

Helseanalyseplattformen (HAP)

Kravspesifikasjon data- og analysetjenester v0.85

|  |
| --- |
|  |



|  |
| --- |
| **Rapportens tittel:**  Kravspesifikasjon data- og analysetjenester v0.85  **Utgitt:**  28. juni 2019  **Utgitt av:**  Direktoratet for e-helse  **Kontakt:**  helsedataprogrammet@ehelse.no  **Besøksadresse:**  Verkstedveien 1, 0277 Oslo  Tlf.: 21 49 50 70 |

Forord

|  |
| --- |
|  |



**Innhold**

[1 Sammendrag 7](#_Toc12622429)

[2 Bakgrunn og overordnet målbilde 8](#_Toc12622430)

[2.1 Etablering av et økosystem 10](#_Toc12622431)

[2.2 Personvern og informasjonssikkerhet 11](#_Toc12622432)

[2.3 Nærmere om relevant regelverk og betydningen for leveransene 13](#_Toc12622433)

[2.4 Forretningsarkitektur 14](#_Toc12622434)

[2.4.1 Forretningskapabiliteter 14](#_Toc12622435)

[2.4.2 Prosesser 18](#_Toc12622436)

[3 Sentrale rammebetingelser 23](#_Toc12622437)

[3.1 Rammebetingelser 23](#_Toc12622438)

[4 Kundens overordnede plan for implementering 23](#_Toc12622439)

[4.1 Stegvis etablering av Helseanalyseplattformen 23](#_Toc12622440)

[4.2 Stegvis etablering av Helsedataservice 24](#_Toc12622441)

[4.3 Arbeidsstrømmer og milepæler 25](#_Toc12622442)

[4.3.1 Arbeidsstrømmer 26](#_Toc12622443)

[4.3.2 Milepæler for 2020 og 2021 27](#_Toc12622444)

[5 Funksjonelle krav 29](#_Toc12622445)

[5.1 Fase 1 29](#_Toc12622446)

[5.2 Funksjonelle krav for data- og analysetjenester 30](#_Toc12622447)

[5.2.1 Dataplattform med innebygget personvern 30](#_Toc12622448)

[5.2.2 Data- og analysetjenester 36](#_Toc12622449)

[5.2.3 Innbyggertjenester 45](#_Toc12622450)

[5.3 Opsjon 1 – Arkiv i Norge 48](#_Toc12622451)

[6 Utforming av Helseanalyseplattformen 50](#_Toc12622452)

[6.1 Metadata, kodeverk og terminologi 50](#_Toc12622453)

[6.2 Integrasjoner 52](#_Toc12622454)

[6.2.1 Integrasjon mot eksterne tjenester og grensesnitt 54](#_Toc12622455)

[6.2.2 Integrasjon av datakilder inn på dataplattformen 57](#_Toc12622456)

[6.2.3 Integrasjon mot Helsenettet 74](#_Toc12622457)

[6.3 Antatt nødvendige tekniske kapabiliteter 77](#_Toc12622458)

[6.3.1 Dataforvaltning 78](#_Toc12622459)

[6.3.2 Informasjonssikkerhet og personvern 79](#_Toc12622460)

[6.3.3 Analyseverktøy 81](#_Toc12622461)

[6.3.4 Integrasjon 82](#_Toc12622462)

[6.3.5 Administrasjonsverktøy 83](#_Toc12622463)

[6.3.6 Infrastruktur 84](#_Toc12622464)

[6.3.7 Utviklerverktøy 85](#_Toc12622465)

[7 Kvalitetskrav 86](#_Toc12622466)

[7.1 Ytelse 86](#_Toc12622467)

[7.2 Kompabilitet 86](#_Toc12622468)

[7.3 Brukskvalitet 88](#_Toc12622469)

[7.4 Robusthet 89](#_Toc12622470)

[7.5 Informasjonssikkerhet og personvern 92](#_Toc12622471)

[7.5.1 Risikostyring 92](#_Toc12622472)

[7.5.2 Personvernprinsipper 93](#_Toc12622473)

[7.5.3 Den registrertes rettigheter 94](#_Toc12622474)

[7.5.4 Ansatte, kompetanse og holdningsarbeid 96](#_Toc12622475)

[7.5.5 Tilgangsstyring 97](#_Toc12622476)

[7.5.6 Fysisk sikkerhet, kryptografi og håndtering av utstyr 99](#_Toc12622477)

[7.5.7 Sikker utvikling og forvaltning 101](#_Toc12622478)

[7.5.8 Kommunikasjonssikkerhet 104](#_Toc12622479)

[7.5.9 Håndtering av personvern- og informasjonssikkerhetsbrudd 105](#_Toc12622480)

[7.6 Vedlikeholdbarhet 108](#_Toc12622481)

[7.7 Portabilitet 109](#_Toc12622482)

# Sammendrag

Dette dokumentet beskriver omfanget for anskaffelsen for data- og analyseplattformen for Helseanalyseplattformen. Dokumentet beskriver behovene som skal dekkes gjennom løsningen som skal anskaffes og skal ikke fylles ut av Leverandøren.

* Kapittel 2 beskriver bakgrunnen for etablering av Helseanalyseplattformen og Kundens overordnede målbilde. Her er også en overordnet dokumentasjon av forretningsarkitekturen.
* Kapittel 3 beskriver sentrale rammebetingelser.
* Kapittel 4 beskriver Kundens overordnende plan for implementering av løsningen.
* Kapittel 5 beskriver Kundens funksjonelle krav til data- og analysetjenester.
* Kapittel 6 beskriver blant annet eksterne systemer som må kunne integreres løsningen, samt Kundens synspunkter om hvilke egenskaper den tekniske løsningen bør inneholde.
* Kapittel 7 beskriver Kundens kvalitetskrav til løsningen

# Bakgrunn og overordnet målbilde

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 for 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 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 bidra til å etablere fellestjenester for bruk av helseregistrene og andre relevante datakilder, slik at registerforvalterne ikke trenger å utvikle, forvalte og drifte slik funksjonalitet 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 kan ligge til grunn for helseanalyser.

Helsedataprogrammet 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 tilrettelegger for innovasjon ved at private/offentlige selskaper får mange nye forretningsmuligheter, gjennom utnyttelse av nettverkseffekter som økosystemet skaper.

Helseanalyseplattformen skal også forsterke personvernet gjennom redusert eksponering av personopplysninger, 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 brukere. Disse brukergruppene har flere behov som i stor grad kan betjenes av de samme tekniske løsningene og organisatoriske funksjonene.

De tekniske komponentene som etableres skal 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 enhet med vedtaksmyndighet og baseres på et nettverkssamarbeid mellom dagens registerforvaltere og andre myndigheter.



Figur 1: Overordnet illustrasjon av Helseanalyseplattformens målbilde

Helsedataprogrammet 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

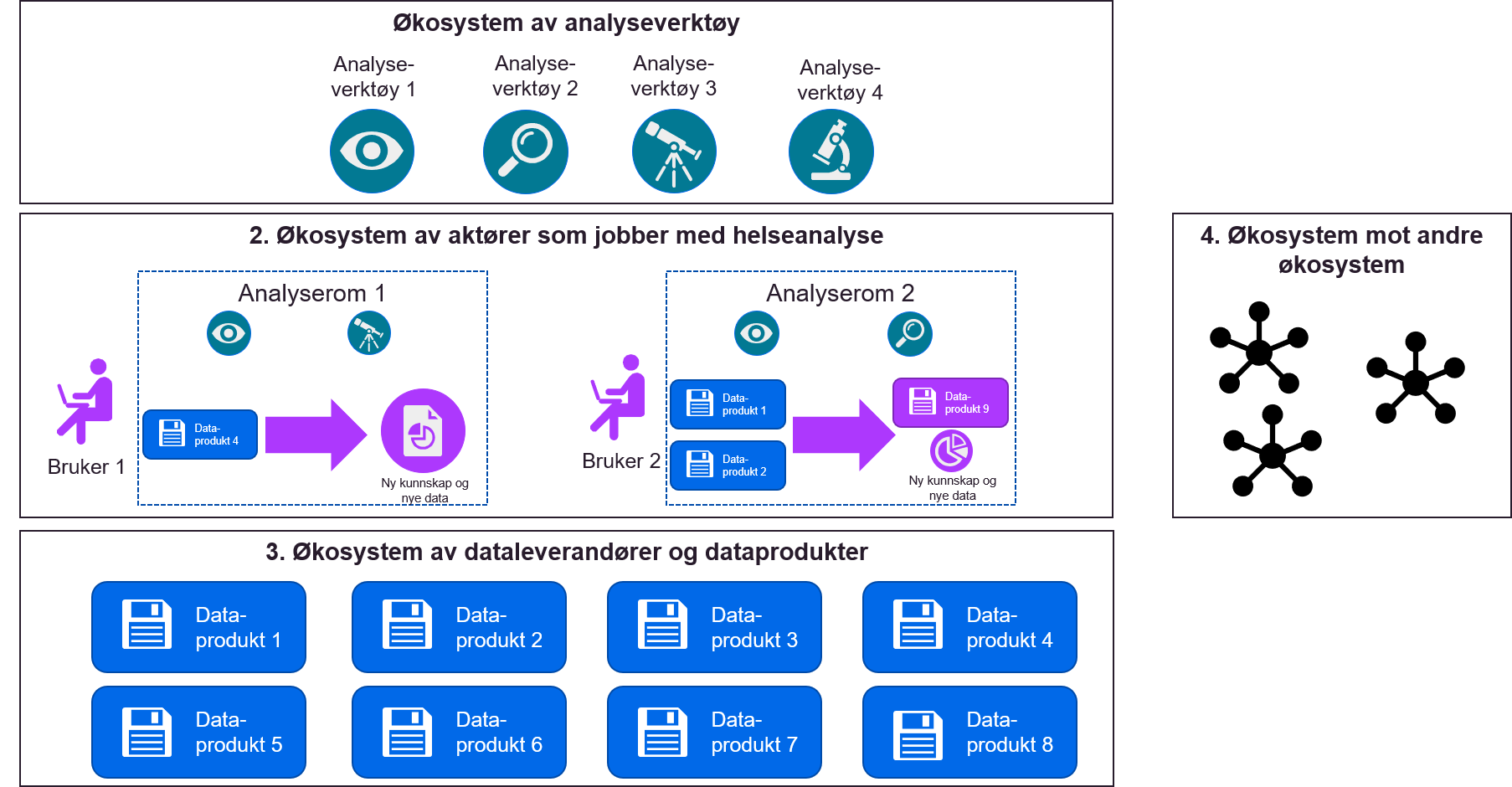
Plattformbegrepet knyttes ofte til moderne løsninger som for eksempel Google og Apple. Disse kjennetegnes ved at det er tre hovedaktører på en og samme tekniske plattform;

* Plattformeier
* Leverandører
* Brukere

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.

Økosystembegrepet i Helsenanalyseplattformen knyttes til flere dimensjoner:

1. Økosystem av analyseverktøy: Vi ønsker å etablere en teknisk løsning der aktører kan tilby sine analyseverktøy, analysetjenester og analyseinfrastrukturer gjennom Helseanalyseplattformen.
2. Økosystem av aktører som jobber med helseanalyse: Vi ønsker å etablere en infrastruktur der ulike aktører, både offentlige og private, kan etablere helseanalyseløsninger på plattformen.
3. Økosystem av dataleverandører med sine dataprodukter: Vi ønsker å etablere et økosystem av dataleverandører slik at dataprodukter fra virksomheter med ulik ekspertise kan tilgjengeliggjøres gjennom Helseanalyseplattformen. Et dataprodukt er et datasett som personer med bestemt domenekunnskap eier, kurerer, og tilgjengeliggjør slik at det kan benyttes av andre.
4. Økosystem med andre økosystem: Analyseøkosystemet må også sees i sammenheng med andre nasjonale og internasjonale økosystemer.



Figur 2: Illustrasjon av ulike dimensjoner av økosystem som treffer Analyseøkosystemet

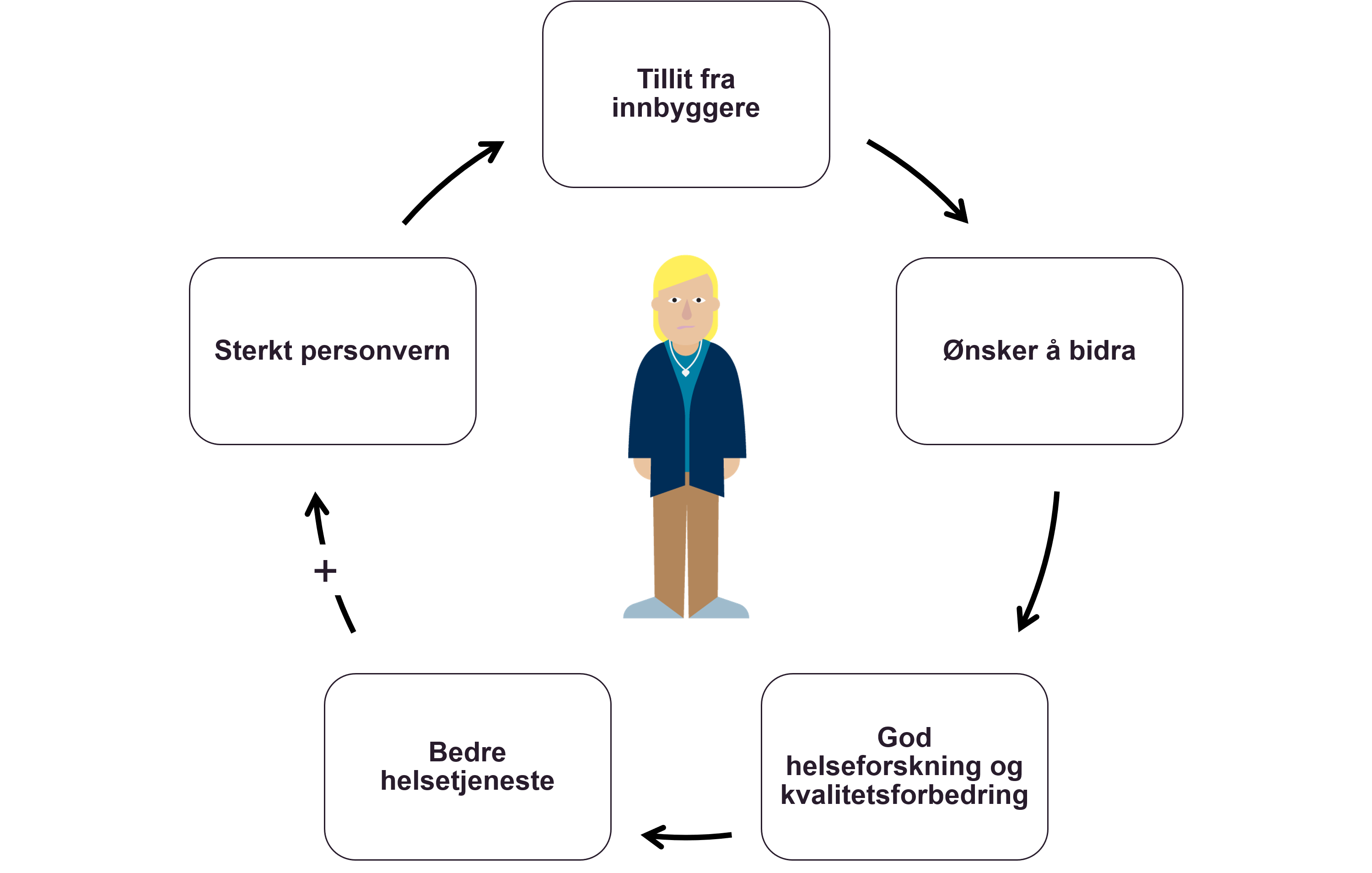
## Personvern og informasjonssikkerhet

Personvern handler om individets rett til privatliv og retten til å ha kontroll over egne personopplysninger. Personvern er en grunnleggende menneskerettighet og er nedfelt i en rekke internasjonale konvensjoner i tillegg til Grunnloven.

Etableringen av Helseanalyseplattformen vil medføre at det behandles et stort antall personopplysninger om mange personer, herunder helseopplysninger av svært privat karakter som har et særskilt vern i norsk lov. Dette er opplysninger som i mange tilfeller er avgitt i all fortrolighet og med en forventning om diskresjon og konfidensialitet. Opplysningene har dermed et høyt beskyttelsesbehov og konsekvensene for den enkelte dersom disse kommer på avveie eller brukes ulovlig, er potensielt store.

Helsedataprogrammets innbyggerundersøkelse viser at villigheten til å dele helsedata generelt er stor, men også at dette er opplysninger som de vil ha beskyttet fra uvedkommende. Befolkningen ønsker god ivaretakelse av personvernet og kontroll over egne personopplysninger. Samtidig er tilbakemeldingen fra innbyggerne at økt innsikt, forståelse og kontroll gir økt trygghet, tillitt og velvilje til å dele.

For at Helseanalyseplattformen skal ha den nødvendige tillitten både hos bruker og den registrerte er det helt avgjørende at både informasjonssikkerhet og grunnleggende personvernrettigheter ivaretas i alle deler av løsningen. Dette er et langt på vei et suksesskriterie for en plattform som er utviklet for å behandle helseopplysninger og avgjørende for at man skal kunne nå målet om god helseforskning og kvalitetsforbedring og gjennom dette en bedre helsetjeneste. Hvis ikke borgerne kjenner seg trygge på at data blir lovlig og sikkert håndtert risikerer man at viljen til å bidra med egne personopplysninger reduseres. Også brukergruppenes vilje til å ta i bruk de ulike verktøy og tjenester er avhengig av at de vet at behandling av data på plattformen vil skje på en slik måte at de etterlever lover og regler.



Figur 3: Illustrasjon rundt hvordan sterkt personvern kan sikre tillitt fra innbygger og opprettholde innbyggers ønsker om å bistå i utviklingen av bedre helsetjenester

Helsedataprogrammet har utviklet seks prinsipper som skal sikre at innbyggers personvern blir ivaretatt. Ved etablering av Helseanalyseplattformen skal innbygger føle seg trygg på at disse prinsippene blir respektert.

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 reservere 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

Prinsippene reflekterer krav og rettigheter i personvernregelverket og skal gjennomsyre det arbeidet som gjøres i utviklingen og innføringen av Helseanalyseplattformen. Det er en forutsetning at det til enhver tid gjeldende regelverk for informasjonssikkerhet og behandling av personopplysninger kan etterleves i systemet samtidig som Kundens behov ivaretas.

Dette krever en leverandør hvor ansatte har høy kompetanse innenfor personvern og informasjonssikkerhet og som forstår og respekterer betydningen av at dette står sentralt i alle deler av leveransen, herunder i egen forretningspraksis og i valg av samarbeidspartnere.

## Nærmere om relevant regelverk og betydningen for leveransene

Leveransene i Helsedataprogrammet vil være underlagt en rekke lover og forskrifter, hovedsakelig knyttet til områdene personvern og sikkerhet, helserett, anskaffelser og generell offentligrettslig regulering som f. eks forvaltningsloven og offentleglova..

For tiden pågår det et lovarbeid i Helse- og omsorgsdepartementet (HOD) som er helt sentralt for leveransene beskrevet i denne anskaffelsen. Lovarbeidet vil antagelig danne grunnlaget for at det foreslås en lovhjemmel for etablering av Helseanalyseplattformen og Helsedataservice. Videre foreslås det samlede og enhetlige lovregler om tilgjengeliggjøring- og sammenstilling av helsedata og hjemmel for å etablere et nytt personidentifiserbart legemiddelregister som skal erstatte Reseptregisteret. Slik vi forstår det er utkast til høringsnotat nå til politisk behandling, og det er forventet at lovarbeidet vil komme på ordinær høring i løpet av sommeren 2019. Det er ventet at HOD parallelt med ordinær høring vil starte et forskriftsarbeid (blant annet for Helseanalyseplattformen), slik at forskriftene kan tre i kraft samtidig med lovhjemmelen tidligst 1.1.2021. Leveransene fra Helsedataprogrammet vil medføre en behandling av personopplysninger som reguleres av EMK artikkel 8, Grunnloven § 102, personopplysningsloven og personvernforordningen.

Videre vil sekundærbruk av helseopplysninger som skjer på plattformen i tillegg reguleres av helseregisterloven der formålet er statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten.

Helseanalyseplattformen skal etter planen inneholde kopier av data fra eksisterende helseregistre, herunder lovbestemte helseregistrene, medisinske kvalitetsregistre og befolkningsbaserte helseundersøkelser. Disse har hjemmel i helseregisterloven.

