analyseverktøy menes de verktøy og egenskaper plattformen bør ha for at sluttbruker effektivt skal kunne analysere data for å produsere innsikt og kunnskap.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Åpne analyseverktøy | Den tekniske plattformen må ha mulighet for sluttbruker å kunne bruke åpne analyseverktøy til å analysere og visualisere data tilgjengeliggjort i analyserom. Eksempel på slike verktøy er Python, R og Jupyter. Det må også være mulig å benytte analysepakker fra eksempelvis CRAN og Python Package Index. |
|  | Eksterne analyseverktøy | Den tekniske plattformen bør legge til rette for bruk av tredjeparts eksterne analyseverktøy ihht et økosystem tankegang der tredjeparts aktører kan tilby sine analyseverktøy eller –tjenester gjennom plattformen. |
|  | Verktøy for å bygge og operasjonalisere rapporter og statistikk | Den tekniske plattformen må gi mulighet for sluttbruker å bygge og operasjonalisere rapporter og statistikk produsert i analyserom på en hensiktsmessig måte. Med å operasjonalisere mener vi å tilgjengeliggjøre analyser og visualiseringer utenfor analyserommet, enten åpent for alle, eller via tilgangsstyrte brukerflater. |
|  | Ta med egne analyseverktøy i analyserom | Den tekniske plattformen bør gi mulighet for sluttbruker å kunne ta med egne prefererte verktøy til analyserommet, for å benytte disse til å analysere data. |
|  | Verktøy for å bygge og operasjonalisere maskinlæringsmodeller og algoritmer | Den tekniske plattformen må ha kapabiliteter og verktøy for å bygge maskinlæringsmodeller og algoritmer, samt operasjonalisere disse. Med operasjonalisering mener vi at algoritmen blir produksjonssatt og det er mulig å score nye data mot algoritmen. |
|  | Data wrangling verktøy | Den tekniske plattformen bør ha mulighet for at sluttbruker i analyserom kan utforske og preparere datasett for analyse ved hjelp av data wrangling verktøy. |

### Integrasjon

Med tekniske kapabiliteter knyttet til integrasjon menes de egenskapene plattformen bør ha for å bringe data inn på dataplattformen, samt å tilgjengeliggjør data til analyse eller andre eksterne aktører på en trygg og sikker måte.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Verktøy for å bygge og forvalte data pipelines | Den tekniske plattformen må ha mulighet for å kunne bygge avanserte data pipelines for å motta og flytte data fra kilde til destinasjon. Både batchbaserte og nær-sanntidsflytting (streaming) av data må støttes. Det må være mulig å kvalitetssikre, transformere og berike data underveis i prosessen. Datamapping og konvertering mellom ulike datastrukturer og formater må støttes. Plattformen må ha gode muligheter for å validere og overvåke data pipelines. |
|  | Verktøy for datakvalitetesregler | Den tekniske plattformen bør inneholde verktøy for å etablere og utføre datakvalitetsregler. Disse bør kunne eksekveres som en del av mottaksprosessen av data fra datapipelines, periodisk, eller ved behov. |
|  | Verktøy for å tilgjengeliggjøre data til analyserom | Den tekniske plattformen må inneholde en kapabilitet som gjør det mulig for Helsedataservice å tilgjengeliggjøre data inn i analyserom. Her har vi sett for oss at dette gjøres ved at data fysisk flyttes fra dataplattform til lagringsmedium i analyserom som kun er tilgjengelig for den som har fått innvilget tilgang til data. |
|  | API Management | Den tekniske plattformen bør tilby verktøystøtte for API Management for å tilgjengeliggjøre grensesnitt på en kontrollert og effektiv måte.  API management bør kunne integrere med autentiseringsløsninger basert på vanlige protokoller, som SAML, OAUTH2, samt Helse-ID.  API management løsning bør støtte kryptering av trafikk, på transport og meldingsnivå.  API management bør støtte kunne detektere og hindre applikasjons angrep som OWASP Top 10, samt forsøk på tjenestenektangrep o.l. |
|  | Import av data inn i analyserom | Den tekniske plattformen må ha mulighet for sluttbruker å kunne importere egne data inn i analyserom, og kunne koble disse med data tilgjengeliggjort fra dataplattform. |