Helseforskningsloven regulerer tilgjengeliggjøring og bruk av helseopplysninger til forskning, og kommer til anvendelse når formålet med behandlingen (hos mottaker) er medisinsk og helsefaglig forskning. Loven har bestemmelser om taushetsplikt som foreslås endret i ovennevnte høringsnotat uten at vi kan se at dette får direkte betydning for leveransene.

Behandling av demografiske og sosioøkonomiske opplysninger på plattformen er underlagt regulering i folkeregisterloven, forvaltningsloven, statistikkloven og personopplysningsloven. Det er fremmet forslag til ny statistikklov som vil ha betydning for om data som forvaltes av SSB kan gjøres tilgjengelig på Helseanalyseplattformen.

Helsepersonelloven har bestemmelser om taushetsplikt som er relevante ved sekundærbruk av pasientopplysninger. Det er antatt at det vil gjøres endringer i helsepersonelloven som gjør at myndigheten får dispensasjon for taushetsplikt vil tillegges Helsedataservice.

Det er lagt til grunn at driften og organiseringen av Helseanalyseplattformen, herunder Helsedataservice, legges til et forvaltningsorgan under HOD som da vil være underlagt forvaltningsloven, offentleglova og arkivloven med tilhørende forskrifter.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) er en bransjenorm utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren. Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Kravene i Normen er sentrale for sektorens tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern. Helsedataprogrammet ved Direktoratet for e-helse er forpliktet til å følge Normen.

Sikkerhetsloven kan komme til anvendelse på dataplattformen hvis denne blir vurdert å inneholde skjermingsverdig informasjon og/eller må anses om et skjermingsverdig objekt eller infrastruktur. Det pågår en prosess i Direktoratet for e-helse hvor man i samarbeid med HOD foretar konkrete verdi- og skadevurderinger på blant annet e-helseløsningene i direktoratet. Dersom sikkerhetsloven kommer til anvendelse på tjenesten vil det stilles omfattende krav til blant annet forebyggende sikkerhetsarbeid, informasjonssikkerhet og informasjonssystemsikkerhet.

Andre lover som er relevante innenfor helse- og omsorgstjenesten er pasientjournalloven, pasient- og brukerrettighetsloven, folkehelseloven, smittevernloven, bioteknologiloven, helseberedskapsloven. Vi går ikke nærmere inn på disse her, da det må vurderes konkret av dataansvarlige for behandling av personopplysninger på Helseanalyseplattformen og andre brukere i hvilken grad dette regelverket får anvendelse på aktiviteter som skjer på eller i tilknytning til dataplattformen.

## Forretningsarkitektur

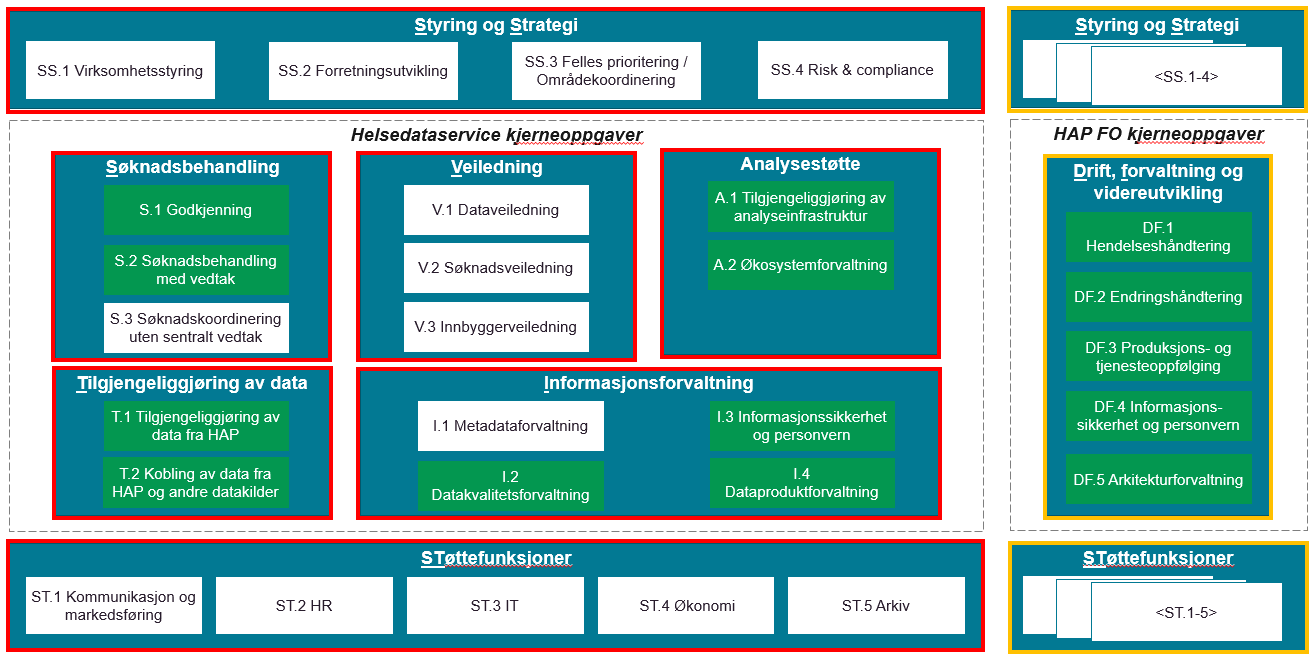
Det er identifisert to sentrale organisasjonsenheter som må etableres i forbindelse med at Helseanalyseplattformen introduseres:

1. Helsedataservice er virksomheten som vil være eier av Helse­analyseplattformen og analyseøkosystemet tilknyttet plattformen. Helsedata­service vil tilby enkelte tjenester som brukerveiledning, søknads- og saksbehandling, samt tilgjengeliggjøre data fra Helseanalyseplattformen. Organisatorisk forankring for denne virksomheten er ikke besluttet i skrivende stund.
2. Helseanalyseplattformens forvaltningsorganisasjon («HAP FO») er virksomheten som vil være ansvarlig for drift og forvaltning av Helseanalyseplattformen. Det er ikke tatt noen endelig beslutning om hvilken virksomhet som vil eie HAP FO, men mest sannsynlig vil den ligge under Norsk Helsenett i rollen nasjonal tjenesteleverandør.

### Forretningskapabiliteter

For å realisere ambisjonene for Helseanalyseplattformen, har vi identifisert ett sett med forretningskapabiliteter som Helsedataservice med tilhørende forvaltningsorganisasjon, HAP FO, må etablere i forbindelse med realisering av målbildet til Helsedataprogrammet. I tillegg har vi identifisert og skissert prosesser innenfor kjerneoppgavene til Helsedataservice.

Figuren under illustrerer de forretningskapabiliteter som er identifisert så langt. Kapabilitetene til Helsedataservice er markert med rød kant, og kapabilitetene til HAP FO er markert med gul kant. Kapabiliteter markert som grønne bokser, er de som er mest relevante i forbindelse med etablering av en dataplattform og analysetjenester.



Figur 4: Forretningskapabiliteter for Helsedataservice og HAP FO

I tabellen under har vi beskrevet nærmere kapabilitetene i forretningsarkitekturen som vi definerer som kjerneoppgaver.

| ID | Navn | Beskrivelse |
| --- | --- | --- |
| S | Søknads-behandling | Helsedataservice skal behandle søknader om godkjenning (virksomhetsgodkjenning), søknader om helsedata, fatte vedtak om tilgjengeliggjøring av data, samt koordinere søknadsbehandling på tvers av ulike dataleverandører. |
| S.1 | Godkjenning | Helsedataservice skal gjennom vurdering av kvalifikasjoner (økonomi, etisk standard, forsknings- eller analysekompetanse, kvalitetssystem/ISO-sertifisering, personvernsertifisering) kunne godkjenne virksomheter og institusjoner (innenfor alle segmenter/målgrupper) som brukere av Helseanalyseplattformen. Dette skal forenkle behandlingen av søknader om tilgang til person­opplysninger på Helseanalyseplattformen fra disse virksomhetene. Godkjenningen skal innebære at bestemte vilkår skal imøtekommes, som ved brudd skal føre til sanksjoner. Sanksjoneringen vil avhenge av bruddets karakter. |
| S.2 | Søknads-behandling med vedtaks-kompetanse | Helsedataservice skal behandle søknader om tilgang til data og søknader om endringer på eksisterende prosjekter, samt fatte vedtak om tilgjengeliggjøring av data der Helsedata­service har vedtakskompetanse. Helsedataservice skal også håndtere klager på fattede vedtak. |
| S.3 | Søknads-behandling og -koordinering uten sentralt vedtak | Helsedataservice skal kunne motta og behandle forespørsler der vedtak ikke er nødvendig, samt kunne motta søknader der Helsedataservice ikke har vedtakskompetanse. Videre skal Helsedataservice kunne koordinere behandlingen av disse søknadene med dataleverandør(ene). |
| V | Veiledning | Helsedataservice skal veilede brukere av Helseanalyseplattformen innenfor de ulike tjenesteområdene som Helsedataservice tilbyr |
| V.1 | Dataveiledning | Helsedataservice skal veilede brukerne om helsedata, registervariabler og tilhørende metadataelementer, samt hjelpe brukerne til å finne hensiktsmessige data til sitt bruk |
| V.2 | Søknadsveiledning | Helsedataservice skal veilede brukere av Helseanalyseplattformen i søknadsprosessen. |
| V.3 | Innbygger-veiledning | Helsedataservice skal veilede innbygger om utøvelse av sine rettigheter knyttet til helse- og personopplysninger som finnes på Helseanalyseplattformen. |
| A | Analysestøtte | Helsedataservice tilby analysetjenester som gjør sluttbrukere i stand til å analysere helsedata på en sikker og fleksibel måte. Tjenestene skal leveres gjennom ett økosystem, i tillegg til at Helsedataservice selv skal kunne levere enkelte tjenester. |
| A.1 | Tilgjengeliggjøring av analyse-infrastruktur | Helsedataservice skal tilgjengeliggjøre en teknisk plattform der sluttbrukere kan håndtere og analysere helsedata på en sikker måte. |
| A.2 | Økosystem-forvaltning | Helsedataservice skal forvalte et økosystem for dataprodukter og analysetjenester der ulike leverandører kan levere tjenestene gjennom plattformen. |
| T | Tilgjengeliggjøring av data | Helsedataservice skal tilgjengeliggjøre data som en sluttbruker har fått innvilget tilgang til, samt kunne trekke tilbake tilgang til data når godkjenning av tilgang ikke er gyldig lenger. |
| T.1 | Tilgjengeliggjøring av data fra Helseanalyseplattformen | Helsedataservice skal tilgjengeliggjøre data fra Helseanalyseplattformen, som en sluttbruker har fått innvilget tilgang til, samt kunne trekke tilbake tilgang til data fra Helseanalyseplattformen når godkjenning av tilgang ikke er gyldig lenger. |
| T.2 | Kobling av data fra Helseanalyseplattformen og andre datakilder | Helsedataservice skal kunne koble data som fins på Helseanalyseplattformen med data som leveres av andre dataleverandører. |
| I | Informasjons-forvaltning | Helsedataservice skal forvalte data på Helseanalyseplattformen slik at arbeidet med å veilede om, og tilrettelegge data blir effektivt. |
| I.1 | Metadata-forvaltning | Helsedataservice skal tilby brukerne metadata om helseregistervariabler og ha en koordinerende rolle for harmonisering av metadata på tvers av datakilder |
| I.2 | Datakvalitets-forvaltning | Helsedataservice skal bidra til å bedre datakvaliteten, både for data og for metadata ved å være et primært kontaktpunkt for å innrapportere datakvalitetsproblemer, samt rapportere datakvalitetsproblemer tilbake til datakildene. |
| I.3 | Informasjons-sikkerhet og personvern | Helsedataservice skal sikre data på plattformen mot brudd på konfidensialitet, integritet og tilgjengelighet, samt sikre personvernet |
| I.4 | Dataprodukt-forvaltning | Helsedataservice skal etablere og forvalte dataprodukter, eksempelvis standardiserte datasett, som går på tvers av dagens registre |
| DF | Drift, forvaltning og videreutvikling | HAP FO skal være ansvarlig for drift, forvaltning og videreutvikling av tekniske løsninger som inngår i Helseanalyseplattformen. |
| DF.1 | Hendelses-håndtering | HAP FO skal være ansvarlig for håndtering av hendelser relatert til tekniske løsninger som inngår i Helseanalyseplattformen. |
| DF.2 | Endringshåndtering | HAP FO skal være ansvarlig for håndtering av endringer relatert til tekniske løsninger på Helseanalyseplattformen. |
| DF.3 | Produksjons- og tjenesteoppfølging | HAP FO skal være ansvarlig for produksjon- og tjenesteoppfølging av tekniske løsninger på Helseanalyseplattformen, inkludert forvaltning av avtaler. |
| DF.4 | Informasjons-sikkerhet og personvern | HAP FO skal sikre data på plattformen mot brudd på konfidensialitet, integritet og tilgjengelighet, samt sikre personvernet |
| DF.5 | Arkitektur-forvaltning | HAP FO skal ivareta en helhetlig dataarkitektur, integrasjonsarkitektur og informasjonslivssyklus etter definerte prinsipper, standarder og retningslinjer. Arkitekturen skal sikre at data er søkbare, tilgjengelige, gjenbrukbare og gir mulighet for samhandling/interoperabilitet (FAIR-prinsippene) |

### Prosesser

Innenfor kapabiliteter knyttet til kjerneoppgavene til Helsedataservice, dvs. informasjonsforvaltning, analysestøtte og tilgjengeliggjøring av data, har vi identifisert og skissert ulike prosesser som i nærmere detalj beskriver aktiviteter som må utføres innenfor disse kapabilitetene. Merk at dette ikke nødvendigvis er noen endelig og utfyllende liste.

| Kapabilitet | Prosess | Beskrivelse |
| --- | --- | --- |
| Informasjons-forvaltning | Behandle retteforespørsel | Denne prosessen beskriver hvordan Helsedataservice mottar og behandler en forespørsel fra innbygger om retting av egne data.  Prosessen starter ved at innbygger henvender seg til Helsedataservice via helsenorge.no med en retteforespørsel. Helsedataservice mottar melding og behandler denne ved å vurdere om data må rettes. Dersom data ikke må rettes gis en tilbakemelding til innbygger med eventuell veiledning om hvorfor data er som de er. Dersom data må rettes sender Helsedataservice melding til dataleverandør med forespørsel om å rette data. Dataleverandør mottar forespørsel og vurderer om data må rettes, foretar retting av data dersom det er behov for det og sender tilbakemelding om utfall til Helsedataservice, som så formidler svar tilbake til innbygger. |
| Informasjons-forvaltning | Behandle innbygger-forespørsel om innsyn i bruk av helsedata | Denne prosessen beskriver hvordan en forespørsel fra innbygger om innsyn i brukslogg og utleveringer av egne helsedata håndteres.  Ulike typer av rapporter kan tilbys, for eksempel standardrapport eller komplett, maskinlesbar datadump. Prosessen starter ved at innbygger retter en forespørsel til Helsedataservice via helsenorge.no om innsyn i brukslogg og utleveringer. Helsedataservice mottar forespørsel om innsyn fra innbygger, og henter oversikt over relevante datautleveringer som er gjort fra Helseanalyseplattformen. Videre hentes logg over bruk av innbyggers egne data fra Helseanalyseplattformen og eventuelt fra Dataleverandør (register). Resultatet sammenstilles og utleveres til innbygger. |
| Informasjons-forvaltning | Behandle slette-/reservasjons-forespørsel | Denne prosessen beskriver hvordan Helsedataservice mottar og behandler en forespørsel fra innbygger om reservasjon eller sletting av egne data.  Prosessen starter ved at innbygger sender en forespørsel til Helsedataservice.  Helsedataservice mottar og behandler forespørselen. Dersom innbygger ikke har rett til å bli slettet eller reservere seg for de konkrete data/register som forespørres, gis en tilbakemelding om utfallet til innbygger. Dersom innbygger har rett til reservasjon/sletting sendes henvendelsen til aktuell dataleverandør (register). Dataleverandør mottar og behandler forespørsel fra Helsedataservice om sletting/reservasjon fra innbygger. Dersom dataleverandør vurderer at innbygger ikke har rett sletting/reservasjon sendes en tilbakemelding til Helsedataservice med begrunnelse, som Helsedataservice videreformidler til innbygger. Dersom dataleverandør vurderer at innbygger har rett til sletting/reservasjon i aktuelt register, så utføres nødvendige operasjoner for å reservere/slette innbygger fra register, før tilbakemelding sendes til Helsedataservice som så formidler utfall til innbygger. Dersom data blir slettet i register så skal dette reflekteres i Helseanalyseplattformen ved neste dataoverføring. |
| Informasjons-forvaltning | Behandle innbygger-forespørsel om innsyn i lagret data | Denne prosessen beskriver hvordan en forespørsel fra en innbygger om innsyn i data lagret på Helseanalyseplattformen håndteres.  Det vil gjelde både data i dataplattformen samt i analyserom (inkluder data som for eksempel en forsker innhenter).  Prosessen starter ved at innbygger sender en forespørsel til Helsedataservice om innsyn i lagret data. Helsedataservice mottar og behandler innsynsforespørsel, dersom data som gjelder den aktuelle innbygger er utlevert til analyserom rettes en forespørsel til ansvarlig for analyserom om å komplementere innsynsforespørsel med persondata i analyserom. Dette kan for eksempel være data som en forsker selv har samlet inn som innbygger har rett til innsyn i. Helsedataservice sammenstiller relevante opplysninger fra Helseanalyseplattformen, og utleverer resultatet til innbygger. |
| Analysestøtte | Klargjøre analyserom | Denne prosessen beskriver hvordan Helsedataservice klargjør analyserom der sluttbrukere kan analysere person- og helseopplysninger.  Prosessen initieres enten av sluttbruker selv, eller av Helsedataservice som en del av prosess for tilgjengeliggjøring av data. Første steg i prosessen er å definere ønsket kapasitet og analyseverktøy. Basert på dette blir det opprettet ett prisestimat, som går videre til en bestilling dersom bruker aksepterer prisestimatet. Helsedataservice mottar og verifiserer ordren, og starter prosessen med å opprette analyserom til sluttbruker. Når analyserommet er klart vil Helsedataservice implementere eventuelle faste dataoverføringer, samt sette opp tilgangsstyring. Deretter sendes melding til sluttbruker om at analyserom er klar til bruk. Til slutt oppdateres kunde- og tjenestekatalog med opplysninger om bestillingen. |
| Analysestøtte | Endre eksisterende analyserom | Denne prosessen beskriver hvordan bruker endrer et eksisterende analyserom.  Eksempler på endringer kan være å øke kapasitet for lagring eller prosessering, legge til nye analyseverktøy til analyserommet eller integrere inn nye datakilder inn i analyserommet på fast basis.  Vi ser for oss to ulike scenario i denne prosessen:  1) sluttbruker om "standardendring", dvs. endring i kapasitet eller legge til standardverktøy, i det andre en mer omfattende endring. I det første scenarioet ser vi for oss en mest mulig automatisert prosess fra Helsedataservice sin side, hvor brukeren gjør sine valg, mottar ett prisoverslag, bestiller, hvor på prosesser utfører endringsordren og til slutt oppdaterer kunde og tjenestekatalog iht. endringen  2) tilsvarende forløp som for det første scenarioet, men endringen er av en slik karakter at det ikke er lagt opp til automatiserte prosesser. Her må manuelle prosesser hos Helsedataservice motta og evaluere endringsforespørselen, sette opp ett tilbud som sluttbruker evaluerer og eventuelt bestiller. |
| Analysestøtte | Avslutte bruk av analyserom | Denne prosessen beskriver hva som skjer når sluttbruker velger å avslutte analyserom på Helseanalyseplattformen.  Helsedataservice mottar en melding fra sluttbruker om å avslutte bruk av analyserom. Helsedataservice vil så utføre følgende steg; lagre og arkivere innstillinger på analyserom, arkiverer data dersom sluttbruker har bedt om det, avvikler analyserommet, oppdaterer fakturagrunnlaget, oppdaterer kunde og tjenestekatalog og sender en melding om avsluttet analyserom til sluttbruker. |
| Analysestøtte | Gjenopprette analyserom | Denne prosessen beskriver et tilfelle der sluttbruker tidligere har avsluttet bruk av analyserommet, men ønsker på et senere tidspunkt å få analyserommet gjenskapt slik det var når han avsluttet sist. Helsedataservice mottar forespørsel om gjennomretting fra sluttbruker og utfører så følgende automatiserte steg; hent fram konfigurasjonsoppsett til arkivert analyserom, oppretter analyserom, tilgangsstyrer analyserom, gir beskjed til sluttbruker om at analyserom er klar til bruk, og oppdater kunde og tjenestekatalog. |
| Tilgjengeliggjøre data | Sammenstille og utlevere brukerdefinert datasett | Denne prosessen beskriver hvordan Helsedataservice vil gå frem med å definere, sammenstille og utlevere et brukerdefinert datasett til sluttbruker.  Prosessen starter etter at Helsedataservice har fattet vedtak om utlevering av brukerdefinert datasett til sluttbruker. Helsedataservice identifiserer hvilke data som skal sammenstilles og utleveres, samt hvem som skal trekke utvalget. Utvalget trekkes av enten sluttbruker, dataleverandør (register) eller Helsedataservice. Helsedataservice koordinerer prosessen med å trekke utvalg og sammenstille data fra dataleverandør(er) og Helseanalyseplattformen. Sluttbruker får utlevert til data til ønsket godkjent infrastruktur. Når data er tilgjengeliggjort, informeres sluttbruker, og status på søknad oppdateres og lukkes. |
| Tilgjengeliggjøre data | Utlevere standard datasett | Denne prosessen beskriver hvordan Helsedataservice vil gå frem med å utlevere et standard datasett til sluttbruker.  Datasettet er koblet ferdig på Helseanalyseplattformen, og prosessen vil inkludere automatisk henting av valgte variabler og filtrering av datasett som definert i søknaden. Prosessen starter etter at Helsedataservice har fattet vedtak om utlevering av standard datasett til sluttbruker. Ett standard datasett fra Helseanalyseplattformen blir generert for sluttbruker. Dersom sluttbruker skal kunne koble data med egne data på individnivå, etableres det ett sett med koblingsnøkler. Dersom sluttbruker ønsker data utlevert til ekstern infrastruktur (for eksempel TSD), genereres filer av datasettet, som så overføres til godkjent preferert infrastruktur. Dersom sluttbruker skal ha data tilgjengeliggjort på Helseanalyseplattformen overføres data til sluttbrukers analyserom på Helseanalyseplattformen. Når data er tilgjengeliggjort, informeres sluttbruker, og status på søknad oppdateres og lukkes. |