### Administrasjonsverktøy

Med tekniske kapabiliteter knyttet til administrasjonsverktøy menes de egenskapene plattformen bør ha knyttet til å administrere og forvalte data- og analysetjenester som sluttbrukere benytter.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Provisjonere analyserom | Den tekniske plattformen må ha mulighet til å effektivt kunne sette opp nye analyserom med tilhørende data for brukere som har blitt innvilget tilgang. |
|  | Bestilling, transaksjonshåndtering og økonomistyring | Den tekniske plattformen bør ha mulighet til å håndtere bestillinger og beregne fakturagrunnlag, samt kunne samhandle med egen løsning for fakturering og bokføring. |
|  | Beregne pris på analyserom | Den tekniske plattformen bør ha mulighet til å kunne beregne pris for de tjenestene som en sluttbruker ønsker å benytte. |
|  | Tjenestekatalog | Den tekniske plattformen bør ha mulighet for å kunne vedlikeholde en tjenestekatalog med de tjenestene som Helsedataservice og aktører i økosystemet tilbyr sine sluttbrukere. |
|  | Kundekatalog | Den tekniske plattformen bør ha mulighet for å kunne vedlikeholde en kundekatalog med de aktørene som benytter HAP sine tjenester. |
|  | Leverandør/ partnerkatalog | Den tekniske plattformen bør ha mulighet for å kunne vedlikeholde en leverandør katalog med de aktørene i økosystemet som tilbyr tjenester på HAP. |
|  | Endre kapasitet - lagring og prosessering | Den tekniske plattformen må gjøre det enkelt for sluttbruker å endre kapasitet i form av lagring og prosessering i sitt analyserom. Dersom dette er en tjeneste sluttbruker betaler for, må faktureringsgrunnlaget også reflektere dette. |
|  | Samtykke og reservasjons-  håndtering | Den tekniske plattformen må gi innbygger mulighet via helsenorge.no til å kunne samtykke og reservere seg mot bruk av egne helsedata på HAP. Det må også være mulig for innbygger å be om å bli slettet. |
|  | Lisenshåndtering | Den tekniske plattformen må ha mulighet til å kunne skaffe en oversikt over, samt kunne administrere software lisenser som er i bruk på plattformen. |
|  | Koblingsnøkkelkatalog | Den tekniske plattformen må ha funksjonalitet for å koble sammen data fra 2 eller flere anonymiserte/pseudonymiserte tabeller på en sikker måte, og må støtte bruk av rolledeling (separation-of-duties) for godkjenning av hver enkelt kobling. |
|  | Avslutte bruk av analyserom | Den tekniske plattformen må gjøre det enkelt for sluttbruker å avslutte og stenge ned ett analyserom som ikke lenger skal benyttes. Det må være mulighet for at innholdet i analyserommet kan arkiveres (for eksempel for forskningens etterprøvbarhet). |
|  | Digital rettighetsadministrasjon | Den tekniske plattformen bør ha støtte for digital rettighetsadministrasjon (DRM) slik at man kan begrense bruksmulighetene til data som er utlevert til sluttbruker. Ved hjelp av DRM systemet bør man kunne knytte datautleveringer til en lisens som regulerer bruk av data.  Man bør også kunne sette ett digital vannmerke på datasett eller lignende mekanismer for å sikre integriteten på datasett. |
|  | Asset management | Den tekniske plattformen bør kunne kontinuerlig produsere en oversikt over maskin- og programvare som inngår i løsningen. |

### Infrastruktur

Med tekniske kapabiliteter knyttet til infrastruktur menes de basis egenskapene plattformen bør ha knyttet infrastruktur.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Kjøremiljø for containere | Den tekniske plattformen bør tilby kjøremiljø for containere som er tilgjengelig for sluttbrukere av analyserom. |
|  | Monitorering av infrastruktur og applikasjoner | Den tekniske plattformen må ha mulighet for å måle ytelse, responsivitet etc. |
|  | Backup | Den tekniske plattformen må ha funksjonalitet for regelmessig sikkerhetskopiering (backup). Funksjonaliteten må kunne testes/verifiseres. |

### Utviklerverktøy

Med tekniske kapabiliteter knyttet til utviklerverktøy menes de egenskapene som trengs for å kunne utvikle applikasjoner på en trygg og effektiv måte på plattformen.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kapabilitet** | **Beskrivelse** |
|  | Applikasjonsutviklingsverktøy | Den tekniske plattformen må inneholde verktøy som muliggjør sikker applikasjons- og tjenesteutvikling. Utviklingsmiljøet bør støtte/kunne integreres med verktøy som undersøker kode og integrasjoner for svakheter og sårbarheter. Verktøy må støtte en sikker utviklingsprosess i smidige miljøer (DevSecOPS). |
|  | Integrasjon mot code repositories | Den tekniske plattformen bør ha mulighet for integrasjon mot kildekode repositories (for eksempel GitHub). |

# Kvalitetskrav

Kvalitetskravene er under arbeid. Denne listen vil derfor være mer bearbeidet i det endelige konkurransegrunnlaget.

Utgangspunktet for kvalitetskrav er standard for kvalitet i produktutvikling – ISO/IEC 25010.

Vi har gruppert kvalitetskravene i følgende kategorier:

* Ytelse
* Kompabilitet
* Brukskvalitet
* Robusthet
* Sikkerhet
* Vedlikeholdbarhet
* Portabilitet

Disse er videre beskrevet i kapitlene under.

### **Ytelse**

Ytelse defineres i forhold til tilgjengelige ressurser under gitte forhold. Kapasitet, særlig brukt som et uttrykk for antall instruksjoner som kan utføres eller antall beregninger som kan foretas pr tidsenhet. Innsats, yteevne og prestasjonsevne er andre begreper for ytelse.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Baseline (utgangspunkt) for ytelse skal være definert | Den ytelsen, prestasjonsevnen, som settes som standard og minimumskrav for en løsning. Dersom ytelsen på noen områder avviker, bør tiltak iverksettes. |
|  | Elementer som påvirker ytelse i løsningen samt nødvendig kapasitet for å opprettholde stabil drift, skal være dokumentert | * Eksempler på elementer: Antall samtidige brukere, transaksjonsvolumer, på timeout for informasjonsutveksling * Kapasitet som løsningen er beregnet for å tåle – normalsituasjon og max. |
|  | Objektive og målbare ytelseskriterier skal være definert, f.eks. svartider og prosesseringstid ved ulik belastning | * Eksempel: xx % av transaksjonene skal være innenfor et gitt tidsintervall * Krav til responstid pr. type/kategori transaksjoner og max./akseptabelt avvik (andel) |
|  | Løsninger skal ha minst like god ytelse som tilsvarende løsninger innen samme løsningsområde |  |
|  | Ytelsen skal ikke forringes i andre komponenter og tjenester i verdikjeden. Avvik fra dette må avtales særskilt | Eksempel: Endringer i Helseanalyseplattformen må avklares mot andre løsninger og aktører f. eks. ID-porten, EPJ’er og Grunndata |
|  | Ytelse skal testes i et egnet testmiljø for ytelsestesting | Ytelsestest skal innfri avtalt baseline for ytelse, i motsatt fall må tiltak iverksettes |

### **Kompabilitet**

Med kompabilitet så menes hvor godt en løsning/et produkt kan samhandle og utveksle informasjon med andre systemer, og/eller hvor godt løsningen/produktet klarer å utføre sine funksjoner i et delt miljø med andre løsninger/produkter. I kompatibilitet legges også overenstemmelse med lover, standarder og rammeverk, interne styringsprinsipper og policy, som ikke tydelig er dekket under andre områder.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Løsninger skal være i overensstemmelse med gjeldende lover, forskrifter, retningslinjer og ev. (bransje)bestemmelser | [Digitaliseringsrundskrivet](https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2623277/), pkt. 1.8 *Følg krav om arkitektur og standarder*  [Difi - Referansekatalogen for IT standarder](https://www.difi.no/referansekatalogen) beskriver pålagte åpne og anbefalte tekniske standarder |
|  | Løsninger skal utformes, utvikles, driftes og forvaltes i overenstemmelse med rammeverk for sikker og effektiv elektronisk samhandling og datautveksling | [Digitaliseringsrundskrivet](https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2623277/), pkt. 1.6 *Bruk nasjonale felleskomponenter og fellesløsninger* og 1.7 *Bruk digital postkasse til innbyggere*  [Difi’s arkitekturrammeverk for samhandling](https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur/arkitekturrammeverk-samhandling) med EIF  [Standardiserte tjenestegrensesnitt (API) for helseregistre](https://ehelse.no/publikasjoner/standardiserte-tjenestegrensenitt-api-for-helseregistre) utarbeidet av Helsedataprogrammet |
|  | Nasjonale felleskomponenter og fellesløsninger skal brukes | [Digitaliseringsrundskrivet](https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2623277/) pkt. 1.6 *Bruk nasjonale felleskomponenter og fellesløsninger*  [Difi - Strategiske prinsipper for nasjonale felleskomponenter](file://shdir.no/Users/Users1/bkrist/Desktop/Strategiske%20prinsipper%20for%20nasjonale%20felleskomponenter) |
|  | Løsningen skal eksponere grensesnitt som fortrinnsvis følger internasjonale og nasjonale standarder | Løsningen skal eksponere grensesnitt som fortrinnsvis følger internasjonale og nasjonale standarder, eksempelvis: [HL7 FHIR](https://ehelse.no/standarder-kodeverk-og-referansekatalog/standarder-og-referansekatalog/anbefaling-om-bruk-av-hl7-fhir-for-datadeling).  Dersom det er behov for grensesnitt som ikke følger en standard så skal dette godt begrunnes og godkjennes av produktansvarlig eller tilsvarende rolle.  Ref. [Digitaliseringsrundskrivet](https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2623277/), pkt. 1.9 *Grenseoverskridende tjenester* |
|  | Endringer i grensesnitt skal være bakoverkompatible så langt det lar seg gjøre | Endringer i grensesnitt skal være bakoverkompatible så langt det lar seg gjøre. Dersom bakoverkompatibilitet ikke er mulig så skal grensesnitt versjoneres. Alle versjoner av grensesnitt skal dokumenteres. Det kan være forretninglogikk som endret fra en versjon til en annen og dette må være dokumentert. |
|  | Løsningens grensesnitt/integrasjoner og datautveksling skal være dokumentert | Dokumentere hvilke API’er som benyttes, hvordan integrasjoner og datautveksling utføres, hvilke data som utveksles og hva integrasjonene omfatter, hvor ofte data oppdateres/utveksles samt estimert datamengde (max.) for gjeldende planperiode |