# Sentrale rammebetingelser

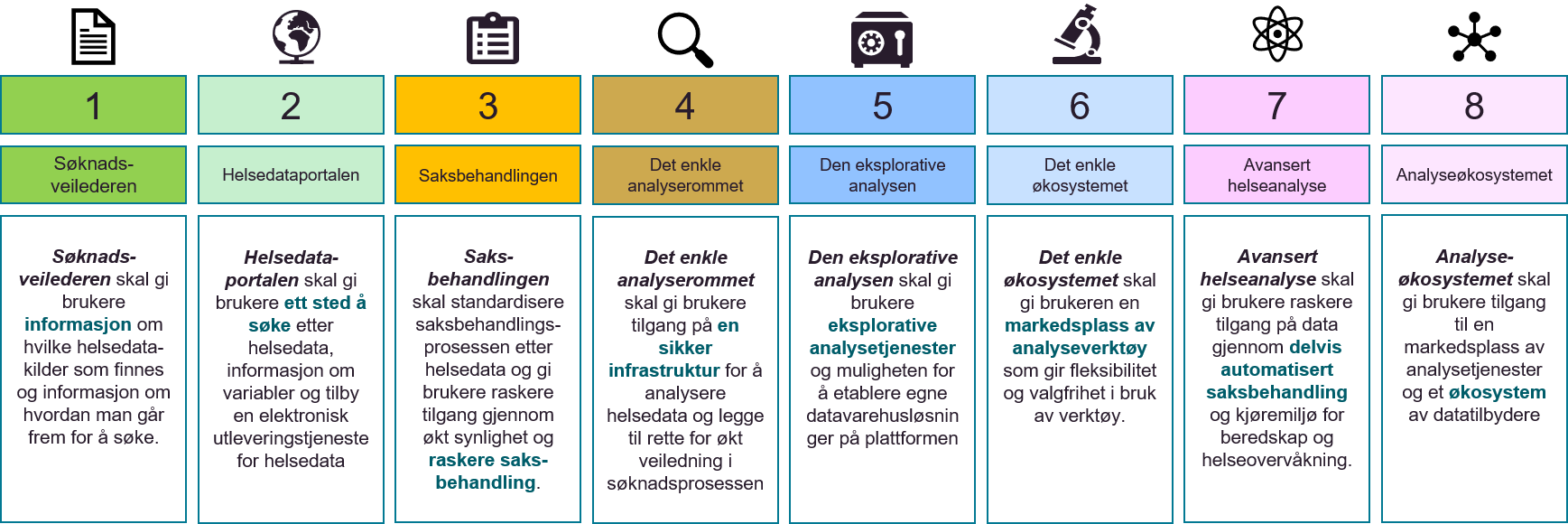
## Rammebetingelser

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

* Behandlingsgrunnlaget for data på Helseanalyseplattformen avhenger av det pågående lovarbeidet i Helse- og omsorgsdepartementet (HOD). Det er antydet fra HOD at nytt regelverk tidligst vil gjelde fra 01.01.2021.  
  Helsedataprogrammet jobber i parallell sammen med dagens registerforvaltere for å identifisere hvilke deler av løsningen det kan være hjemmelsgrunnlag for innenfor dagens regelverk. Høringsnotat om lovhjemmel for etablering av teknisk og organisatorisk løsning for Helseanalyseplattformen vil etter planen komme på ordinær høring før sommeren 2019 med tre måneder høringsfrist. Arbeid med forskrifter vil antagelig påstartes parallelt.
* Integrasjonsarbeid mot datakilder og systemer som eies av andre virksomheter (for eksempel registerforvaltere) avhenger av tett samarbeid i både planlegging og gjennomføring sammen med disse.
* Helsedataprogrammets finansiering er i stor grad basert på årlige tilskudd over statsbudsjettet. Dette vil påvirke realiseringshastighet.
* Helsedataprogrammet vil etter opprinnelig plan gå ut 2020, men det vurderes fortløpende hvorvidt programperioden bør utvides med ett år. En eventuell forlengelse av programperioden besluttes høsten 2019, blant annet basert på anbefalinger fra ekstern kvalitetssikrer etter KS2-arbeidet. En forlengelse av programperioden vil medføre at en del linjefunksjoner og styringsoppgaver fortsatt vil håndteres av programorganisasjonen.
* Det er ikke besluttet hvilken virksomhet som skal være plattformeier for Helseanalyseplattformen på sikt. Dette vil avgjøres av HOD og gjøres som en del av arbeidet med å etablere forskrift for Helseanalyseplattformen. Kontrakten vil inngås med Direktoratet for e-helse, men det vil være nødvendig med mekanismer for å flytte kontrakten.
* Innbyggers portal for å få sine personvernsrettigheter oppfylt vil være helsenorge.no.

# Kundens overordnede plan for implementering

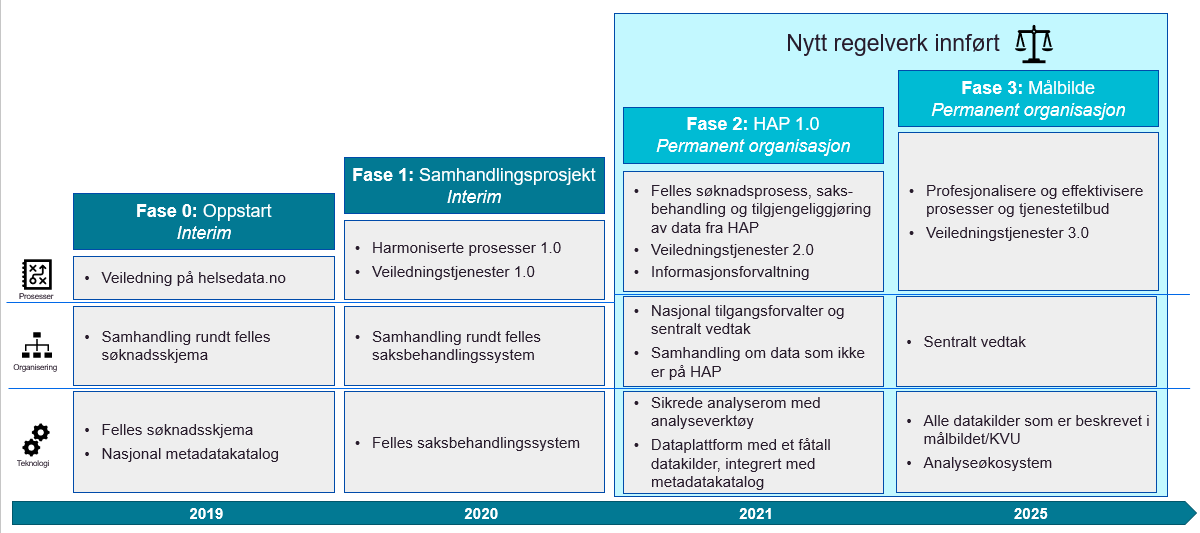
## Stegvis etablering av Helseanalyseplattformen

Figur 5 illustrerer overordnet den anbefalte stegvise etableringen av Helseanalyseplattformen som kunden bruker som overordnet veikart på utvikling av konseptet for analyseøkosystem. 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 kunne levere analysetjenester og -verktøy knyttet til økosystemet. 

Figur 5: Illustrasjon av stegvis utvikling av Helseanalyseplattformen

## Stegvis etablering av Helsedataservice

Helsedataservices forretningsarkitektur vil realiseres stegvis i takt med den teknologiske utviklingen av Helseanalyseplattformen, samt regelverksutviklingen som drives av Helse- og omsorgsdepartementet (HOD). Denne utviklingen er beskrevet gjennom fire steg og illustrert i Figur 6.



Figur 6: 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 for helsedata utvides med metadata fra flere helseregistre, og arbeidet med å harmonisere variabler kan begynne.

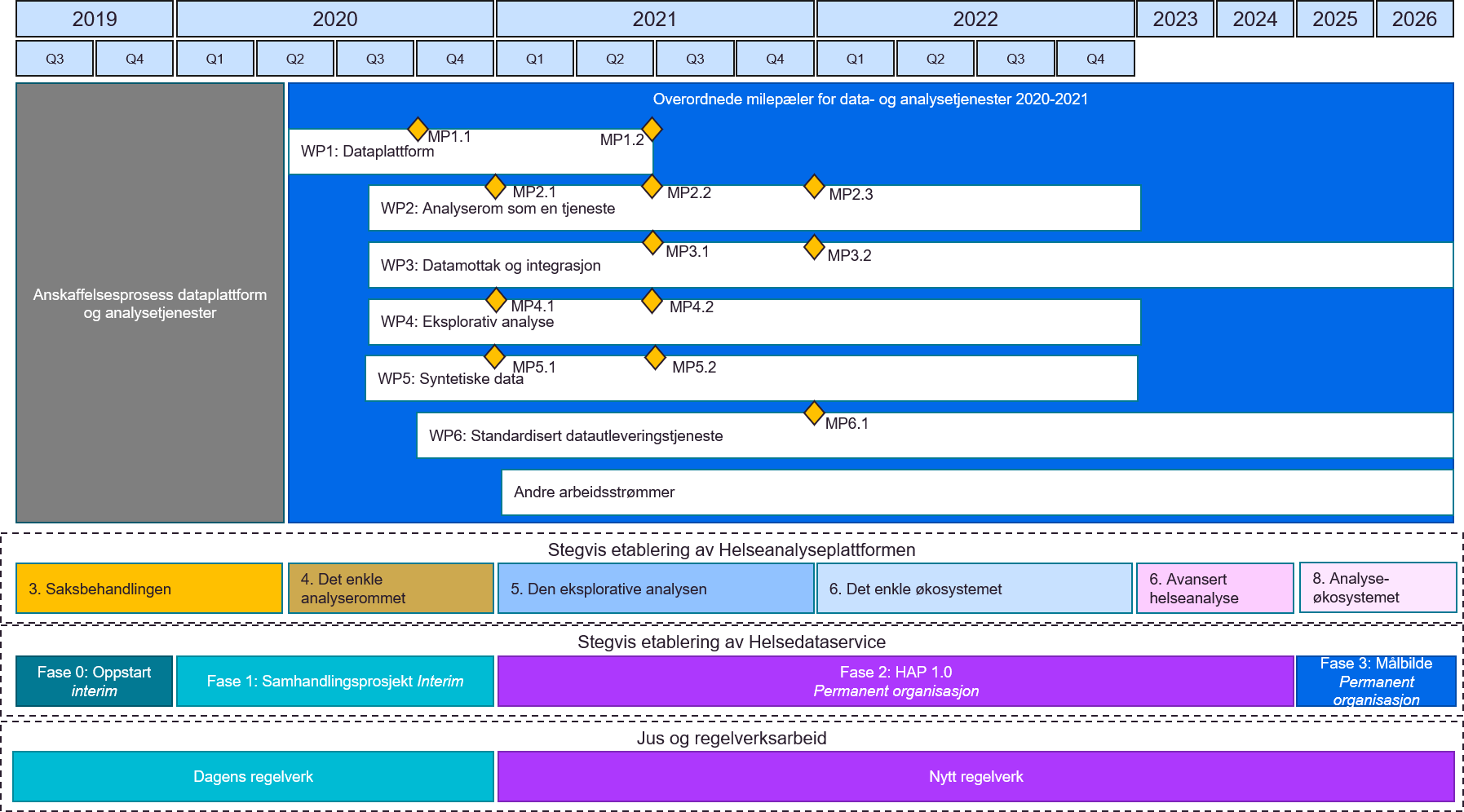
**Helsedataservice fase 2, "HAP 1.0 permanent organisasjon",** starter når et nytt regelverk innføres. Dette vil etter planen medføre at Helsedataservice får hjemmel for å etablere en dataplattform med helseregisterdata, samt vedtaksmyndighet for tilgjengeliggjøring av data. Fra og med denne fasen vil 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 Helseanalyseplattformen slik at behovet for samhandling om data som ikke er på Helseanalyseplattformen, 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.

## Arbeidsstrømmer og milepæler

Figur 7 illustrerer sammenhengen mellom programmets stegvise realiseringsstrategi av hhv Helseanalyseplattformen (kapittel 4.1) og Helsedataservice (kapittel 4.2) opp imot rammebetingelsen rundt regelverksutvikling, samt forslag til arbeidsstrømmer knyttet til denne anskaffelsen som skal realisere løsninger og tjenester på Helseanalyseplattformen.



Figur 7: Kundens overordnede forslag til milepæler og arbeidsstrømmer for anskaffelsen

Vi foreslår at arbeidet organiseres i følgende seks arbeidsstrømmer som alle bør starte i 2020.

* WP1: Dataplattform
* WP2: Analyserom som en tjeneste
* WP3: Datamottak og integrasjon
* WP4: Eksplorativ analyse
* WP5: Syntetiske data
* WP6: Standardisert datautleveringstjeneste

Hvis Leverandøren må gjerne foreslå annen nedbrytningsstruktur hvis det er mer hensiktsmessig.

### Arbeidsstrømmer

Tabell 1 beskriver Kundens forslag til arbeidsstrømmer for implementering av data- og analysetjenester.

Tabell 1: Forslag til arbeidsstrømmer for data- og analysetjenester

| Arbeidsstrømmer | Beskrivelse |
| --- | --- |
| WP1: Dataplattform | Etablering av den sentrale infrastrukturen som gjør det mulig å lagre og forvalte helsedata på en sikker måte, samt å etablere utviklingsplattform for at prosjektet skal kunne etablere digitale tjenester til sluttbrukere. Infrastrukturen må knyttes til helsenettet. |
| WP2: Analyserom som en tjeneste | Etablere tekniske løsning som gjør Helsedataservice i stand til å kunne tilby analyserom som en tjeneste til sluttbrukere.  På sikt vil det tilbys ulike typer analyserom med ulike kapabiliteter til de ulike aktørgruppene. |
| WP3: Datamottak og integrasjon | Knytte data fra helseregistre og andre datakilder til plattformen.  I første omgang er planen å knytte data fra følgende registre til Helseanalyseplattformen:   * Grunndata (Folkeregisteret) * DÅR * NPR * KPR * MFR * DÅR * Kreftregisteret |
| WP4: Eksplorativ analyse | Etablere en eksplorativ analysetjeneste. I første omgang vil dette gjøres gjennom å etablere 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 som utledes av kohortutforskeren og vises til forsker skal være anonymt og ikke inneholde direkte eller identifiserbare helse- og personopplysninger. |
| WP5: Syntetiske data | 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: Standardisert datautleveringstjeneste | Etablere standardiserte datasett som går på tvers av registre og legge opp til en søknadsprosess som i stor grad er automatisert (i større grad basert på avvikshåndtering enn tradisjonell saksbehandling). |

### Milepæler for 2020 og 2021

Tabellen under beskriver Kundens mål for milepæler. Måldatoer for milepælene er tentative og vil detaljeres nærmere i samarbeid mellom Kunden, Leverandøren og andre aktører i sektoren.

Tabell 2: Milepæler knyttet opp imot arbeidsstrømmer

| Arbeids-strømmer | Milepæler | Godkjenningskriterium | Måldato |
| --- | --- | --- | --- |
| WP1: Data-plattform | MP1.1: Dataplattform og utviklingsmiljø etablert | Godkjenningskriteriet for denne milepælen er at den grunnleggende infrastrukturen med dataplattformen og utviklingsmiljøet er etablert og testet. | 30.10.20 |
| MP1.2: Dataøkosystem etablert | Godkjenningskriteriet for denne milepælen er at den grunnleggende infrastrukturen for å legge til rette for et dataøkosystem er etablert | 30.06.21 |
| WP2: Analyse-rom som en tjeneste | MP2.1: Det enkle analyserommet etablert | Godkjenningskriteriet for denne milepælen er at Helsedataservice kan tilby analyserom som en tjeneste ut mot sluttbrukere. | 31.12.20 |
| MP2.2: Eksterne analyseinfrastrukturer integrert med dataplattformen | Godkjenningskriteriet for denne milepælen er at Helsedataservice i etterkant av godkjent vedtak kan tilgjengeliggjøre data til definerte eksterne analyseinfrastrukturer som et alternativ til å tilgjengeliggjøre data til analyserom som er helintegrert på Helseanalyseplattformen | 30.06.21 |
| MP2.3: Det avanserte analyserommet etablert | Godkjenningskriteriet for denne milepælen er at Helsedataservice kan tilby en avansert versjon av analyserom som en tjeneste ut mot sluttbrukere. | 31.12.21 |
| WP3: Data-mottak og integrasjon | MP3.1: Datakopier fra utvalg registre etablert på dataplattformen | Godkjenningskriteriet for denne milepælen er at datakopier/dataprodukter fra Folkeregisteret, NPR, KPR, DÅR, MFR og Kreftregisteret er etablert på plattformen, kan saksbehandles og tilgjengeliggjøres fra Helsedataservice. | 30.06.21 |
| MP3.2: Datakopier fra utvalg registre etablert på dataplattformen #2 | *Ikke bestemt. Vil detaljeres på et senere tidspunkt* | 31.12.21 |
| WP4: Eksplorativ analyse | MP4.1: Kohortutforsker etablert | Godkjenningskriteriet for denne milepælen er en produksjonsklar løsning av en kohortutforsker på et begrenset sett med variabler. I utvikling av første versjon av kohortutforskeren kan det forutsettes at løsningen etableres på fryste datasett. | 31.12.20 |
| MP4.2: Eksplorativ analysetjeneste etablert | Godkjenningskriteriet for denne milepælen er en utvidet løsning av kohortutforskeren som inkluderer ytterligere variabler, nye analyser og en løsning der datagrunnlaget oppdateres jevnlig. | 30.06.21 |
| WP5: Syntetiske data | MP5.1: Pilot av syntetiske data tilgjengelig på helsedata.no | Godkjenningskriteriet for denne milepælen er at syntetiske data for variabler fra ett helseregister er publisert på helsedata.no. Det kan forutsettes at arbeidet vil gjøres i tett samarbeid med eksisterende registerforvalter. | 31.12.20 |
| MP5.2: Syntetiske data etablert | Godkjenningskriteriet for denne milepælen er at syntetiske data som går på tvers av flere helseregistre er publisert på helsedata.no | 30.06.21 |
| WP6: Standardisert data-utleverings-tjeneste | MP6.1: Standardisert data-utleveringstjeneste etablert | Godkjenningskriteriet for denne milepælen er at man har etablert standardiserte dataprodukter som går på tvers av flere helseregistre, selvbetjente løsninger for å gjøre utvalg i dataproduktene og har etablert (automatiserte) prosesser for å håndtere saksbehandlingen. Denne leveransen har en tett avhengighet med leveransene knyttet til søknad og saksbehandling og må derfor detaljeres i samarbeid på et senere tidspunkt | 31.12.21 |

# Funksjonelle krav

Dette kapittelet beskriver kundens funksjonelle krav og behov knyttet til data- og analyseplattformen. De funksjonelle kravene er kategorisert innenfor følgende gruppering: «Dataplattform med innebygget personvern», «Data- og analysetjenester» og «Innbyggertjenester» som illustrert i Figur 1: Overordnet illustrasjon av Helseanalyseplattformens målbilde.