### **Brukskvalitet**

Omfatter både Universell Utforming (UU) og brukeropplevelse (User eXperience, UX)

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Løsningen skal følge universell utforming (UU)) | Løsninger skal utformes universelt iht. E-helses gjeldende retningslinjer, og minimum iht. krav i forskrift om Universell Utforming (UU). Digitale skjema skal utformes iht. gjeldende retningslinjer fra Difi for offentlige skjema  [Forskrift om universell utforming av IKT](https://lovdata.no/dokument/SF/forskrift/2013-06-21-732)  E-helses retningslinjer (under utforming) |
|  | Løsningen skal gi brukeren støtte i gjennomføring av en oppgave | Løsninger skal gi brukeren støtte til å *gjennomføre sin oppgave* og gjøre *informerte og hensiktsmessige valg* for sin situasjon. Valg skal i størst mulig grad gjøres reversible, og kritiske valg skal utfordres |
|  | Informasjonen som presenteres i løsningene skal oppleves *kontekstuelt* *relevant* for brukerens oppgave, rolle og situasjon, og bidra til å *redusere usikkerhet* knyttet til valg | Helsenorges [*skjema for vurdering av relevans*](https://drive.google.com/file/d/1pWV-2cWcS8ULy6_LaYbnSR4tob3kS_u4/view) |
|  | Informasjonens *troverdighet* skal ivaretas gjennom etterprøvbarhet, konsistens på tvers og et reelt presisjonsnivå for tall og fakta | Reelt presisjonsnivå betyr å passe på at presisjonsnivået for tall og fakta vi opererer med ikke er større enn at vi med rimelighet kan måle eller estimere. Et urealistisk presisjonsnivå kan gi et urealistisk inntrykk av pålitelighet - f.eks kan tallet 123,456 framstå mer pålitelig enn 120 +/- 5, selv om sistnevnte faktisk er mer pålitelig.  Helsenorges [*Innholdsstrategi*](https://helsenorge.no/Sider/redaksjon/innholdsstrategi/default.aspx)og[*Retningslinjer for kvalitet*](https://helsenorge.no/Sider/redaksjon/innholdsstrategi/retningslinjer-for-kvalitet.aspx) |
|  | Løsninger *skal* kunne *konfigureres og tilrettelegges for måling* av avtalte måleindikatorer for brukskvalitet | For eksempel brukerens evne til å gjennomføre sin oppgave og til å gjøre informerte og hensiktsmessige valg for sin situasjon |
|  | Løsninger skal kvalitetssikres gjennom *brukertest og/eller andre relevante metoder* iht. E-helses retningslinjer, både i utviklingsfasen og løpende etter behov | *E-helses retningslinjer* (under utforming) |

### **Robusthet**

Med robusthet menes hvor godt en løsning/et produkt tåler påkjenninger og stress uten at det oppstår avvik eller avbrudd. Pålitelighet vurderes ut ifra forventet bruksmønster og risikokilder som mange brukere, stort transaksjonsvolum, hard/høy belastning.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Det skal lages en kontinuitetsplan for plattformen | Det skal lages en kontinuitetsplan for plattformen. Planen skal gjenspeile de krav som er gitt i ISMS til Direktoratet for e-helse og Norsk Helsenett. Hensikten med å ha en slik plan er å være forberedt på eventuelle hendelser som kan føre til nedetid eller ustabilitet på plattformen.  Se policy for informasjonssikkerhetskontinuitet: <https://isms.ehelse.no/main/policy/book/> view?bookguid=SA16972726418X36EU0 |
|  | Det skal lages en gjenopprettingsplan for plattformen | Det skal lages en gjenopprettingsplan for plattformen. Planen skal gjenspeile de krav som er gitt i ISMS til Direktoratet for e-helse og Norsk Helsenett som også innebærer test av planen. Hensikten med å ha en gjenopprettingsplan er å kunne være i stand til å gjenopprette plattformen raskest mulig dersom plattformen skulle bli helt utilgjengelig. Planen må ta høyde for at infrastrukturen som plattformen kjørte på ikke lenger er tilgjengelig grunnet uforutsette hendelser. Dette kan f.eks. være målbevisst angrep mot infrastrukturen eller naturkatastrofer.  Se policy for informasjonssikkerhetskontinuitet: <https://isms.ehelse.no/main/policy/book/> view?bookguid=SA16972726418X36EU0 |
|  | Automatisk skalering | Løsningen skal kunne automatisk skalere ved behov. Dette gjelder for eksempel dersom det kommer så mange forespørsler at nåværende ressursallokering ikke lenger klarer å ta unne forespørsler som kommer. Løsningen skal også kunne skalere ned igjen automatisk. Hensikten med å kunne skalere automatisk er å ha en fleksibel plattform som ikke bruker mer ressurser enn nødvendig til enhver tid. |
|  | Deploy uten nedetid | Det skal være mulig å deploye nye versjoner av løsningen uten nedetid. Det vil gjøre at man kan deploye til produksjon midt på dagen under høy last uten at det påvirker brukerne av plattformen. Det vil også være en forutsetning for å kunne oppnå hyppige deploy til produksjon i en devsecops-prosess. |
|  | Teknisk plattform må legge til rette for høy oppetid | Løsningen skal ha høy oppetid. Konsumenter av grensesnittene til plattformen skal ha en opplevd høy opplevd oppetid. Leverandøren bes å beskrive hva som kan forventes av opplevd oppetid for sluttbruker. |
|  | Løsninger skal innfri avtalt tjenestenivå (f.eks. tilgjengelighetskrav, tolerert tidsavbrudd/RTO og datatap/RPO) og skal være stabile i bruk | Leverandøren bes angi tidsvindu for følgende:   * RTO: Recovery Time Objective, maksimal gjenopprettingstid til normal drift * RPO: Recovery Point Objective, maksimalt tidsvindu hvor data (transaksjoner) kan være tapt ved en større driftsforstyrrelse |
|  | Dokumentasjon på tilgjengelighet | Tilgjengelighet og responstid må kunne dokumenteres. For dette bør det logges jevnlig tilgjengeligheten og responstiden. Om det ikke følger med slik logging med plattformen eller andre softwarekomponenter bør det utvikles funksjonalitet for denne typen logging. |

### **Sikkerhet**

Omfatter 1) Informasjonssikkerhet: Håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. 2) Personvern: Retten til å bestemme over egne personopplysninger og retten til et privatliv.

Fysisk sikring og personellsikring er ikke omhandlet.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Informasjonssystemer og informasjon skal kategoriseres og klassifiseres | Det er behov for å kunne klassifisere informasjon i løsningen. Eksempler på klassifiseringsklasser er:   * Åpen   + Informasjon som er ment å være offentlig, eksempelvis søknadsveiledningsdokumenter. * Intern   + Informasjon som kan deles mellom saksbehandlere og som kan gjøres tilgjengelig på intranett, eksempelvis informasjon om virksomhetsstyring. * Skjermet   + Informasjon som kan deles mellom saksbehandlere med tjenstlig behov for tilgang til informasjonen, eksempelvis personopplysninger for søker. * Sterkt skjermet   + Informasjon som kun kan deles mellom eksplisitte saksbehandlere med et konkret tjenstlig behov for tilgang til informasjonen, eksempelvis sensitive personopplysninger.   Leverandøren bes beskrive hvordan løsningen legger til rette for klassifisering av informasjon i disse. |
|  | Administrasjon av Begrenset/Sterkt Begrenset innhold. | Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for utvidede tilgangsrettigheter for tilgang til større mengder data/informasjon. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes. Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger. All tildeling av autorisasjon skal registreres i et autorisasjonsregister. Registeret skal som minimum inneholde:   * informasjon om hvem som er tildelt autorisasjon * til hvilken rolle autorisasjonen er tildelt (om rolle benyttes i virksomheten) * formålet med autorisasjonen * tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt * tidsbegrensninger på autorisasjoner, f.eks. forskningsprosjekt, ansettelses- eller avtaleforhold * informasjon om hvilken virksomhet den autoriserte er knyttet til * roller og rettigheter som har blitt tildelt brukerne * alle innlegginger, endringer og sletting av tilganger basert på autorisasjoner   Leverandøren bes beskrive hvordan løsningen legger til rette for et autorisasjonsregister. |
|  | Oversikt over utstyr som programvare og maskinvare | Det er en forutsetning at leverandøren 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. Leverandøren bes beskrive hvordan de ivaretar oversikt over og kontroll på utstyr og programvare som benyttes i løsningen. |
|  | Konfigurasjonskart | Leverandøren skal dokumentere alle konfigurasjoner i et konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen. Dokumentasjonen skal vise leverandørens og eventuelle underleverandørers datasentre og lokasjoner.   * Leverandøren bes beskrive hvorledes de dokumenterer konfigurasjoner av utstyr og programvare. |
|  | Konfigurasjons endringer og Kontroll. | Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før risikoreduserende tiltak er gjennomført. Eksempler kan være:   * Prosess for godkjenning og gjennomføring av endringer * 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 kunden * Leverandøren bes beskrive hvordan de planlegger og gjennomfører konfigurasjonsendringer i utstyr og/eller programvare. |
|  | Risikostyring og kontinuerlig oppfølging av risiko. | Leverandøren skal ha rutiner for å jevnlig følge opp risiko, evaluere at tiltak er gjennomført i henhold til risikoanalyse, samt vurdere om eksisterende fungerer etter hensikt, og om nye tiltak er nødvendig f.eks. pga. at risikonivået er endret. |
|  | Løsninger skal etableres i tråd med prinsippene for innebygd personvern | * [Digitaliseringsrundskrivet](https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2623277/), pkt. 1.5 *Innebygd personvern* * Datatilsynet: [Innebygd personvern](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/) * E-helses Policy for programvareutvikling og innebygget personvern |