De funksjonelle kravene er beskrevet som brukerhistorier. Dette er gjort fordi det er ønskelig å oppnå en best mulig løsning gjennom å gi leverandørene størst mulig spillerom i design av løsning.

Fase 1 handler om etableringen av den funksjonelle grunnmuren som vil gjøre det mulig å starte utviklingen av data- og analysetjenester. De funksjonelle kravene for denne delen av løsningen er beskrevet i kapittel 5.1.

Når det gjelder de funksjonelle kravene for data- og analysetjenester så er disse beskrevet i kapittel 5.2. Prioritering og ytterligere detaljering av disse EPOSene og brukerhistoriene vil gjøres som en del av en smidig utviklingsprosess.

Kvalitetskravene som beskrevet i kapittel 7 gjelder for hele løsningen.

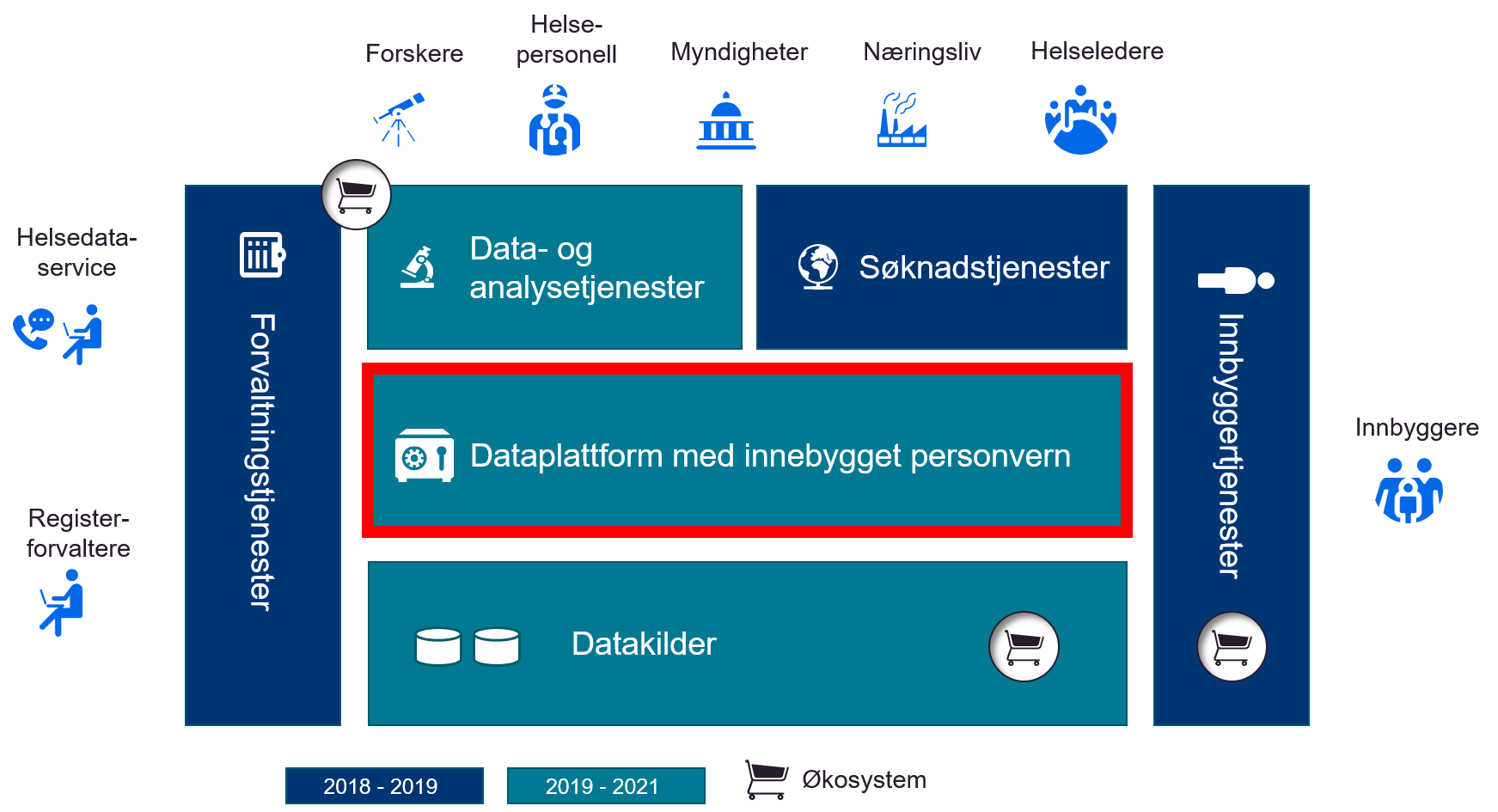
## Fase 1

|  |
| --- |
| Tittel: Dataplattform og utviklingsmiljø |
| **EPOS**  Som Helsedataservice ønsker jeg å etablere en dataplattform og et utviklingsmiljø slik at jeg kan hente inn data og bygge data- og analysetjenester. |
| **Beskrivelse**  Når fase 1 er gjennomført, ønsker Kunden å være i stand til følgende   1. Ha en teknisk infrastruktur som gjør det mulig å integrere mot datakilder på helsenettet, motta og håndtere personopplysninger 2. Ha et utviklingsmiljø (internt analyserom) som prosjektet vil bruke for å utvikle nye data- og analysetjenester, som eksplorativ analyse.   Fra et funksjonelt ståsted må, som et minimum, følgende kapabiliteter og integrasjoner være etablert:  *Kapabiliteter*   * Funksjonalitet for å kunne innhente informasjon fra helseregistre gjennom filoverføring * Funksjonalitet for å håndtere ulike krypteringsmekanismer og -løsninger ifm integrasjon * Funksjonalitet for å kunne lagre og håndtere data * Funksjonalitet for tilgangsstyring og initielt oppsett en rollebasert modell for tilgangsstyring * Legge til rette for funksjonalitet som gjør det mulig å etterleve innbyggers rettigheter ettersom man tar inn nye datakilder på plattformen * Utviklingsmiljø for å kunne etablere data- og analysetjenester som eksplorativ analyse   *Integrasjoner*   * Integrasjon mot Helsenettet * Integrasjon mot HelseID * Integrasjon mot personvernkomponenten på helsenorge.no * Integrasjon mot innsynsløsning på helsenorge.no |
| **Akseptansekriterier**  *<Leverandøren bes foreslå akseptansekriterier for fase 1>* |

## Funksjonelle krav for data- og analysetjenester

Målbildet for Helseanalyseplattformen er beskrevet i kapittel 2. Brukerhistoriene som beskrevet under er ikke en komplett liste brukerhistorier, men er ment å gi Leverandøren en best mulig forståelse for hva som ligger innenfor hvert EPOS.

### Dataplattform med innebygget personvern



For at Helsedataservice og andre leverandører i et økosystem skal kunne levere et godt tilbud av data- og analysetjenester vil etableringen av en dataplattform med innebygget personvern stå sentralt. Dataplattformen vil være den tekniske løsningen der Helsedataservice er dataansvarlig og løsningen vil brukes for å tilgjengeliggjøre data på en sikker og effektiv måte til godkjente formål. Dataplattformen vil også stå sentralt i etableringen av et dataøkosystem – her vil Helsedataservice kunne ta rollen som databehandler for dataprodukter som tredjeparts dataleverandører velger å tilgjengeliggjøre gjennom Helseanalyseplattformen. Dataplattformens krav er beskrevet gjennom følgende fire EPOS:

* Tilgjengeliggjøring av data
* Forvaltning av data (inkludert etterleve innbyggers rettigheter)
* Integrasjon og mottak av data
* Dataøkosystem

#### Tilgjengeliggjøring av data

|  |
| --- |
| Tittel: Tilgjengeliggjøring av data |
| **EPOS**  Som Helsedataservice ønsker jeg funksjonalitet for å tilgjengeliggjøre helsedata fra forskjellige dataleverandører på en sikker og effektiv måte, slik at både personvernet og sluttbrukernes behov for rask tilgang til helsedata ivaretas. |
| **Beskrivelse**  Helsedataservice skal tilgjengeliggjøre data fra Helseanalyseplattformens dataplattform som en bruker av data har fått innvilget tilgang til via søknad eller gjennom annet hjemmelsgrunnlag.  Helsedataservice bør ha mulighet for å tilgjengeliggjøre og tilgangsstyre data på ulike måter og til ulike plattformer:   * Tilgjengeliggjøring av relevante data til innbygger til helsenorge.no * Tilgjengeliggjøring til andre nasjonale og internasjonale forhåndsgodkjente, sikre analyseinfrastrukturer, slik som Tjenester for Sensitive Data (TSD) fra Universitetet i Oslo, eller NTNU sin HUNT Cloud. Det bør legges opp til en mest mulig automatisert utleveringsprosess for analyseinfrastrukturer som er mye brukt * Tilgjengeliggjøring til sluttbrukers eget analyserom på Helseanalyseplattformen * Direkte utleveringer til sluttbrukers egen infrastruktur, for eksempel vha. filoverføringer * Tilgjengeliggjøring av data gjennom API‑er * Tilgjengeliggjøring av data til eksplorative analysetjenester   Alle brukerhistoriene knyttet til tilgjengeliggjøring av data er tett knyttet til anskaffelsen om søknads- og saksbehandlingstjenester og prosesser som etableres for søknadshåndtering.  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. * **Bruker av data** – Denne aktøren er en samlebetegnelse på sluttbrukere som analyserer helsedata for å skape ny kunnskap eller innsikt. For eksempel forskere, myndighetsaktører eller helseledere * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. |
| **Brukerhistorier**   1. Som forsker ønsker jeg å få data tilgjengeliggjort direkte til eksterne nasjonale og internasjonale analyseinfrastrukturer, slik at jeg kan benytte disse i min forskning 2. Som forsker ønsker jeg mulighet for å få data ulevert direkte til meg, slik at jeg kan benytte egen infrastruktur til å analysere data 3. Som bruker av data ønsker jeg mulighet til å motta løpende oppdaterte data, slik at data jeg benytter i min analyse er mest mulig oppdatert 4. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data fra dataplattformen til ulike analyserom basert på godkjent bruk på en rask og sikker måte, slik at bruker av data får rask tilgang til data 5. Som Helsedataservice ønsker jeg å kunne trekke tilbake tilgang til data, slik at jeg kan sikre at sluttbrukere som ikke lenger har gyldig tilgang ikke får tilgang til data 6. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre åpne data på helsedata.no, slik at disse blir tilgjengelig for flest mulig. 7. Som Helsedataservice ønsker jeg å kunne tilgjengeliggjøre data for eksplorativ analyse slik at sluttbrukere kan analysere helsedata uten å måtte søke om data. 8. Som Helsedataservice ønsker jeg å tilby en tjeneste for nøkkelforvaltning av unike koblingsnøkler for prosjekter, slik at det skal bli enklere for bruker av data å koble data fra flere dataleverandører på en måte som fremmer personvernet. 9. 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 data på dataplattformen. 10. Som Helsedataservice ønsker jeg å tilgangsstyre tilgjengeliggjøring av data 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 11. Som Helsedataservice ønsker jeg fullstendig oversikt over alle tilgjengeliggjøringer av data, slik at jeg oppfyller mine plikter som dataansvarlig og kan etterprøve at tilgjengeliggjøringen er i samsvar med personvernregelverket |

#### Forvaltning av data

|  |
| --- |
| Tittel: Forvaltning av data |
| **EPOS**  Som Helsedataservice ønsker jeg å forvalte helsedata på en sikker og enkel måte, slik at både personvernet og sluttbrukernes legitime behov for rask tilgang til helsedata ivaretas. |
| **Beskrivelse**  Helsedataservice skal forvalte data som ligger på Helseanalyseplattformens dataplattform. Dette innebærer blant annet å ha oversikt over hvilke data som håndteres, hva dataene betyr, hva de brukes til, hvilke prosesser de inngår i og hvem som kan bruke den.[[3]](#footnote-4)  For at Helseanalyseplattformen skal ha den nødvendige tillitten både hos bruker av data og hos den registrerte (innbygger) er det avgjørende at både informasjonssikkerhet og grunnleggende personvernrettigheter ivaretas. Innbyggerne har flere rettigheter knyttet til behandling av deres egne helse- og personopplysninger og dataplattformen må tilrettelegge for at de blir ivaretatt.  Innbygger har et krav på innsyn i opplysninger om seg selv for å ha kontroll over egne opplysninger. Dataplattformen må derfor tilrettelegge for funksjonalitet rundt innsynretten og retten til dataportabilitet. Videre må det være mulig for innbygger å få en oversikt over hvilke samtykker og reservasjoner de har gitt i ulike sammenhenger knyttet til data som ligger på dataplattformen.  Dataplattformen må også tilrettelegge for at opplysninger om innbygger kan rettes og slettes, samt at behandlingen av opplysningene opphører dersom innbygger krever det, gjennom deres rettighet til protest og begrensning.  Helsenorge.no er innbyggers inngang til egne helseopplysninger og helsedata. Innbyggers innsynsmuligheter og muligheter for å ivareta sine rettigheter skal skje gjennom helsenorge.no. Dataplattformen må derfor kunne integreres mot Helsenorge.  *Detaljerte brukerhistorier knyttet til innbyggers rettigheter sett fra innbyggers ståsted er beskrevet i kapittel 5.2.3.1*  Som en del av forvaltningen av dataplattformen vil også Helsedataservice etablere og forvalte ferdig koblede, standardiserte dataprodukter basert på eksisterende registerdata.   * **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. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. |
| **Brukerhistorier**   1. Som Helsedataservice ønsker jeg å kunne forvalte standardiserte, ferdigkoblede dataprodukter, slik at jeg kan tilgjengeliggjøre disse til sluttbruker på en rask og sikker måte. 2. Som Helsedataservice ønsker jeg tilgang til en instans av dataleverandørs forvaltningsrom (se kapittel 5.2.2.3) slik at jeg kan etablere og forvalte standardiserte dataprodukter. 3. Som Helsedataservice ønsker jeg mekanismer for å kunne rette og korrigere personopplysninger som er uriktige, før de tilgjengeliggjøres til bruker, slik at jeg ivaretar den registrertes rettigheter 4. Som Helsedataservice ønsker jeg mekanismer for å kunne slette personopplysninger som er feil eller ulovlig, slik at jeg ivaretar den registrertes rettigheter 5. Som Helsedataservice ønsker jeg å kunne motta og behandle forespørsler om innsyn, retting og sletting av data for de tilfeller jeg håndterer personopplysninger, slik at jeg kan oppfylle mine plikter som dataansvarlig eller som databehandler på vegne av dataansvarlig 6. Som Helsedataservice ønsker jeg å kunne motta og behandle forespørsler om begrensning, protest og dataportabilitet, slik at jeg kan oppfylle mine plikter som dataansvarlig 7. Som Helsedataservice ønsker jeg å underrette mottaker som har fått utlevert personopplysninger som er rettet, slettet eller begrenset, slik at jeg kan oppfylle mine plikter som dataansvarlig 8. Som Helsedataservice ønsker jeg å motta varsel om ulovlig behandling av personopplysninger og mekanismer for midlertidig stans av videre behandling, slik at jeg kan behandle personopplysninger i samsvar med personvernregelverket. |

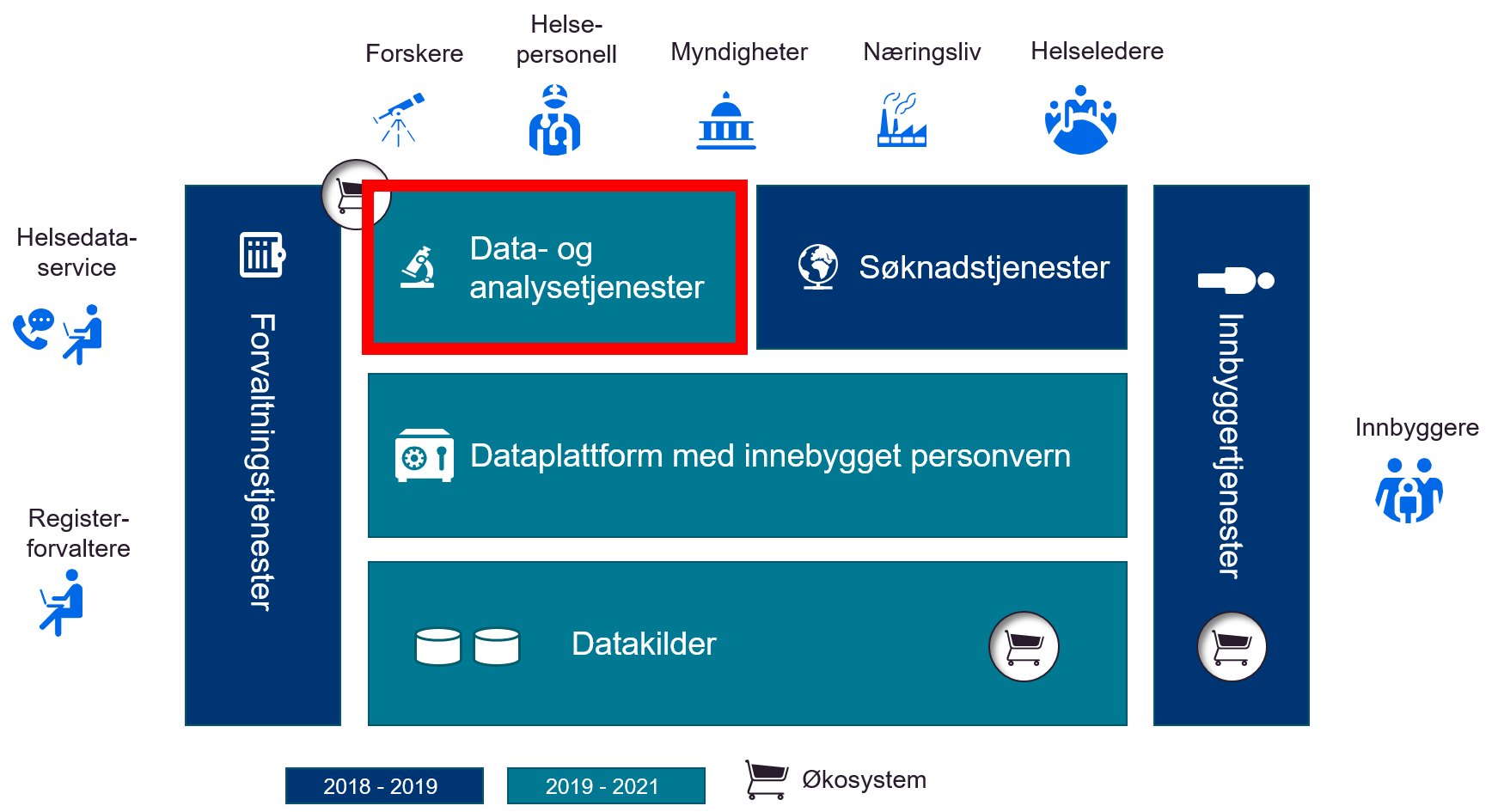
#### Integrasjon og mottak av data

|  |
| --- |
| Tittel: Integrasjon og mottak av data |
| **EPOS**  Som Helsedataservice ønsker jeg fleksible og sikre mekanismer for å innhente data til Helseanalyseplattformen, slik at jeg kan gi et godt tjenestetilbud av datatjenester ut til sluttbrukere. |
| **Beskrivelse**  En sentral del av dataplattformen er innhenting av data fra helseregistre og andre datakilder slik at dataprodukter fra mange ulike kilder kan tilgjengeliggjøres gjennom Helseanalyseplattformen. I dette ligger også integrasjon mot ulike datakilder. Tabell 4 i kapittel 6.2.2 beskriver på et overordnet nivå datakildene som potensielt inngår.   * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. |
| **Brukerhistorier**   1. Som Helsedataservice ønsker jeg å kunne motta data fra aktører med ulike dataformater, standarder, frekvenser, volum og grensesnitt slik at datatilbudet gjennom plattformen blir best mulig. 2. Som Helsedataservice ønsker jeg gode mekanismer for å validere data ved mottak, slik at jeg har gode prosesser for feilhåndtering. 3. Som Helsedataservice ønsker jeg å kunne opprette og tilgjengeliggjøre unike krypteringsnøkler og sertifikater til ulike dataleverandører, slik at jeg sikrer konfidensialiteten i dataoverføringer på tvers av ulike dataleverandører. |

#### Dataøkosystem

|  |
| --- |
| Tittel: Dataøkosystem |
| **EPOS**  Som dataleverandør ønsker jeg å kunne tilgjengeliggjøre kvalitetssikrede dataprodukter gjennom Helseanalyseplattformen på en sikker måte slik at de kan gjenbrukes av andre aktører. |
| **Beskrivelse**  Det er et mål om å etablere et økosystem av dataleverandører slik at dataprodukter fra mange ulike virksomheter og kunnskapsområder innenfor helsesektoren kan tilgjengeliggjøres gjennom Helseanalyseplattformen. Et dataprodukt er i sin enkleste form et datasett som personer eier, kurerer, og tilgjengeliggjør slik at det kan benyttes av andre.  Ved å benytte Helseanalyseplattformen som en plattform for å publisere og tilgjengeliggjøre disse dataproduktene vil det kunne føre til økt gjenbruk av dataene og gjøre det enklere for sluttbrukere å finne gode datasett for sine problemstillinger. Etableringen av Helsedataservice vil også gjøre det mulig for dataleverandører å bruke Helsedataservice som en tilgangsforvalter for dataproduktet.  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, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. * **Dataleverandør** – Denne aktøren eier, kurerer og tilgjengeliggjør et dataprodukt. |
| **Brukerhistorier**   1. Som forsker ønsker jeg en god oversikt over åpne data, grensesnitt og statistikker, slik at jeg raskt kan finne frem til eksisterende kunnskap og relevante data. 2. Som dataleverandør ønsker jeg å kunne publisere mitt dataprodukt på Helseanalyseplattformen, slik at dataene kan gjenbrukes 3. Som dataleverandør ønsker jeg å kunne knytte metadata om variabler til mitt dataprodukt, slik at det er enkelt å kunne finne relevante data 4. Som dataleverandør ønsker jeg å kunne tilgangsstyre mitt dataprodukt, slik at jeg kan sikre at det bare kan brukes av aktører som har lov til å bruke det 5. Som dataleverandør ønsker jeg å kunne knytte en datalisens til mitt dataprodukt, slik at jeg kan sikre at bruken er riktig. 6. Som dataleverandør ønsker jeg å kunne benytte Helsedataservice som en tilgangsforvalter slik at jeg ikke selv trenger å gjøre tilgangsstyring av dataproduktet mot nye brukere. |

### Data- og analysetjenester



Data- og analysetjenester er ulike former for tjenester som gjennom Helseanalyseplattformen tilbys ut til sluttbrukere, som kan være forskere, helsepersonell, myndigheter, næringsliv eller helseledere.

#### Analyserom

|  |
| --- |
| Tittel: Analyserom |
| **EPOS**  Som bruker av data ønsker jeg tilgang til en sikker og skalerbar data- og analyseinfrastruktur slik at jeg kan analysere helsedata på en hensiktsmessig og effektiv 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 Helseanalyseplattformen. 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** – Denne aktøren er en samlebetegnelse på sluttbrukere som analyserer helsedata for å skape ny kunnskap eller innsikt. For eksempel forskere, myndighetsaktører eller helseledere * **Forsker** – Denne aktøren er en samlebetegnelse for personer involvert i et forskningsprosjekt. Kan være forskere som jobber både i privat og offentlig sektor. * **Dataansvarlig for analyserommet** – Denne aktøren har det formelle dataansvaret for data som ligger i analyserommet. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. * **Leverandør av analysetjenester til økosystemet** – Denne aktøren tilbyr analysetjenester og -verktøy på gjennom analyseøkosystemet på Helseanalyseplattformen |
| **Brukerhistorier**   1. ***Opprette og administrere analyserom***    1. 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 på helsedata    2. Som bruker av analyserom ønsker jeg gode grensesnitt for å kunne endre kapasitet i et eksisterende analyserom slik at jeg er kan reagere på endringer i behov    3. Som bruker av analyserom ønsker jeg enkelt å kunne avslutte bruken av analyserom slik at kostnader ikke løper utover den perioden jeg trenger    4. Som bruker av analyserom ønsker jeg en totaloversikt over medgåtte kostnader knyttet til mine analyserom, slik at jeg kan drive effektiv kostnadskontroll    5. Som dataansvarlig for analyserommet ønsker jeg å kunne håndtere tilgangsstyring av analyserommet på en enkel måte slik at jeg til enhver tid har kontroll på hvem som har tilgang til data    6. 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.    7. Som dataansvarlig for analyserommet ønsker jeg å kunne se hvilke behandlingsaktiviteter som er gjort i analyserommet, slik at jeg kan etterprøve at bruken er i samsvar med personvernregelverket, herunder at bruken er lovlig, i tråd med formålet og at det ikke behandles flere opplysninger enn det som er nødvendig og relevant    8. Som dataansvarlig for analyserommet ønsker jeg mekanismer for å kunne rette og korrigere personopplysninger som er uriktige, slik at jeg ivaretar den registrertes rettigheter    9. Som dataansvarlig for analyserommet ønsker jeg å sikre at data etter endt prosjekt slettes i samsvar med relevant regelverk, slik at jeg oppfyller mine plikter    10. Som dataansvarlig for analyserommet ønsker jeg å kunne motta ~~og administrere~~ forespørsler om innsyn, retting og sletting av data for de tilfeller jeg håndterer personopplysninger, slik at jeg kan oppfylle mine plikter som dataansvarlig.    11. Som dataansvarlig for analyserommet ønsker jeg å kunne motta ~~og administrere~~ forespørsler om begrensning, protest og dataportabilitet, slik at jeg kan oppfylle mine plikter som dataansvarlig    12. Som dataansvarlig for analyserommet ønsker jeg å motta varsel om ulovlig behandling av personopplysninger og mekanismer for midlertidig stans av videre behandling, slik at jeg kan behandle personopplysninger i samsvar med personvernregelverket.    13. Som bruker av data- og analysetjenester 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. 2. ***Importere og tilgjengeliggjøre data inn i analyserom***    1. Som bruker av analyserom må jeg kunne ta med egne data inn i analyserommet, slik at jeg kan analysere disse på en sikker måte    2. Som forsker ønsker jeg å kunne innhente ytterligere opplysninger fra innbyggere direkte inn til mitt analyserom slik at jeg sikrer at disse dataene kan behandles på en sikker måte 3. ***Analysere og behandle data***    1. Som bruker av analyserom må jeg kunne lagre person- og helseopplysninger i analyserommet på en sikker måte, slik at jeg sikrer at data jeg er ansvarlig for ikke kommer på avveie    2. Som bruker av analyserom ønsker jeg tilgang til et bredt utvalg med analyseverktøy i analyserommet slik at jeg kan analysere helsedata med de verktøyene som er riktig for meg    3. Som bruker av analyserom ønsker jeg muligheten for å ta med egne verktøy, analysepakker eller containere inn i mitt analyserom slik at jeg har full fleksibilitet i hvilke verktøy jeg bruker    4. Som bruker av analyserom ønsker jeg å kunne bygge og operasjonalisere algoritmer slik at de kan gi ny kunnskap og innsikt på usette data    5. Som bruker av analyserom ønsker jeg gode visualiseringsverktøy slik at jeg kan presentere data på en forståelig måte for mine sluttbrukere    6. Som bruker av analyserom ønsker jeg verktøy for å kvalitetssikre, koble og transformere data fra ulike kilder slik at datagrunnlaget mitt blir riktig    7. Som bruker av analyserom 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    8. Som bruker av analyserom ønsker jeg å kunne aksessere analyserom fra lokasjoner, slik at jeg har fleksibilitet rundt hvor jeg jobber fra. 4. ***Eksportere data ut fra analyserom***    1. Som bruker av analyserom må jeg kunne hente ut resultater av analyser, slik at jeg kan dele resultatene med andre uten at personopplysninger kommer på avveie    2. Som dataansvarlig for analyserommet ønsker jeg gode mekanismer for å sikre hvilke data som forlater analyserommet, slik at jeg etterlever mitt ansvar som dataansvarlig    3. Som forsker må jeg kunne arkivere data fra analyserommet på sikker måte slik at resultatene fra forskningen er etterprøvbare 5. ***Publisere innsikt til brukerflater***    1. Som bruker av analyserom ønsker jeg en enkel måte å tilgjengeliggjøre resultater gjennom rapporter og statistikk, slik at kunnskapen kommer til de som trenger det i tide    2. Som bruker av analyserom ønsker jeg en sikker og god måte å tilgangsstyre resultater på slik at jeg kan sikre at ingen som ikke skal ha tilgang får tilgang    3. Som bruker av analyserom ønsker jeg å kunne tilgjengeliggjøre data til fagsystemer slik at mine sluttbrukere kan konsumere kunnskapen på en enkel måte 6. ***Plattformeiers administrasjon av analyserom***    1. Som Helsedataservice ønsker jeg å kunne automatisk provisjonere opp nye analyserom basert på bestilling, slik at forvaltningskostnadene mine er lave    2. Som Helsedataservice ønsker jeg oppdatert faktureringsgrunnlag av analyserommene slik at jeg kan fakturere sluttbrukere på en riktig måte 7. ***Økosystem av analyseverktøy***    1. Som Helsedataservice ønsker jeg å gjøre det mulig for leverandører av analyseverktøy å levere tjenester gjennom plattformen slik at brukere får størst grad av fleksibilitet og et bredest mulig tilbud    2. Som Helsedataservice ønsker jeg å gjøre det enkelt for leverandører av analysetjenester å etablere seg som leverandør på plattformen slik at prosessen er mest mulig smidig    3. 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: Brukerflater |
| **EPOS**  Som sluttbruker ønsker jeg å få presentert analyseresultater som er tilpasset mitt behov, slik at jeg enkelt kan bruke helsedata som støtte i mitt arbeid. |
| **Beskrivelse**  Mange aktører har behov for å se resultatene som kommer av at det gjøres analyser på helsedata. Fra et funksjonelt ståsted har disse aktørene har delvis overlappende behov. En forskjell er knyttet til hvilke data som brukes i analysen og i hvilke kanaler resultatet blir presentert. Eksempelvis vil helsepersonell som oftest ønske at resultater blir presentert gjennom fagsystemene, mens myndighetsaktører vil benytte andre brukerflater.  Under følger noen eksempler på type bruk for ulike aktører:   * Myndighetsaktører har behov for tilgang til nøkkelindikatorer for å kunne følge opp kvaliteten i helsetjenesten. * Helsepersonell har behov for å bruke helsedata til beslutningstøtte i behandling og for eget kvalitetsarbeid. * Helseledere har behov for enkle måter å konsumere data slik at data kan brukes for kvalitetsforbedring, styring og som beslutningsstøtte. * Næringslivsaktører som for eksempel legemiddelindustrien, har behov for for å følge opp effekt av egne produkter og tjenester. Det kan være både etter egne ønsker og myndighetspålagte krav.   Leverandøren skal ikke etablere disse tjenestene, men tilby en teknologiplattform som gjør det mulig for et økosystem av aktører som jobber med helseanalyse (ref Figur 2) å publisere nye resultater til ulike sluttbrukere. Sluttbrukernes behov er derfor ikke beskrevet utfyllende under. Disse brukerhistoriene må sees i sammenheng med brukerhistoriene knyttet til EPOS *Analyserom* som beskrevet i kapittel 5.2.2.1.  Brukerhistoriene under er beskrevet for følgende aktører:   * **Konsument av analysetjenester** – Denne aktøren er en samlebetegnelse for brukere som bruker resultater fra helseanalyse som beslutningsstøtte i sitt arbeid. |
| **Brukerhistorier**   1. Som konsument av analysetjenester ønsker jeg en enkel måte å få tilgang til resultater slik at jeg effektiv kan bruke disse i mitt arbeid. 2. Som konsument av analysetjenester ønsker jeg stor fleksibilitet rundt hvilke kanaler resultater leveres til meg, slik at jeg kan få tak i de dataene jeg trenger når jeg trenger det. 3. Som konsument av analysetjenester ønsker jeg å kunne sammenligne data fra min egen virksomhet med andre datakilder, slik at jeg kan se om det er områder med mulighet for kvalitetsforbedring. 4. Som konsument av analysetjenester har jeg behov for analyser med data i nær sanntid, slik at jeg kan overvåke smittsomme sykdommer, pandemier o.a. |

#### Dataleverandørs forvaltningsrom

|  |
| --- |
| Tittel: Dataleverandørs forvaltningsrom |
| **EPOS**  Som dataleverandør ønsker jeg tilgang til en infrastruktur der jeg kan kvalitetssikre, strukturere og berike min rådata slik at jeg kan skape og forvalte dataprodukter iht. FAIR prinsippene. |
| **Beskrivelse**  Helseanalyseplattformen bør tilby en infrastruktur som gjør at en dataleverandør kan drive datakvalitetsarbeid og skape dataprodukter ut fra data som er samlet inn. Dataleverandørs forvaltningsrom bør sees på som en variant av et analyserom. Kravene man har som dataansvarlig er derfor de samme her som for analyserom (selv om de ikke er beskrevet konkret under dette EPOS).  Brukerhistoriene under er beskrevet for følgende aktører:   * **Bruker av forvaltningsrom** – Dette kan være myndighetsaktører, næringslivsaktører eller andre som bruker et forvaltningsrom for å produsere dataprodukter. Der behovene er spesifikke for en av disse gruppene vil det være spesifisert. * **Dataansvarlig for forvaltningsrom** – Denne aktøren har det formelle dataansvaret for data som ligger i forvaltningsrommet. * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. |
| **Brukerhistorier**   1. Som bruker av forvaltningsrom må jeg kunne lagre person- og helseopplysninger i forvaltningsrommet på en sikker måte, slik at data jeg er ansvarlig for ikke kommer på avveie 2. Som bruker av forvaltningsrom ønsker jeg å kunne sette opp integrasjoner til mine kildesystemer slik at rådata fra kildesystemene kan tilgjengeliggjøres i forvaltningsrommet på en sikker måte 3. Som bruker av forvaltningsrom ønsker jeg å kunne etablere og forvalte kvalitetsregler slik at jeg kan kvalitetssikre mine dataprodukter 4. Som bruker av forvaltningsrom ønsker jeg å kunne berike mine data med data fra andre kilder, slik at jeg kan ivareta høy datakvalitet på mine dataprodukter 5. Som bruker av forvaltningsrom ønsker jeg å skape dataprodukter oppfyller de internasjonale FAIR[[4]](#footnote-5) prinsippene, slik at de kan gjenfinnes og gjenbrukes. 6. Som bruker av forvaltningsrom ønsker jeg å vedlikeholde informasjonsmodeller på mine data og dataprodukter, slik at jeg kan sikre god datakvalitet |

#### Eksplorativ analyse

|  |
| --- |
| Tittel: Eksplorativ analyse |
| **EPOS**  Som forsker ønsker jeg søknadsfri tilgang til å gjøre eksplorativ analyse i store, koblede, datasett, slik at jeg kan analyse data umiddelbart uten å måtte gå via en søknadsprosess. |
| **Beskrivelse**  Eksplorativ analyse er analysetjenester der sluttbrukere fritt kan analysere data uten at personopplysninger eksponeres. Hensikten er at brukere skal kunne få umiddelbar tilgang til data, uten å gå via en søknadsprosess, men samtidig sikre anonymiteten til individet. Data må derfor være tilrettelagt på en slik måte at de ikke kan spores tilbake til enkelt individer.  Kohortutforsker er et eksempel på eksplorativ analyse. Dette er en tjeneste der sluttbrukere selv vil kunne sette definerte inklusjon- og eksklusjonskriterier for et datasett. Målet med en slik tjeneste er å kunne identifisere den potensielle størrelsen av en kohort/utvalg for en gitt problemstilling tidlig i et forskningsprosjekt. Bruker skal ikke kunne se annet enn anonymiserte resultater som matcher kriteriene. En slik tjeneste vil forutsette direkte tilgang/oppslag mot personopplysninger.  SSBs microdata.no er et eksempel på en eksisterende eksplorativ analysetjeneste for enkelte demografiske og sosioøkonomiske variabler fra SSB.  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. * **Bruker av eksplorativ analyse** – Denne aktøren er en samlebetegnelse på sluttbrukere som analyserer helsedata for å skape ny kunnskap eller innsikt. For eksempel forskere, myndighetsaktører eller helseledere * **Helsedataservice** - Denne aktøren vil i fremtiden gjøre saksbehandling, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. |
| **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 tilgang på helsedata og kan starte forskningsarbeidet raskt. 3. Som Helsedataservice ønsker jeg å forsikre meg om at det ikke er mulig å identifisere enkeltindivider gjennom kohortutforskeren slik at personvernet til innbyggerne er ivaretatt 4. Som forsker ønsker jeg søknadsfri tilgang til å gjøre eksplorativ analyse i store, koblede, datasett, slik at jeg kan analyse data umiddelbart uten å måtte gå via en søknadsprosess. 5. Som forsker ønsker jeg dokumentasjon over alle variabler som er tilgjengelig for eksplorativ analyse, slik at det er enkelt for meg å plukke ut de dataene jeg har behov for. 6. Som forsker ønsker jeg mulighet til å hente ut resultater fra eksplorativ analyse, slik at det er mulig for meg å bruke resultatene i mitt videre arbeide. |

#### Syntetiske data

|  |
| --- |
| Tittel: Syntetiske data |
| **EPOS**  Som Helsedataservice ønsker jeg å tilby syntetiske data, slik at brukere kan utvikle nye løsninger uten å trenge direkte eller indirekte identifiserbare personopplysninger. |
| **Beskrivelse**  Syntetiske data er genererte data med tilsvarende statistiske/matematiske egenskaper, struktur og relasjoner som reelle data. For Helsedataservice er det et mål å kunne tilby syntetiske data hvor personopplysningene i det originale datasettet ikke er mulig å gjenskape. Syntetiske data kan dermed brukes til å skjerme reelle data mot uønsket bruk.  Syntetiske data kan ha følgende bruksområder:   * Mulighet for registerforvalter til å generere representative testdata til det enkelte register * Benytte syntetiske data som testdata i utvikling av tjenester på Helseanalyseplattformen * Benytte syntetiske data for metode- og verktøyutvikling i et forskningsprosjekt * Benytte syntetiske data for innovasjonsformål rundt helsedata.   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, fatte vedtak om tilgang til helsedata, være ansvarlig for tilgjengeliggjøring av data fra dataplattformen samt være plattformeier for Helseanalyseplattformens økosystem. I tillegg vil denne aktøren kunne være tjenestetilbyder på Helseanalyseplattformen. Helsedataservice vil etter planen være dataansvarlig for data på dataplattformen. * **Registerforvalter** – Denne aktøren er forvaltningsansvarlig og data ansvarlig for et eller flere helseregistre. |
| **Brukerhistorier**   1. Som registerforvalter ønsker jeg å kunne tilby syntetiske datasett for mine data slik at andre aktører kan bruke disse til å teste mot mine tjenester 2. Som Helsedataservice ønsker jeg å kunne tilby syntetiske datasett slik at andre aktører kan bruke disse til å teste mot mine tjenester 3. Som forsker ønsker å jeg tilgang til ett mest mulig representativt syntetisk datasett, 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. |

#### 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[[5]](#footnote-6) 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.  Brukerhistoriene under er beskrevet for følgende aktører:   * **Registerforvalter** – Denne aktøren er forvaltningsansvarlig og data ansvarlig for et eller flere helseregistre. |
| **Brukerhistorier**   1. Som registerforvalter ønsker jeg en tjeneste for å lagre person- og helseopplysninger, slik at jeg slipper å tilrettelegge for dette selv. 2. Som registerforvalter ønsker jeg muligheten for å innhente data fra skjemaløsninger, slik at registeret inneholder relevante data. 3. Som registerforvalter ønsker jeg gode mekanismer for å sikre hvilke data som forlater registeret, slik at jeg har kontroll på personopplysninger 4. Som registerforvalter ønsker jeg selv å kunne håndtere tilgangsstyring av registeret 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 5. Som registerforvalter ønsker jeg å enkelt kunne se hvilke behandlingsaktiviteter som er gjort i registeret, slik at jeg kan etterprøve at bruken er i samsvar med personvernregelverket 6. Som registerforvalter ønsker jeg mekanismer for å kunne rette og korrigere personopplysninger som er uriktige, slik at jeg ivaretar den registrertes rettigheter 7. Som registerforvalter ønsker jeg mekanismer for å kunne slette personopplysninger som er feil eller ulovlig, slik at jeg ivaretar den registrertes rettigheter 8. Som registerforvalter ønsker jeg å kunne motta og administrere forespørsler om innsyn, retting og sletting av data, slik at jeg kan oppfylle mine plikter som dataansvarlig 9. Som registerforvalter ønsker jeg å kunne motta og administrere forespørsler om begrensning, protest og dataportabilitet, slik at jeg kan oppfylle mine plikter som dataansvarlig 10. Som registerforvalter ønsker jeg å kunne underrette mottakere som har fått utlevert personopplysninger som er rettet, slettet eller begrenset, slik at jeg oppfyller mine plikter som dataansvarlig |

### Innbyggertjenester



Innbygger skal i hovedsak få oppfylt sine rettigheter i forbindelse med lagring og behandling av helsedata gjennom helsenorge.no. Selv om det ikke er en del av anskaffelsen å lage brukergrensesnitt for innbygger på helsenorge.no må Helseanalyseplattformen legge til rette for dette, og utvikle funksjonalitet som dekker behovene under i samarbeid med helsenorge.no.