|  | Personopplysninger skal behandles iht. GDPR og løsningens behandling av personopplysninger og sensitive personopplysninger skal være dokumentert | * [De 7 grunnleggende personvernprinsippene](file://shdir.no/Users/Users1/bkrist/Desktop/%20%20https/www.datatilsynet.no/regelverk-og-verktoy/veiledere/grunnleggende-personvernprinsipper/?id=7770): *Lovlig, rettferdig og gjennomsiktig*, *Formålsbegrensning*, *Dataminimering, Riktighet, Lagringsbegrensning, Integritet og fortrolighet*, *Ansvarlighet* * [E-helses mal for databehandleravtale](https://ehelse.no/mal-for-databehansedleravtale) |
|  | Sletterutiner | Leverandøren skal ha sletterutiner som sikrer at slettet data ikke kan gjenskapes.   * Leverandøren bes beskrive hvordan data slettes. |
|  | Slettede opplysninger som er kopiert ut på sikkerhetskopier | Leverandøren bes beskrive hvordan slettede data som er tatt sikkerhetskopi av, håndteres, f.eks hvordan sikrer leverandøren at det ikke legges tilbake data som er slettet til plattform eller analyserom ved tilbakeføring av sikkerhetskopi.  Eksempel: Personopplysninger kan være slettet som følge av tilbaketrukket samtykke eller at formål ikke lenger er gyldig) |
|  | Sikring av APIer | API'er som tilgjengeliggjøres skal være sikret med tilgangskontroll og beskyttelse av konfidensialitet og integritet. Kun sikre protokoller skal benyttes.  Penetrasjons tester må kunne inkludere APIs |
|  | Sikker Utviklingsprosess – Sikker SDLC | Programvareutviklimg må følge DevSecOps prinsipper med innbygget sikkerhet i alle ledd.  Må tilrettelegge for automatiserte tester/verifikasjon i alle ledd, og sikre at kode/biblioteker som benyttes ikke har sårbarheter eller at sårbarhetene mitigeres i tilstrekkelig grad basert på kundens akseptable risiko nivå. |
|  | Revisjon av Utviklingsprosjekter | Leverandøren må legge til rette for at kunden kan revidere sikkerhet basert på OWASP ASVS, og bidra til støtte for automatisering av slik kontroll. |
|  | Sikring av Kontainermiljø | All dataflyt, også intern, må benytte sikre protokoller for transport. Utvikling basert på Kontainerteknologi bør følge prinsipper om sikker SDLC og DevSecOps. Automatisk støtte i de forskjelle steg bør være tilgjengelig, slik at sikkerhetsfunksjonalitet kan automatiseres og ikke bli en flaskehals i et smidig utviklingsløp. |
|  | Det skal være en plan for operasjonalisering og hvordan endringen påvirker drifts- og forvaltningsorganisasjon | F.eks. konsekvens i roller, ansvar og oppgaver |
|  | Rollebasert Tilgangskontroll | For å skille på brukere med ulike rettigheter forventes det at leverandøren implementerer og vedlikeholder rollebasert tilgangsstyring. Leverandøren bes redegjøre for sin tilgangsstyringsmodell. |
|  | Tilgang til administrasjons- og driftsgrensesnitt skal skje via sikrede og godkjente arbeidsstasjoner. | Leverandøren bes redegjøre for hvordan de sikrer arbeidsstasjoner som benyttes for administrasjon og tilkoblingen mot administrasjonsgrensesnitt i den eksterne tjenesten. |
|  | Beskyttelse av Autorisasjonsregister | Autorisasjonsregisteret skal være beskyttet mot uautoriserte endringer, og skal kunne benyttes til å hente ut informasjon om autorisasjoner minimum 5 år etter en autorisasjon er trukket tilbake.  Leverandøren bes beskrive hvordan de sikrer autorisasjonsregisteret. |
|  | Revisjon | Leverandøren skal jevnlig gjennomføre interne revisjoner, herunder testing av tekniske, organisatoriske og fysiske sikkerhetstiltak.  Leverandøren bes beskrive hvordan de planlegger, gjennomfører og dokumenterer revisjoner og testing. |
|  | Underleverandør styring | Leverandøren skal sørge for at eventuelle underleverandører følger sikkerhetsrelaterte retningslinjer og krav.  Leverandøren bes beskrive hvordan de følger opp sikkerhetsarbeidet hos sine underleverandører. |
|  | Sikkert Datamottak | Det må være mulig å motta data av variert størrelse (opp til 100Gb filer) i et sikkert data mottak, hvor verifikasjon og scanning av data for skadevare utføres ved hjelp av verktøy som kan benytte signaturer, heuristisk og anomali basert metoder.  Skadevare i data som mottas skal ikke kunne spre seg til andre soner.  All trafikk in/ut av datamottak skal overvåkes.  Datamottak bør inneholde verktøy for å overvåke endringer i filer/filsystem, som File Integrity Monitoring (FIM)  Datamottak må ha evnen til å pakke ut og utføre dekryptering av filer. |