I tilfeller der brukere av Helseanalyseplattformen har behov for å interagere med innbygger skal dette også foregå via helsenorge.no.

#### Innbyggers rettigheter

|  |
| --- |
| Tittel: Innbyggers rettigheter |
| **EPOS**  Som innbygger ønsker jeg innsyn i hvilke data som finnes om meg på Helseanalyseplattformen, hva de er brukt til og mulighet til å regulere bruken, slik at jeg har kontroll på egne helseopplysninger. |
| **Beskrivelse**  For at Helseanalyseplattformen skal ha den nødvendige tillitten både hos bruker og den registrerte er det helt avgjørende at både informasjonssikkerhet og grunnleggende personvernrettigheter ivaretas. Innbyggerne har flere rettigheter knyttet til behandling av deres egne helse- og personopplysninger og dataplattformen må tilrettelegge for at de blir ivaretatt.  Innbygger har et krav på innsyn i opplysninger om seg selv for å ha kontroll over egne opplysninger. Dataplattformen må derfor tilrettelegge for funksjonalitet rundt innsynretten og retten til dataportabilitet. Videre må det være mulig for innbygger å få en oversikt over hvilke samtykker og reservasjoner de har gitt i ulike sammenhenger.  Dataplattformen må også tilrettelegge for å at opplysninger om innbygger kan rettes og slettes, samt at behandlingen av opplysningene stopper opp dersom innbygger krever det, gjennom deres rettighet til protest og begrensning.  Helsenorge.no er innbyggers inngang til egne helseopplysninger og helsedata. Innbyggers innsynsmuligheter og muligheter for å ivareta sine rettigheter skal skje gjennom helsenorge.no. Dataplattformen må derfor kunne integreres mot Helsenorge.   * **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 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. 2. Som innbygger ønsker jeg en enkel oversikt over hvilke opplysninger som er lagret om meg på dataplattformen, slik at jeg får kontroll over egne opplysninger. 3. Som innbygger ønsker jeg å kunne få utlevert og ta med meg data om meg selv, slik at jeg kan behandle dem der jeg måtte ønske det. 4. Som innbygger ønsker jeg å kunne gi tilbakemelding om midlertidig stans for videre behandling av opplysninger om meg, slik at jeg har eierskap og kontroll på mine data. 5. Som innbygger ønsker jeg å kunne gi tilbakemelding om feilregistreringer, slik at jeg kan få rettet opp feil i data om meg selv. 6. 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. 7. 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. 8. Som innbygger ønsker jeg mulighet til å samtykke til behandling av personopplysninger på dataplattformen, slik at jeg har eierskap og kontroll på mine data 9. Som innbygger ønsker jeg informasjon om hvordan dataplattformen håndterer mine helsedata, på en enkelt tilgjengelig måte, slik at jeg forstår hvilke rettigheter jeg har og hvordan mine person- og helsedata blir behandlet. 10. Som innbygger ønsker jeg en samlet over alle mine samtykker jeg har gitt, slik at jeg enkelt kan ha oversikt over hvor mine person- og helsedata blir benyttet 11. Som innbygger ønsker jeg enkelt å kunne trekke samtykker, slik at dataene umiddelbart ikke lenger blir brukt til forskning eller andre formål |

#### Samhandling mellom bruker av data- og analysetjenester og innbygger

|  |
| --- |
| Tittel: Samhandling mellom bruker av data- og analysetjenester og innbygger |
| **EPOS**  Som bruker av data- og analysetjenester ønsker jeg å kunne samhandle med innbyggere for å få samtykke til bruk av opplysninger og innhente nye data. |
| **Beskrivelse**  Brukere av data- og analysetjenester kan ha behov for samhandling i form av dialog og interaksjon 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 avsender. 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.  Helsenorge.no er den offentlige nettsiden for innbyggers inngang til helseopplysninger og helsedata. Bruk av selvbetjeningsløsninger på helsenorge.no er samtykkebasert og frivillig. Målet er all informasjon til og samhandling med innbygger skal tilbys via helsenorge.no for å lage en samlet nettside for helsesektoren. De underliggende tjenestene til helsenorge.no inneholder funksjonalitet for å sende meldinger samt lagre samtykker og reservasjoner, som gir innbygger mulighet til å få en samlet oversikt på tvers av helsesektoren. Det gir også innbygger mulighet å kunne administrere disse via helsenorge.no, dersom det er behov. Mer informasjon om tjenesten er tilgjengelig på: <https://helsenorge.no/om-helsenorge-no>  Det vil også være behov for å integrere med tjenester som leveres av anskaffelsen på søknad- og saksbehandlingstjenester for å realisere disse tjenestene.   * **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. * **Bruker av data- og analysetjenester** – Denne betegnelsen dekker forskere, næringslivsaktører, myndigheter og andre som er ansvarlig for eller behandler data på Helseanalyseplattformen. |
| **Brukerhistorier**   1. Som bruker av data- og analysetjenester ønsker jeg å kunne sende samtykkeforespørsler til et utvalg innbyggere for å for eksempel kunne bruke helsedata som allerede er samlet inn til nye formål eller om deltakelse i forskningsprosjekter (kliniske studier, helseundersøkelser o.a.). 2. Som bruker av data- og analysetjenester ønsker jeg å kunne sende ut undersøkelser til et utvalg av innbyggere og få svarene på Helseanalyseplattformen, slik at jeg har en enkel og sikker måte å få inn data på. 3. Som bruker av data- og analysetjenester ønsker jeg å kunne ha dialog med deltagere i forskningsprosjekter, slik at jeg kan innhente kompletterende opplysninger og informere om resultater. 4. Som bruker av data- og analysetjenester ønsker jeg gode verktøy til å håndtere samtykker, slik at jeg bare behandler data jeg har behandlingsgrunnlag for. |

## Opsjon 1 – Arkiv i Norge

Helseanalyseplattformen (HAP) vil etter planen eies av et offentlig organ ("Helsedataservice") etter arkivloven[[6]](#footnote-7). Organet vil være forpliktet til å ha arkiv, og arkivet vil være omfattet av arkivloven og arkivforskriftens bestemmelser, jf. arkivloven § 6.

Informasjonen som ligger i registrene som lagres på og behandles på Helseanalyseplattformen er mest sannsynlig er å anse som en del av Helsedataservices arkiv. Grunnen til dette er at Helseanalyseplattformen mottar slike dokumenter som ledd i sin virksomhet, og at dokumentene har dokumentasjonsverdi. Slike dokumenter vil derfor være underlagt arkivlovens kapittel II, herunder forbudet mot overføring av arkivmateriale til utlandet, jf. arkivloven § 9 b.7

Gjeldende arkivloven § 9 b fastsetter at det er forbudt å føre arkivmateriale ut av landet. § 9 b er i utgangspunktet til hinder for lagring av arkivmateriale i skytjenester, hvis arkivmateriale lagres på servere i utlandet. Arkivloven er imidlertid ikke til hinder for lagring av arkivmateriale i skytjenester, såfremt serverne ligger i Norge.

Med andre ord, ved bruk av skytjenester for lagring av arkivmateriale under dagens regelverk, må man kunne fastslå med sikkerhet, at arkivmateriale lagres på servere i Norge.

Regelverket er likevel ikke til hinder for at kopier av data på Helseanalyseplattformen lagres i skytjenester i EØS – området. Men dette forutsetter da at det komplette arkivet oppdateres fortløpende med arkivverdig informasjon.

Det er lagt frem forslag om ny arkivlov i NOU 2019:9. Dersom denne vedtas, vil den åpne for lagring av arkivmateriale på skytjenester med bruk av datasenteret i EØS-området. NOUen er foreløpig ikke sendt på høring, og det er usikkert om og når ny lov eventuelt vil tre i kraft.

Direktoratet vil søke unntak fra bestemmelsen i §9b i gjeldende arkivlov inntil nytt regelverk er på plass.

Dersom slikt unntak ikke innvilges av Riksarkivet og løsningen er basert på behandling og lagring av arkivverdig materiale på servere i datasentre i EØS området, vil det være behov for å utløse følgende opsjon:

* Som Helsedataservice ønsker jeg å kunne arkivere alt arkivverdig materiale som lagres på Helseanalyseplattformen fortløpende (daglig) på servere i datasenter i Norge.[[7]](#footnote-8)

# Utforming av Helseanalyseplattformen

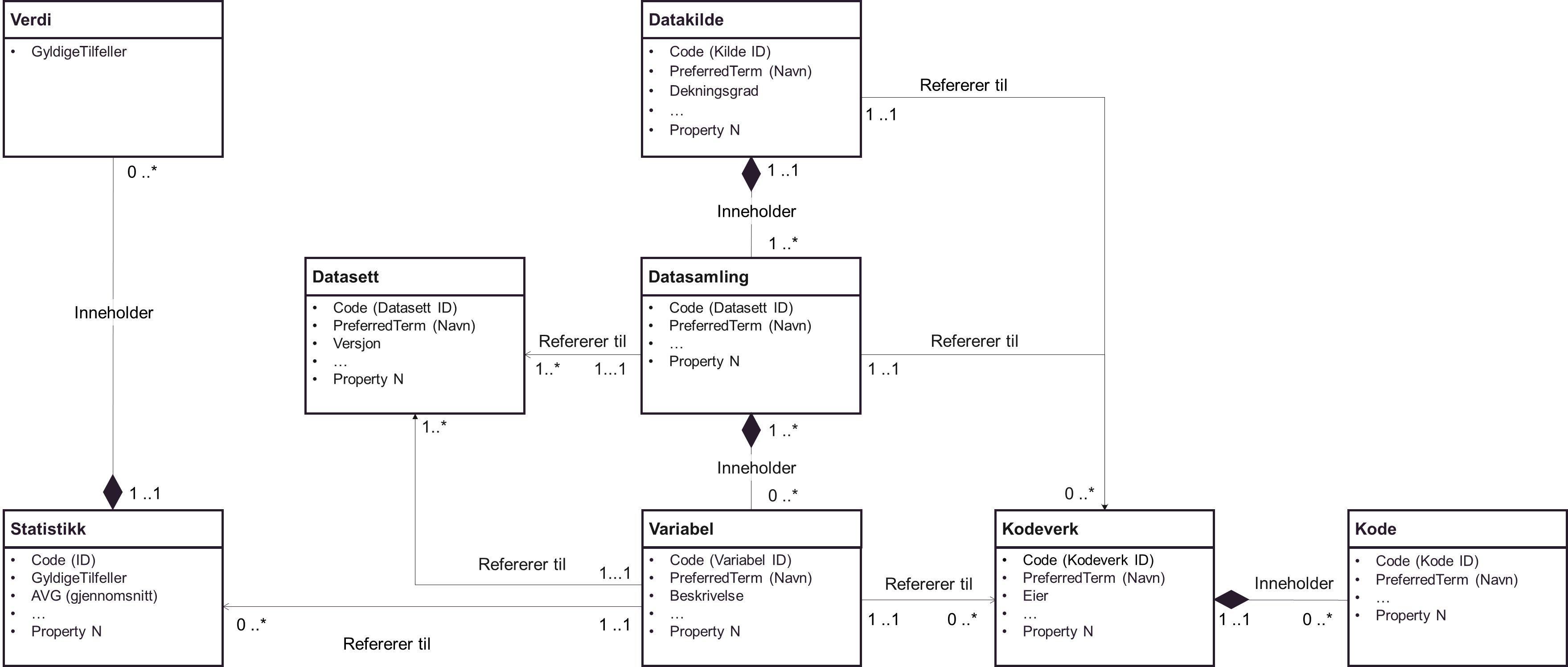
## Metadata, kodeverk og terminologi

Programmet jobber med realisering av en nasjonal variabelkatalog som vil inneholde metadata om selve registrene med tilhørende variabler. I tillegg vil den samme løsningen bli benyttet til å forvalte nasjonale kodeverk og terminologi. Variabelkatalogen er basert på løsningen HealthTerm som leveres av den danske leverandøren CareCom. Planen er at alle sentrale helseregistre og et utvalg av nasjonale kvalitetsregistre skal være tilgjengeliggjort i løsningen ila. 2019. HealthTerm vil også erstatte dagens volven.no og finnkode.no, og vil dermed også inneholde informasjon om alle nasjonale kodeverk og terminologier. Dette muliggjør at man kan mappe direkte til det nasjonale kodeverket ved definisjon av enkeltvariabler i registrene. Løsningen tilbyr et REST API som muliggjør uthenting av all data som er tilgjengeliggjort i løsningen. Leverandøren vil derfor kunne benytte løsningen for både å hente ut metadata, samt også kodeverk med tilhørende beskrivelser. Det vil bli gitt en kort beskrivelse av logisk informasjonsmodell og informasjonselementer for metadata i den nasjonale variabelkatalogen. Underlaget er hentet fra en versjon 0.9 av spesifikasjonen, så det vil kunne komme endringer her.

Figur 8 viser den logiske informasjonsmodellen for metadata om helsedata til sekundærbruk. Med logisk informasjonsmodell menes hvilke klasser som inngår i informasjonsmodellen og hvordan de logiske relasjonene mellom de ulike klassene skal håndteres.

For å forstå den logiske informasjonsmodellen under vil det være hensiktsmessig å ha kjennskap til et utvalg begrep:

* Datakilde er definert som eieren av dataene. I denne versjonen av spesifikasjonen et en datakilde ekvivalent med et helseregister.
* Datasamling er definert som et sub-register innenfor en datakilde, altså en delmengde av variablene i den aktuelle datakilden. Eksempler på datasamlinger kan være sektorer i Norsk pasientregister eller skjema i medisinske kvalitetsregistre.
* Datasett er et teknisk hjelpemiddel som brukes til å definere hvilke variabler som inngår i ulike årganger/versjoner av de ulike datasamlingene i en datakilde.
* Variabler er de informasjonsbærende elementene i registeret, og beskriver hvilken informasjon som finnes i registrene.
* Kodeverk representerer i denne sammenhengen et verdisett. Et kodeverk kan for eksempel representere en variabels verdisett. Det kan også representere en samling verdier som brukes til å beskrive en datakilde.
* Kode er i denne sammenheng det samme som svaralternativene i et verdisett.
* Statistikk er definert som de statistiske egenskapene ved en årgang/versjon av en variabel.
* Verdi er definert som antall gyldige tilfeller av et svaralternativ/utfall av en variabel.



Figur 8 Logisk informasjonsmodell for metadata om helsedata til sekundærbruk

Hver enkelt datakilde er definert ut fra et sett metadataelement om datakilden. Metadataelementer er elementer som beskriver egenskaper ved kilden. Dette vil eksempelvis være navn på registeret, eier og type innhold.

* En datakilde inneholder en eller flere datasamlinger.
* Hver datasamling er definert ut fra et sett med egne metadataelement. Her vil metadataelementet beskrive egenskaper ved datasamlingen. Dette vil eksempelvis være navn på datasamlingen som eksempelvis en sektor innenfor Norsk pasientregister.
* Hver datasamling inneholder variabler som er definert ut fra et sett metadataelement om variabelen. Samme variabel kan inngå i flere datasamlinger. For variabelen vil metadataelementet eksempelvis være navn på variabelen, en beskrivelse av hva den representerer, og gyldighetsperiode.
* Hver datasamling refererer til ett eller flere datasett som definerer forskjellige årssett/versjoner av datasamlingen.
* Hver variabel refererer til ett eller flere datasett.
* Gjennom referansene fra variabel og datasamling til datasett synliggjør man hvilke variabler som inngår i hvilke versjoner av en datasamling.

Variabler kan referere til kodeverk. For diskre variabler (variabler med svaralternativ) utgjør dette kodeverket variabelens verdisett der kodeverket inneholder koder som representerer alle mulige verdier(svaralternativ) en variabel kan ha. Også kontinuerlige variabler kan referere til kodeverk for begrepsdefinisjon av variabelen, men disse vil ikke ha koder som representer variabelens mulige verdier.

Hver variabel kan også referere til statistikk om seg selv, som gjennomsnitt, standardavvik og årstall statistikken er gyldig for. For diskre variabler kan statistikk inneholde antall utfall av de ulike mulige verdiene i variabelens verdisett.

Datakilder og datasamlinger kan også referere til kodeverk for å forenkle filtrering og søk på tvers av de ulike kildene/datasamlingene. For eksempel kan et register referere til de ulike hovedkapitlene i ICD-10 som kilden adresserer. En kan også definere svaralternativene for en property som egne kodeverk, for å standardisere innholdet i disse.

## Integrasjoner

Figur 9 viser oversikt over planlagte integrasjoner mot Helseanalyseplattformen. Figuren er basert på Archimate notasjon.

Figuren viser et helhetsbilde i forhold til hva som er planlagt av integrasjoner per juni 2019, men det vil her kunne komme endringer både i forhold til hvilke integrasjoner det er behov for og når de skal realiseres. Det er i figuren gjort et skille mellom integrasjon mot 1) eksterne tjenester og grensesnitt, og 2) datakilder til plattformen.

Hver av komponentene er nærmere beskrevet i henholdsvis kapittel 6.2.1 og kapittel 6.2.2. I tillegg er det beskrevet et eget avsnitt som tar for seg integrasjon mot Helsenettet (kapittel 6.2.3) som vil være sentralt for oppkobling mot de fleste komponentene i helse- og omsorgsektoren.



Figur 9: Application communication diagram (v0.3) på nivå 1 for Helseanalyseplattformen

### Integrasjon mot eksterne tjenester og grensesnitt

Tabell 3 viser en oversikt over komponenter og grensesnitt som er tenkt å integrere med Helseanalyseplattformen. Det er for hver komponent beskrevet type grensesnitt og forretningsmessig kontekst. Tabellen er beskrevet med utgangspunkt i planen slik den foreligger per i dag, men det vil kunne komme endringer både i forhold til hvilke komponenter og når den enkelte komponent er tenkt integrert med Helseanalyseplattformen.

Tabell 3: Beskrivelse over eksterne tjenester og grensesnitt som Helseanalyseplattformen etter planen vil integreres mot

| Løsning | Eier | Beskrivelse | Grensesnitt/ protokoll | Forretningsmessig kontekst |
| --- | --- | --- | --- | --- |
| HelseID | Norsk Helsenett | HelseID er en felles påloggingsløsning for helse- og omsorgssektoren. For mer informasjon: <https://www.nhn.no/helseid/> | OpenID Connect/SAML | HelseID skal etter planen benyttes som påloggingsløsning for forsker og andre brukere av Helseanalyseplattformen. HelseID er et sentralt tillitsanker som fødererer mot andre påloggingsløsninger som eksempelvis ID-porten. En begrensing vil potensielt være støtte for utenlandske brukere, så man vil potensielt måtte se på alternativer her. |
| Filoverførings-tjenesten (Nextcloud Files) | Norsk Helsenett | Nextcloud er en Open Source fildelingstjeneste, for å kunne håndtere store datafiler for midlertidig overføring.  For mer informasjon: <https://nextcloud.com/> | Ikke besluttet (WebDAV API et alternativ) | Nextcloud Files skal i hovedsak benyttes for ad-hoc overføring av store datafiler mellom registerforvaltere, men vil potensielt også kunne benyttes for overføring av data til Helseanalyseplattformen og forsker. Løsningen vil kunne benyttes både for manuell overføring via et web grensesnitt, men også for system-til-system overføring via API. Tjenesten vil bli tilgjengeliggjort gjennom helsedata.no. |
| HealthTerm | Direktoratet for e-helse | En nasjonal komponent som inneholder alle nasjonale kodeverk og terminologi i tillegg til informasjon om registervariabler med tilhørende metadata. | REST API | HealthTerm skal etter planen inneholde både kodeverk og terminologi i tillegg til metadata om variabler i registrene. Dette vil være kilde for variabelutforskeren på helsedata.no og er planlagt implementert i midten av 2019.I tillegg vil løsningen være kilde for kodeverk og terminologi, samt metadata om variabler og datakilder for data og analyseplattformen. HealthTerm vil erstatte dagens finnkode og volven.no. |
| Saks-behandlingsløsning for helsedata | Direktoratet for e-helse | En felles saksbehandlingsløsning for behandling av søknader for tilgang til data. Løsningen vil bli benyttet av Helsedataservice og være felles på tvers av registerforvaltere. Pega er anskaffet til dette formålet | Ikke bestemt | Saksbehandlerløsningen vil være sentral for å sette rammene for hva den enkelte søker skal få tilgang til av data. Det bør ses på hvordan man basert på vedtaket om rammene for datatilgang i størst mulig grad kan automatisere tilgjengeliggjøring av data i brukerens analyserom. |
| Helsedata.no | Direktoratet for e-helse | Helsedata.no er en webportal basert på EPIServer CMS som er inngangsporten for forsker og andre brukere av helsedata. | Løsningen støtter de fleste moderne protokoller som eksempelvis REST/SOAP. Helsedata.no vil typisk gjøre oppslag mot eller referere til tjenester på Helseanalyseplattformen for å kunne eksponere tjenesten til sluttbruker. | Helsedata.no vil fungere som en inngangsport for forskere og andre brukere av helsedata. For alle tjenester som tilbys vil portalen fungere som en inngangsport. Hvordan selve tjenestene tilgjengeliggjøres til sluttbruker vil kunne variere. Her vil alt fra tett integrasjon til linking mot tjenestene være en mulighet. |
| Helsenorge.no – Digital dialog | Direktoratet for e-helse | Digital dialog er en funksjonalitet som tilbys gjennom innbyggerportalen Helsenorge.no for å tilby digital dialog mellom innbygger og aktører i helsesektoren. | Løsningen er basert på meldingsutveksling via AMQP. Selve meldingskøene driftes av NHN og det tilbys sertifikater og adressering via adresseregistret. For mer informasjon se: [Link](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjaiaGZt7HiAhWQ_CoKHUwfBngQFjAAegQIABAC&url=https%3A%2F%2Fehelse.no%2FDocuments%2FEPJ-l%25C3%25B8ftet%2FEPJ-l%25C3%25B8ftet%2520AMQP%2520spesifikasjon%2520helsenorge.no).pdf&usg=AOvVaw3e2tNJ2Mfe1dUBGmua08sB) | Digital dialog er tenkt benyttet for å kunne tilby digital dialog med innbygger via Helseanalyseplattformen. Det vil kunne være behov for dette både for digital dialog mellom forsker og innbygger, men også innbygger og helsedataservice. Formålet er å kunne håndtere henvendelser fra innbygger for eksempel ved spørsmål om innsynsforespørsler, eller for deltagelse i et forskningsprosjekt. |
| Helsenorge.no – Innsyn | Direktoratet for e-helse | Innsyn via Helsenorge.no er en funksjonalitet som muliggjør at aktører i sektoren kan tilby innsyn til innbygger for hvilken informasjon som er lagret om dem. | Løsningen tilbyr innsyn både ved asynkrone forespørsler via digital dialog (AMQP). Eller ved at aktøren som ønsker å tilby innsyn tilgjengeliggjør et REST grensesnitt i tråd med en definert spesifikasjon. | Innsynsfunksjonaliteten er tenk benyttet for å tilby innbygger innsyn i sine helsedata som ligger tilgjengelig på Helseanalyseplattformen. |
| Helsenorge.no – Personvern-komponenten | Direktoratet for e-helse | Personvernkomponenten er en nasjonal komponent for å tilby funksjonalitet for samtykke, reservasjon og fullmakt. Administrasjon av personverninnstillinger tilbys til innbygger via helsenorge.no | Løsningen kan nås både via meldingsutveksling (AMQP) og synkrone REST oppslag. For kontroll av personverninnstillinger vil typisk REST oppslag være aktuelt, mens AMQP kan benyttes for å abonnere på endringer i innbyggers personverninnstillinger. | Personvernkomponenten er tenkt benyttet i hovedsak for å tilby funksjonalitet for samtykke og reservasjon. Helseanalyseplattformen vil kunne abonnere på endringer for å identifisere tilfeller der innbygger trekker sitt samtykke/reserverer seg og det er behov for å slette helseopplysninger som er lagret om innbyggeren. |
| Tjenester for sensitive data (TSD) | Universitetet i Oslo | TSD er et fullt sett med tjenester, fra innsamling av data, til analyse, behandling og lagring, i sikrede omgivelser. | Løsningen tilbyr et REST API for import og eksport av data.  For mer informasjon se: [Link](https://www.uio.no/english/services/it/research/sensitive-data/use-tsd/import-export/import-data-using-the-tsd-api.html) | Løsningen vil fungere som et eksternt analyserom der forsker kan velge å eksportere data til løsningen etter godkjent søknadsprosess. |
| Microdata.no | SSB | Analyseplattform utviklet i samarbeid mellom NSD - Norsk senter for forskningsdata (NSD) og Statistisk sentralbyrå (SSB). Løsningen muliggjør analyse basert på reelle data, men uten at forskeren faktisk får se innholdet. | Ukjent | Det vil kunne være aktuelt å tilby enkelte variabler fra Helseanalyseplattformen som kilde til microdata.no. |
| HUNT Cloud | NTNU | HUNT Cloud er en analyseplattform utviklet av Helseundersøkelsen i Nord Trøndelag. Løsningen tilbyr funksjonalitet for lagring og analyse av data. | Ukjent | Løsningen vil fungere som et eksternt analyserom der forsker kan velge å eksportere data til løsningen etter godkjent søknadsprosess. |
| Fakturerings-system | Direktoratet for økonomistyring | DFØ er tilbyder av løsning for økonomi og regnskap til Direktoratet for e-helse. Denne løsningen vil trolig bli benyttet for utfakturering fra Helseanalyseplattformen. | Ukjent | Løsningen vil bli benyttet for utfakturering mot brukere av Helseanalyseplattformen. |
| Autorisasjons-tjenester | Ulike eiere avhengig av løsning | Med autorisasjons-tjenester menes det her alle typer av eksterne tjenester som benyttes for autorisasjon og tilgangsstyring. | Ulike grensesnitt avhengig av løsning. | Det vil kunne være behov for å benytte en rekke ulike eksterne autorisasjonstjenester for å kunne gjøre beslutning om tilgang på Helseanalyseplattformen. Dette kan både være ulike LDAP tjenester, SAAS tjenester, og andre informasjonskilder (Policy-information-point) som grunnlag for beslutning om tilgang. |
| FALK | Helse Midt IKT | Falk er en felleskomponent for autentisering og administrasjon av tilganger til medisinske kvalitetsregistre. For mer informasjon se: [Link](https://www.kvalitetsregistre.no/artikkel/ny-losning-palogging-testes-ut-i-februar) | Ukjent | Løsningen vil potensielt kunne benyttes for å gi tilgang til data for Nasjonale medisinske kvalitetsregistre. |

### Integrasjon av datakilder inn på dataplattformen

Tabell 4 viser en oversikt over potensielle datakilder til Helseanalyseplattformen og egenskaper ved disse. Dette er forutsetninger slik de foreligger hos den enkelte datakilde per i dag, men det vil kunne komme endringer spesielt med tanke på hyppighet, formater og mekanismer for dataoverføring. Eventuelt også basert på anbefalinger fra leverandør. Tabellen er ikke uttømmende, men viser et utvalg av de viktigste datakildene som er planlagt på kort og mellomlang sikt. Formålet med tabellen er å gi leverandøren et bilde hva type datakilder og forutsetninger som vil ligge til grunn ved overføre til, og behandling av data på Helseanalyseplattformen.

Tabell 4: Beskrivelse av datakilder som Helseanalyseplattformen skal integreres mot

| Datakilde | Eier | Type innhold  (Hendelse) | Juridisk grunnlag | Frekvens på hvor ofte data er tenkt overført | Volum Totalt | Størrelse | Historikk | Endringstakt | Datakvalitet | Integrasjons-muligheter | Utvekslings-format | Kjøremiljø | Prioritet |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sentrale helseregistre** | | | | | | | | | | | | | |
| Norsk Pasientregister  Somatikk/Psykiatri | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger)  [Metadata](http://hrr.uit.no/hrr/) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2007-12-07-1389) | Overføres i tråd med hyppigheten på produksjon av kvalitetssikrede datasett i NPR som brukes til forskning | Ca. 3 mill. distinkte personer pr år, ca. 15 mill. distinkte episoder pr år, ca. 5 mill. personer (ca. hele befolkningen) totalt i registeret | Avhenger av overføringsformat og struktur  Ca. 20-30 GB pr år, ca. 5 TB totalt (Inn) | Årsdatafiler frem til 2017 deretter rene DB forekomster | Midlertidige månedlige tall til enkelte formål, i hovedsak tertialvis. | Generelt god, men varierer på enkelte underområder. | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP).  API integrasjoner i fremtiden? Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 1 |
| Norsk Pasientregister  Venteliste | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger)  [Metadata](http://hrr.uit.no/hrr/) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2007-12-07-1389) | Overføres i tråd med hyppigheten på produksjon av kvalitetssikrede datasett i NPR som brukes til forskning | Som over, samme XML, men basert på henvisninger (ca. 5-10 mill.) | Som over, er i samme DB og kommer i samme meldingsstruktur | Årsdatafiler frem til 2013, deretter rene DB forekomster | Månedlig (foreløpig) og tertialvis (endelig) | Generelt høy på det som gir utsalg på ventelistetall. | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP).  API integrasjoner i fremtiden? Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 1 |
| Norsk Pasientregister  Avtalespesialist | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger)  [Metadata](http://hrr.uit.no/hrr/) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2007-12-07-1389) | Overføres i tråd med hyppigheten på produksjon av kvalitetssikrede datasett i NPR som brukes til forskning | Telles sammen med overstående | Som over, er i samme DB og kommer i samme meldingsstruktur | Årsdatafiler frem til 2014, deretter rene DB forekomster | Tertialvis | Noen mangler på kompletthet, utfordringer med enkelte enheter | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP).  API integrasjoner i fremtiden? Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 2 |
| Norsk Pasientregister  Personskade | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger)  [Metadata](http://hrr.uit.no/hrr/) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2007-12-07-1389) | Overføres i tråd med hyppigheten på produksjon av kvalitetssikrede datasett i NPR som brukes til forskning | Telles sammen med overstående | Som over, er i samme DB og kommer i samme meldingsstruktur | Årsdatafiler frem til 2016, deretter rene DB forekomster | Tertialvis | Noen mangler på kompletthet | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP).  API integrasjoner i fremtiden? Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 2 |
| Norsk Pasientregister  Rusbehandling / spesifikk rapportering ut over ordinær aktivitet | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger)  [Metadata](http://hrr.uit.no/hrr/) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2007-12-07-1389) | Overføres i tråd med hyppigheten på produksjon av kvalitetssikrede datasett i NPR som brukes til forskning | Telles sammen med overstående | Som over, er i samme DB og kommer i samme meldingsstruktur | Årsdatafiler frem til 2015, deretter rene DB forekomster | Tertialvis |  | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP).  API integrasjoner i fremtiden? Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 2 |
| Kommunalt pasient- og brukerregister  KUHR | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2017-08-25-1292) |  | Ca. 50 millioner episoder i året / omtrent hele befolkningen |  | Full historikk tilbake til hjemmel 01.07.2016 | Hver natt fra KUHR, kan ta 14 dager fra lege til NAV + tid til vedtak, normalt samme dag. | Kontrollert av NAV i forhold til organisatoriske/økonomiske forhold. | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP). Potensielt API integrasjoner i fremtiden. Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 1 |
| Kommunalt pasient- og brukerregister  IPLOS | Hdir | [Informasjonsmodell](https://www.helsedirektoratet.no/tema/statistikk-registre-og-rapporter/helsedata-og-helseregistre/informasjonsmodell-og-meldinger) | helseregisterloven §11, [Forskrift](https://lovdata.no/dokument/SF/forskrift/2017-08-25-1292) |  |  |  |  | En gang i året. |  | Filoverføring pr i dag (via meldingsutveksling EDI (AMQP; SMTP). Potensielt API integrasjoner i fremtiden. Ligger i databaser/datavarehus i dag | DB/XML/CSV/API – avhengig av volum | Infrastruktur hos NHN | 1 |
| Dødsårsaksregistret | FHI | Informasjon om dødsårsak.  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrr/) | Helseregister-loven §11 | Overføres i tråd med fryste datasett (2-3 ganger per år) | Ca. 1,5 millioner personer. | Ca. 10 GB | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. Utledede variabler vil endres. Utarbeider 2-3 fryste datasett per år. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Statistisk korrekt. | Filoverføring | CSV | Driftes hos NHN og er på helsenettet. | 1 |
| Medisinsk fødselsregister | FHI | Svangerskap, Fødsel, Fødte og Fødende. Inkluderer nemndbehandlede aborter  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrr/) | Helseregister-loven §11,  Medisinsk fødselsregisterforskriften | Overføres i tråd med fryste datasett (2-3 ganger per år) | Ca. 3.mill fødte | Ca. 25 GB | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. Utledede variabler vil endres. Utarbeider 2-3 fryste datasett per år. |  | Filoverføring | CSV | Driftes hos NHN og er på helsenettet. | 1 |
| Abortregisteret | FHI | Svangerskap, begjæring om avbrudd og eventuell nemndbehandling  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrr/) | Abortregister-forskriften | Overføres i tråd med fryste datasett (Årlig) | Ca. 650,000 begjæringer | Ca. 1 GB | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. Utarbeider årlige fryste datasett. |  | Filoverføring | CSV | Driftes hos NHN og er på helsenettet. | 3 |
| Hjerte- og karregisteret | FHI | Behandling av pasienter i spesialisthelsetjenesten, knyttet til hjerte- og kardiagnoser, samt dødelighet  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrr/) | Helseregister-loven §11,  Hjerte- og karregisterforskriften | Overføres i tråd med fryste datasett (Årlig) | Ca. 5.5 millioner episoder | Ca. 10 GB | Inneholder fullt datasett for hver overføring. | Oppdatert en gang per år fra NPR, med historiske endringer og nye tilfeller. Utledede variabler vil endres. Utarbeider årlige fryste datasett. |  | Filoverføring | CSV | Driftes hos NHN og er på helsenettet. | 2 |
| SYSVAK | FHI | Vaksiner og vaksinand  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrr/) | Helseregister-loven §11,  SYSVAK-registerforskriften | Må vurderes | Ca. 30 mill. vaksinasjoner | Ca. 35 GB | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. Opererer ikke med fryste datasett. |  | Filoverføring | CSV | Driftes hos NHN og er på helsenettet. | 2 |
| Kreftregistret insidensregister | Kreft-registeret | Diagnosetidspunkt  Link til metadata-beskrivelse: [Link](http://hrr.uit.no/hrrpilot/index/en/HRR/HRR.d.1/KREFTREGISTERET/fStudy/KREG) | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Cancer in Norway | Ca. 1,8 millioner krefttilfeller for 1,5 millioner pasienter | Ca. 3 GB | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Kompletthet på 99% | Filoverføring | CSV | Driftes av Kreftregisteret. Er på helsenettet. | 1 |
| **Grunndata** | | | | | | | | | | | | | |
| Modernisert folkeregister | Direktoratet for e-helse | Personopplysninger, Navn, Adresse, fødsels- og dødsdato. | Folkeregister-loven | Kontinuerlig oppdatering via feed | Alle personer som er, eller har vært bosatt i Norge |  |  | Registeret blir kontinuerlig oppdatert med data fra FREG hos Skatteetaten |  | Hendelsesbasert feed, WebService. | FHIR XML/JSON | NHN | 1 |
| **Nasjonale medisinske kvalitetsregistre - Kreftregistret** | | | | | | | | | | | | | |
| Nasjonalt kvalitetsregister for barnekreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport | Varierer for de ulike kvalitetsregistrene | Varierer for de ulike kvalitetsregistrene | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for melanom | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for kreft i spiserør og magesekk | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for prostatakreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for brystkreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for gynekologisk kreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for lungekreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for lymfoide maligniteter | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Nasjonalt kvalitetsregister for tykk- og endetarmskreft | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer, korreksjoner og nye tilfeller. | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| Polyposeregisteret | Kreft-registeret | Diagnose, behandling og oppfølging | Kreftregister-forskriften §1.7 | Årlig i forbindelse med frys av data ved publisering av Kvalitetsregisterrapport |  |  | Inneholder fullt datasett for hver overføring. | Inaktivt etter 2013 | Kvalitetssikret data hentet fra datavarehus. Kvalitetssikret for forskningsformål. Komplett svært høy, men forskjellig for de ulike kvalitetsregistrene | Filoverføring | CSV | Driftes av Kreftregisteret | 3 |
| **Nasjonale medisinske kvalitetsregistre - OpenQreg** | | | | | | | | | | | | | |
| HISREG (Nordisk register for hidradenitis suppurativa) | UNN HF | Internasjonalt kvalitetsregister. Registrerer data om pasient, behandling, livskvalitet og oppfølging av pasienter med hudsykdommen hidradenitis suppurativa.  Link: <https://www.kvalitetsregistre.no/registers/nordisk-register-hidradenitis-suppurativa> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 5000 pasienter | Ca. 10 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes for tiden hos Helse Nord IKT og er på helsenettet. Skal i 2019 flyttes til NHN. | 3 |
| Muskelregisteret (Norsk register for arvelige og medfødte nevromuskulære sykdommer) | UNN HF | Nasjonalt kvalitetsregister. Data om pasienter med genetisk betinget sykdom i muskulatur, ryggmarg eller perifere nerver.  Link: <https://www.kvalitetsregistre.no/registers/norsk-register-arvelige-og-medfodte-nevromuskulaere-sykdommer> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 5000 pasienter | Ca. 1 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| Nakke (Nasjonalt kvalitetsregister for ryggkirurgi, Degenerativ Nakke) | UNN HF | Nasjonalt kvalitetsregister. Data om pasienter som er operert for degenerative tilstander i nakken.  Link: <https://www.kvalitetsregistre.no/registers/nasjonalt-kvalitetsregister-ryggkirurgi> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 10.000 pasienter | Ca. 5 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos Helse Nord IKT og er på helsenettet. | 3 |
| NoRGast (Norsk register for gastrokirurgi) | UNN HF | Nasjonalt kvalitetsregister. Data for pasienter operert i organer i fordøyelsessystemet.  Link: <https://www.kvalitetsregistre.no/registers/norsk-register-gastrokirurgi-norgast> |  | Anslagsvis ca. 2 ganger i året. | P.t. om lag 25.000 pasienter | Ca. 5 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| NRA (Norsk register for analinkontinens) | UNN HF | Nasjonalt kvalitetsregister. Data om pasienter som sliter med lekkasje av og/eller avføring.  Link: <https://www.kvalitetsregistre.no/registers/norsk-register-analinkontinens> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 1000 pasienter | Ca. 1 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| Rygg (Nasjonalt kvalitetsregister for ryggkirurgi, Degenerativ Rygg) | UNN HF | Nasjonalt kvalitetsregister. Data om pasienter som er operert for degenerative tilstander i ryggen.  Link: <https://www.kvalitetsregistre.no/registers/nasjonalt-kvalitetsregister-ryggkirurgi> |  | Anslagsvis ca. 2 ganger i året. | P.t. om lag 25.000 pasienter | Data er p.t. lagret i to databaser. En med data fra 2006-2019, og en med data fra 2019. Ca. 10 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos Helse Nord IKT og er på helsenettet. | 3 |
| NORIC (Nasjonalt register for invasiv kardiologi) | FHI/Helse Bergen HF | Nasjonalt kvalitetsregister. Data om pasienter og invasive behandlinger i hjertet.  Link: [https://www.kvalitetsregistre.no/registers/norsk-register-invasiv-kardiologi-noric](https://www.kvalitetsregistre.no/registers/norsk-register-invasiv-kardiologi-noric%20) |  | Anslagsvis ca. 2 ganger i året. | P.t. om lag 165.000 pasienter | Data er lagret i 9 sykehusspesifikke databaser. Tilsammen utgjør disse ca. 100 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip)  Det overføres 9 sykehusspesifikke databaser, samt én nasjonal base med alle data fra de 9. | Driftes hos NHN og er på helsenettet. | 3 |
| AblaNor (Nasjonalt register for ablasjonsbehandling og elektrofysiologi i Norge) | Helse Bergen HF | Nasjonalt kvalitetsregister. Registrerer elektrofysiske undersøkelser og ablasjoner. Samler data fra behandling, prosedyre og oppfølging.  Link: <https://www.kvalitetsregistre.no/registers/nasjonalt-register-ablasjonsbehandling-og-elektrofysiologi-i-norge-abla-nor> |  | Kommer i produksjon i 2019. Forventet oppdateringsfrekvens ca. 2 ganger i året. | Ukjent | Ukjent. Antageligvis rundt 10 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| LTMV/LangMek (Nasjonalt register for langtids mekanisk ventilasjon) | Helse Bergen HF | Nasjonalt kvalitetsregister. Data om pasienter som er avhengig av mekanisk pustehjelp, utenfor sykehus.  Link: <https://www.kvalitetsregistre.no/registers/nasjonalt-register-langtids-mekanisk-ventilasjon> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 10.000 pasienter | Ca. 2 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| Smerteregisteret (Nasjonalt kvalitetsregister for smertebehandling) | Helse Bergen HF | Nasjonalt kvalitetsregister. Data om pasienter med særdeles krevende smertetilstander.  Link: <https://www.kvalitetsregistre.no/registers/nasjonalt-kvalitetsregister-smertebehandling> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 5000 pasienter | Ca. 2 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| SOReg (Norsk kvalitetsregister for fedmekirurgi) | Helse Bergen HF | Nasjonalt kvalitetsregister. Data om pasienter og kirurgisk behandling av fedme.  Link: [https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-fedmekirurgi](https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-fedmekirurgi%20) |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 10.000 pasienter | Ca. 5 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| NGER (Norsk gynekologisk endoskopiregister) | Sykehuset i Vestfold HF | Nasjonalt kvalitetsregister. Data om kvinner som har fått endoskopiske gynekologiske operasjoner.  Link: <https://www.kvalitetsregistre.no/registers/norsk-gynekologisk-endoskopiregister> |  | Anslagsvis ca. 2 ganger i året. | P.t. om lag 30.000 pasienter | Ca. 10 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| NorSpis (Norsk kvalitetsregister for behandling av spiseforstyrrelser) | Nordlandssykehuset HF | Nasjonalt kvalitetsregister. Data om pasienter som lider av spiseforstyrrelser.  Link: <https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-behandling-av-spiseforstyrrelser-norspis> |  | Anslagsvis ca. 2 ganger i året. | P.t. mindre enn 1000 pasienter | Ca. 1 MB (kryptert) | Inneholder fullt datasett for hver overføring. | Kontinuerlig oppdatert, med historiske endringer og nye tilfeller. Utledede variabler vil endres. | Validert i henhold til kliniske krav. | Filoverføring (SCP) | Kryptert og pakket SQL (zip) | Driftes hos NHN og er på helsenettet. | 3 |
| **Nasjonale medisinske kvalitetsregistre - eReg** | | | | | | | | | | | | | |
| Nasjonalt Barne og Ungdomsdiabetes-register - eReg\_BDR | NHN/ OUS | Behandlingsdata, for barn/ungdom med diabetes | Journal/ Kvalitet. | Daglig innregistrering/bruk | Ca. 3000 årlige behandlinger fordelt på ca. 20 sykehus. | 500MB | Overfører en og en melding etter hver registrert, også endringsmeldinger. | 1. gang pr. år 10-20 variabler av totalt 450 pr. 2019. | 100% strukturert (Sql). | ebXML HIS:80601 + CSV (adminkataloger) | ebXML ,HIS8061. + mulighet for CSV. | Sentral drift NHN | 3 |
| Nasjonalt CPRN register | NHN/ SVHF | Nasjonalt CP register, ungdom. Oppfølging Behandling. | Journal/ Kvalitet. | Daglig innregistrering/bruk | 500-5000 registreringer pr. år. | 2 GB | Overfører en og en melding etter hver registrert, også endringsmeldinger. | 1.Gang pr. år. Få nye variabler. I dag ca 1000 variabler. | 100% strukturert (Sql). | ebXML HIS:80601 + CSV (adminkataloger) | ebXML, HIS80601. + mulighet for CSV. | Sentral drift NHN | 3 |
| Nasjonalt CPOP register | NHN/ SVHF | Nasjonalt CPOP register, ungdom. Oppfølging Behandling. | Journal/ Kvalitet. | Daglig innregistrering/bruk | 500-5000 registreringer pr. år. | 2 GB | Overfører en og en melding etter hver registrert, også endringsmeldinger. | 1.Gang pr. år. Få nye variabler. I dag ca 500 variabler. | 100% strukturert (Sql). | ebXML HIS:80601 + CSV (adminkataloger) | ebXML, HIS80601. + mulighet for CSV. | Sentral drift NHN | 3 |
| Neonatalregisteret | NHN/ OUS | Nasjonalt Nyfødtmedisinsk neonatalregister | Journal/ Kvalitet. | Daglig innregistrering/bruk | x | x | Overfører en og en melding etter hver registrert, også endringsmeldinger. | 1 Gang pr år, 1200 variabler | 100% strukturert (Sql). | ebXML | ebXML, HIS80601. + mulighet for CSV. | Flyttes fra OUS til Sentral drift NHN 2019 | 3 |
| **Nasjonale medisinske kvalitetsregistre - MRS** | | | | | | | | | | | | | |
| Hjertekirurgi  <https://www.kvalitetsregistre.no/registers/norsk-hjertekirurgiregister> | FHI/HSØ | Nasjonalt kvalitetsregister  Nasjonalt Hjertekirurgiregister.  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 4300 pasienter | 750mb | Kan gjøres som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Hjertestans  <https://www.kvalitetsregistre.no/registers/norsk-hjertestansregister> | FHI/HSØ | Nasjonalt kvalitetsregister  Nasjonalt hjertestansregister Har hendelser med hjertestans prhospitalt og inhopitalt.  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 18200 pasienter siden 26.9.2014 | 550mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Hjertesvikt  <https://www.kvalitetsregistre.no/registers/norsk-hjertesviktregister> | FHI/HMN | Nasjonalt kvalitetsregister  Nasjonalt hjertesviktregister  Samler data for behandling av på hjertesvikt-poliklinikk  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 24000 pasienter siden 01.01.2014 | 1300mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Hjerneslag  <https://www.kvalitetsregistre.no/registers/norsk-hjerneslagregister> | FHI/HMN | Nasjonalt kvalitetsregister  Norsk Hjerneslagsregister  Samler data om alle hjerneslag i Norge  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 100 000 pasienter siden 10.12.2014 | 13500mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Hjerteinfarkt  <https://www.kvalitetsregistre.no/registers/norsk-hjerteinfarktregister> | FHI/HMN | Nasjonalt kvalitetsregister  Norsk Hjerteinfarktregister  Samler data om alle hjerteinfarkt i Norge  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 100 000 pasienter  siden 10.12.2014 | 57700 mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Intensiv  <https://www.kvalitetsregistre.no/registers/norsk-intensivregister> | HV | Nasjonalt kvalitetsregister  Norsk Intensivregister  Samler data om alle pasienter behandlet på norske intensivenheter | Egen konsesjon, fritak fra samtykke | Daglig innregistrering/bruk | 93 000 pasienter siden 16.12.2015 | 27700mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Korsbånd  <https://www.kvalitetsregistre.no/registers/nasjonalt-korsbandregister> | HV | Nasjonalt kvalitetsregister  Nasjonalt korsbåndregister  Samler data om korsbåndoperasjoner | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 1400 pasienter siden 18.12.2015 | 100mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Leddprotese  <https://www.kvalitetsregistre.no/registers/nasjonalt-register-leddproteser> | HV | Nasjonalt kvalitetsregister  Nasjonalt reregister forleddproteser  Samler data om leddproteser | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 1000 pasienter siden 4.08.2017 | 100mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Barnehofte  <https://www.kvalitetsregistre.no/registers/nasjonalt-barnehofteregister> | HV | Nasjonalt kvalitetsregister  Samler data fra barnehoftelidelser | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 200 pasienter  Siden 01.11.2018 | 256mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Norartritt  <https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-artrittsykdommer-norartritt> | HV | Nasjonalt kvalitetsregister  Samler data om Artrittpasienter | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 11400 pasienter  Siden 30.06.2016 | 8400mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| NorVas  <https://www.kvalitetsregistre.no/search?for=norvas> | HN | Nasjonalt kvalitetsregister  Samler data om Vaskulittpasienter  (NB biobanken inngår ikke) | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 1000  pasienter | 600mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| NorKar  <https://www.kvalitetsregistre.no/registers/norsk-karkirurgisk-register-norkar> | FHI/HMN | Nasjonalt kvalitetsregister  Norsk Karkirurgisk register, smaler data om karkirurgi.  Inngår i nasjonalt Hjerte- Kar-register. | Hjerte- Kar- forskriften | Daglig innregistrering/bruk | 22000  pasienter | 4340mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Leppe- Kjeve Gane  <https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-leppe-kjeve-ganespalte> | HV | Nasjonalt kvalitetsregister  Samler data om Leppe kjeve og ganespaltepasienter. | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 10 000 pasienter | 200mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| NorScir  <https://www.kvalitetsregistre.no/registers/norsk-ryggmargsskaderegister-norscir> | HMN | Nasjonalt kvalitetsregister  Norsk register for ryggmarsskadepasienter | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 4000 pasienter siden 29.01.2015 | 930mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Norsk MS-register  <https://www.kvalitetsregistre.no/registers/norsk-ms-register-og-biobank> | HV | Nasjonalt kvalitetsregister  Samler data om multrippel sklerose pasienter  NB Biobanken inngår ikke) | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 9000  Siden 01.07.2014 | 1270mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| NakkeRygg  <https://www.kvalitetsregistre.no/registers/norsk-nakke-og-ryggregister> | HN | Nasjonalt kvalitetsregister  Norsk nakke rygg register NNRR samler data om pasienter med nakke og ryggplager | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 10100  pasienter siden 28.10.2015 | 475mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Nasjonalt Traumeregister  <https://www.kvalitetsregistre.no/registers/nasjonalt-traumeregister> | HSØ | Nasjonalt kvalitetsregister  Samler data om pasienter med utløst traumealarm. | Egen konsesjon, fritak fra samtykke | Daglig innregistrering/bruk | 35 000 pasienter Siden 01.07.2014 | 6100mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Parkinson  <https://www.kvalitetsregistre.no/registers/norsk-parkinsonregister-og-biobank> | HV | Nasjonalt kvalitetsregister  Samler data om Parkinsonpasienter | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 300 pasienter  Siden 13.12.2018 | 100mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). Kvalitetssikres årlig, Validert i henhold til kliniske krav. | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Norsk porfyriregister  <https://www.kvalitetsregistre.no/registers/norsk-porfyriregister> | HV | Nasjonalt kvalitetsregister  Norsk porfyriregister Samler data om Porfyripasienter (5 lidelser) | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 5000 pasienter  Siden  31.05.2016 | 256mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Øre-nese-hals.Tonsille  <https://www.kvalitetsregistre.no/registers/norsk-kvalitetsregister-ore-nese-hals-tonsilleregisteret> | HMN | Nasjonalt kvalitetsregister  Samler data om mandeloperasjoner | Egen konsesjon, samtykke | Daglig innregistrering/bruk | 20000 pasienter  Siden 06.01.2017 | 300mb | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Kvarus  <https://www.kvalitetsregistre.no/registers/nasjonalt-kvalitetsregister-behandling-av-skadelig-bruk-eller-avhengighet-av-rusmidler-kvarus> | HV | Nasjonalt kvalitetsregister  Samler data om spesialisert rusbehandling | Egen konsesjon, samtykke | Daglig innregistrering/bruk |  | Under etablering | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| Nyre  <https://www.kvalitetsregistre.no/registers/norsk-nyreregister> | HSØ | Nasjonalt kvalitetsregister  Samler data om nyresviktpasienter og nyrebipsier | Egen konsesjon, samtykke | Daglig innregistrering/bruk |  | Under etablering | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |
| HofteBrudd  <https://www.kvalitetsregistre.no/registers/nasjonalt-hoftebruddregister> | HV | Nasjonalt kvalitetsregister  Samler data om hoftebruddpasienter | Egen konsesjon, samtykke | Daglig innregistrering/bruk |  | Under etablering | Kan gjøre som enkeltmelding eller bolk med alle data. | 1-2 ganger pr år. | 100% strukturert (Sql). | Kan settes opp med SSIS eller tilsvarende. | JSON, csv, excel, xml, men kan tilpasses. | Sentral drift NHN |  |