|  | Fjernaksess | Leverandøren skal implementere fysiske sikringstiltak for bruk av fjernaksess.  Leverandøren bes på en overordnet måte beskrive sine fysiske sikringstiltak. |
|  | Separasjon av data fra forskjellige kunder | Leverandøren skal separere data som tilhører forskjellige kunder. Leverandørens egne data skal separeres fra kundenes data.  Leverandøren bes beskrive sin sikkerhetsarkitektur med hensyn til separasjon av data som tilhører forskjellige kunder. |
|  | Logg og Sporing | For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over følgende:   * Autorisert bruk av informasjonssystemene skal registreres. * Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet. * Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk. * Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk. * Andre viktige komponenter bør registrere autorisert bruk og forsøk på uatorisert bruk. * Leverandøren bes beskrive hvordan de vil etablere hendelsesregistrering i løsningen. |
|  | Analyse av Logger | Logger (data og informasjon) i hendelsesregistrene skal kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd. Videre skal loggene fra hendelsesregistre kunne eksporteres eller gjøres tilgjengelig for eksterne analyseverktøy.  Leverandøren bes beskrive hvordan data fra hendelsesregistre kan tilgjengeliggjøres for analyse. |
|  | Beskyttelse av logger | Loggene i (hendelsesregistrene) skal sikres mot uautorisert endring og sletting. Leverandøren bes beskrive hvordan de sikrer hendelsesregistrene. |
|  | Beskyttelse av data under transport, prosessering og lagring | Leverandøren skal ha mekanismer for sikring av data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.  Leverandøren bes beskrive hvordan de sikrer data under transport, prosessering og lagring. |
|  | Krypteringsnøkler | Kryptering forutsetter en forsvarlig behandling av partenes krypteringsnøkkel(er).  Leverandøren bes beskrive hvordan de håndterer krypteringsnøkler.  Leverandøren skal legge til rette for at kryperingsnøkler kan administrers av ekstern part ved hjelp av en Hardware Security Modul. |
|  | Bruk av Krypteringsnøkler og Algoritmer | Leverandøren må legge sikre at Bruk av kryptering algoritmer er i henhold til etablerte standarder og krav som sikrer mot bruk av utdatert algoritmer og/eller nøkler som har kjente svakheter eller er kompromitterte eller ikke lenger ansees som sikre nok til formålet.  Det må være mulig å bytte algoritme og nøkler, og kryptert materiale må kunne re-krypteres med ny algoritme/nøkler i en slik situasjon. |
|  | Kontinuerlig Deteksjon av Sikkerhetshendelser | Leverandøren bør sørge for Kontinuerlig deteksjon av Sikkerhetshendelser, evne til å varlse/(integrere med Hendelseshåndteringsprosesser og varslings rutiner hos Sky-leverandør og Kunde. Må kunne følge de nødvendige lovkrav, inkludert bevissikring og uttrekk/eksportering av logger, samt mulight til å utføre forensic analyse etter hendelser.  Deteksjon bør være basert på en kombinasjon av nettverks basert teknologi (f.eks IDS) som inspiserer datastrømmer mellom komponenter og endepunkt baserte komponenter som kan analysere trafikk fra endepunkter (f.eks. HIPS, EDR) |
|  | Overvåkning av Trusselnivå | Leverandøren bør sørge for at informasjon om aktuell sikkerhetsstatus samt eventuell endringer i risikonivået Kontinuerlig gjøres tilgjengelig for kunde, slik at kan oppfylle sitt behov for sikkerhetsstyring. |
|  | Blokkering av Utgående trafikk fra Analyserom basert på Klassifisering. | Leverandøren må sørge for at det er mulig å begrense og/eller sperre for all utgående trafikk fra Rom eller Soner som klassifiseres som BEGRENSET eller STERKT BEGRENSET. |
|  | Beskyttelse mot Tjenestenektangrep | Den tekniske plattformen må ha mekanismer for å beskytte mot applikasjonsbaserte- og nettverks-baserte tjenestenektangrep. |
|  | Fysisk sikkerhet | Den tekniske plattformen må tilfredsstille høye krav til fysisk sikring av datasentre, herunder adgangskontroll, perimeter- og skallsikring, samt beskyttelse mot både naturkatastrofer og uønskede ondsinnete handlinger. |
|  | Sikker Dataplattform | Dataplattform skal kunne etableres med et sikkerhetsnivå som er minst like høyt som dagens registre. |

### **Vedlikeholdbarhet**

Med vedlikeholdbarhet så menes hvor enkelt og kostnadseffektivt det er å utføre modifisering av en løsning/et produkt for å korrigere feil, forbedre ytelsen, endre attributter/funksjoner osv. Herunder at produktet/løsningen er forvaltningsvennlig i kunde- og brukerdimensjonen og kan styres, følges opp og forvaltes i tråd med god praksis.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Løsninger skal ha god endringsevne | Det skal være enkelt og kostnadseffektivt å korrigere/endre og en endring skal kun gjøres ett sted. God endringsevne innebærer å lage en løsning med løse koblinger mellom komponenter og holde kompleksitet på kode på et lavt nivå. |
|  | Løsningen skal tilrettelegges for automatisert verifisering/testing | Løsninger skal tilrettelegges for automatisert testing. Endringer i produksjon skal kunne verifiseres og reverseres. Løsninger skal testes med syntetiske testdata og endringer skal regresjonstestes. |
|  | Kildekoden til løsningen skal benytte et versjonskontrollsystem | Det er viktig at all kode lagres i et versjonskontrollsystem med adgangskontroll. Kun autentiserte og autoriserte brukere kan sjekke inn kode i systemet. Alle kodeendringer skal være sporbare og kunne knyttes til en gitt oppgave. |
|  | Løsningens system- og driftsdokumentasjon skal være iht. god praksis | F.eks. beskrive følgende:   * Formål og virkemåte * Brukere, interessenter og aktører og samhandling i verdikjeden * Bredding og bruk av tjenestene * Teknisk løsning og oppsett * Analoge tjenester (saksbehandling og støttetjenester) |
|  | Løsningens forvaltningsdokumentasjon skal være i tråd med god praksis | F.eks. beskrive følgende:   * Dataansvar (pålagt iht. GDPR) * Tidsmessighet og ajourhold ift. lover, forskrifter og pålegg * Plan for løpende vedlikehold og videreutvikling * Kostnadsstruktur og finansiering * Lisens- og avtaleforhold |
|  | Løsningen skal tilrettelegges for automatisert verifisering/testing | Automatisert testing gjør det lettere og raskere å utvikle ny kode. |
|  | Utfasing av gamle versjoner av tjenester | Gamle og utdaterte versjoner skal kunne fases ut ihht et omforent utfasingsregime. Dvs at utfasing av gamle tjenester skal være koordinert med konsumenter av tjenestene. Dette bør forankres i en avtale med konsumentene. |

### **Portabilitet**

Portabilitet eller flyttbarhet, er evnen et produkt/en løsning har til å kjøre korrekt på ulike plattformer og i miljøer som f.eks. test- og produksjonsmiljøer og på reserveløsning.

|  |  |  |
| --- | --- | --- |
| **ID** | **Kvalitetskrav** | **Beskrivelse** |
|  | Løsningens krav til teknisk plattform og arkitektur og bruk av ulike miljøer, skal være dokumentert | * Portabilitet angår evne og mulighet ev. begrensinger til å kunne tilpasse seg skiftende omgivelser og betingelser. * Avhengigheten i oppsett av test- og driftsmiljøer eller komponenter i disse slik som bruk av database, fysisk/virtuelt Infrastruktur, middleware og lisenser |
|  | Bruk av proprietært utstyr, tilbehør og/eller programvare bør unngås | Valg skal begrunnes og dokumenteres. Plattformen som skal etableres bør unngå "vendor lock-in" dersom mulig |

1. <https://ehelse.no/Lists/Publikasjoner/Attachments/27/Konseptvalgutredning%20for%20Helseanalyseplattformen.pdf> [↑](#footnote-ref-2)
2. <https://www.regjeringen.no/contentassets/1fe9cf37e64344e1a3b3c62f950b100b/170630_helsedatalovutvalget.pdf> [↑](#footnote-ref-3)
3. <https://helseatlas.no/> [↑](#footnote-ref-4)
4. <https://www.kreftregisteret.no/Registrene/data-og-statistikk/statistikkbank/> [↑](#footnote-ref-5)
5. Denne brukerhistorien er tenkt løst gjennom anskaffelsen som går på videreutvikling av helsedata.no (søknadstjenester og saksbehandling), men er tatt med her som informasjon til Leverandøren. [↑](#footnote-ref-6)
6. <https://ehelse.no/Documents/E-helsekunnskap/Sluttrapport%20-%20Referansearkitektur%20Helseregistre.pdf> [↑](#footnote-ref-7)
7. <https://ehelse.no/Documents/Rapporter%20og%20dokumenter%20standardisering/Anbefaling%20om%20bruk%20av%20HL7%20FHIR%20for%20datadeling.pdf> [↑](#footnote-ref-8)