### Integrasjon mot Helsenettet

De fleste registrene som skal benyttes i Helseanalyseplattformen forvaltes i dag av aktører som er tilknyttet Helsenettet, enten av registrene selv eller av Norsk Helsenett og registrene er plassert ~~spesielt~~ beskyttede omgivelser med bruk av kryptering, sterkt fysisk og logisk tilgangskontroll, hvor det for eksempel ikke er tillat med tilgang direkte mot internett.

Selve helsenettet er ikke å anse som et sikret nett, og i prinsippet vil trusselbildet være likt internett. Aktører som er tilkoblet har forpliktet seg til å etablere et sikkerhetsnivå etter Normen, samt at Norsk Helsenett mulighet til å regulere hvem som kan kommunisere med hvem gjør at risiko for sikkerhetshendelser reduseres.

Det er viktig at alle nye aktører som kobles til Helsenettet ikke introduserer økt risiko for aktører på Helsenettet, og Norsk Helsenett stiller strenge krav til nye tilkoblinger, blant annet bed at de må forplikte seg til å følge Normen.

For å gjøre data fra disse kildene tilgjengelig på Helseanalyseplattformen, og ivareta beskyttelsesbehovet, må en del kapabiliteter være på plass:

* Overføringskapasitet og kvalitet på forbindelsen må kunne skaleres slik at gjenoppretting er mulig innenfor ønsket tid (Recovery Time Objective, RTO) er mulig, samt sikre at kommunikasjon mellom dataplattform og registre fungerer godt.
* Tilkobling må følge Normen – alle tilkoblinger mot Helsenettet må sikres med minst 2 uavhengige tekniske tiltak (Faktaark 20c, Normen). Soner som inneholder personopplysninger skal aldri kunne aksessere Internett tjenester direkte, kun via proxy hvor tilgang kan begrenses.

For å koble seg til Helsenettet, må virksomheten dokumentere at man har etablert en sikkerhetsarkitektur som sikrer at kun autorisert personell kan få tilgang til helse- og personopplysninger, og sikkerhetsarkitekturen må godkjennes av NHN før tilkobling.

#### Godkjenning og oppfølging

For at en ekstern tjeneste skal få tilgang til å kommunisere med tjenester i Helsenettet forutsettes det at man kan kontrollere trafikken som kommer inn mot nettet. Det er derfor et krav om at slik trafikk skal gå via dedikerte kanaler som Norsk Helsenett har kontroll på.

Norsk Helsenett (NHN) kontrollerer hvem som kan benytte dedikerte kanaler inn mot Helsenettet. Før en virksomhet får lov til å benytte koblingen gjøres det en sikkerhetsmessig vurdering av den tekniske løsningen som er satt opp hos leverandøren. Dersom løsningen er satt opp i henhold til kravene fra Norsk Helsenett gjøres det en åpning inn mot Helsenettet.

Kommunikasjon fra Helseanalyseplattformen mot Helsenettet må termineres i et fast punkt inn mot NHN, og videre kommunikasjon internt i Helsenettet mot de forskjellige registrene forutsettes implementert av NHN.

Det er også viktig at virksomheten har prosesser på plass for å implementere og følge opp sikkerheten ved en slik tilkobling. Prosessene og den tekniske løsningen vil være tema for gjennomgang ved eventuelle tilsyn og revisjoner, og vil innbefatte leverandøren så vel som deres underleverandører.

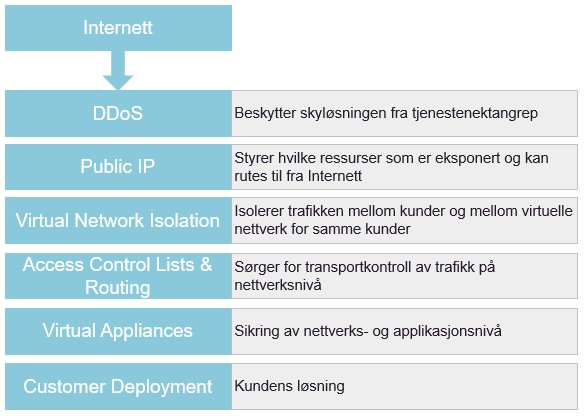
Krav til intern revisjon og forventninger til testing er nærmere beskrevet i kvalitetskravene under kapittel 7, spesielt Sikker utvikling og forvaltning (kapittel 7.5.7).

Leverandøren plikter å følge Norm for informasjonssikkerhet i helse- og omsorgssektoren[[8]](#footnote-9) ved tilkobling til Helsenettet.

#### Overordnet nettverkssikkerhet

For å koble en ekstern tjeneste til Helsenettet vil det være nødvendig å benytte flere lag med sikkerhet for å sikre tilgang til selve tjenesten, men også kontrollere trafikken til helsenettet. Eksterne tjenester sikres etter de samme krav som en tradisjonell løsning med perimeternettverk for å eksponere tjeneste-endepunkter og segmentering/nettverkssikkerhet for å beskytte de indre delene av løsningen.

En generisk grafisk fremstilling av en tjeneste med ulike sikkerhetsmekanismer illustreres under i Figur 10: Sikkerhetsmekanismer.



Figur 10: Sikkerhetsmekanismer

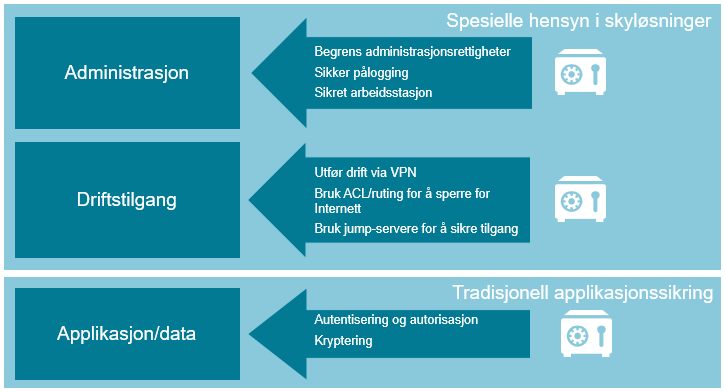
Flere leverandører av eksterne tjenester har dokumentert sine respektive referansearkitekturer. Til tross for at navnestandardene på enkelte av komponentene varierer vil modellen ovenfor være gjenkjennelig.

Det finnes flere måter å oppnå tilstrekkelig sikkerhet på og sikre at det er kontroll på trafikken som sendes inn til Helsenettet~~.~~ Det forventes at leverandøren kan tilby og beskrive en helhetlig sikkerhetsmodell for tilgang til Helsenettet.

#### Tilgang for brukere med utvidede rettigheter

For leverandørens personell med drifts- og vedlikeholdsoppgaver er det viktig at det innføres sikkerhetstiltak for brukere som administratorer eller andre med utvidede rettigheter i tillegg til vanlig tilgang for brukere av løsningen.

Eksempler på hensyn som må adresseres i eksterne tjenester i tillegg til forslag til sikkerhetstiltak illustreres under i Figur 11.



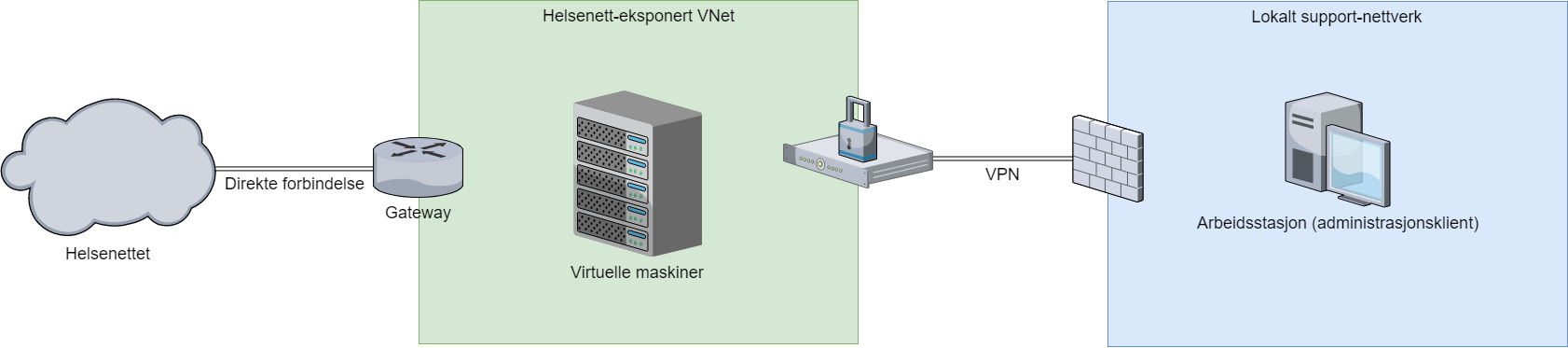
Figur 11: Sikkerhetshensyn og tiltak

#### Administrasjon, drift og fjerntilgang

Administrasjon av eksterne tjenester utføres ofte via både web-baserte administrasjonsgrensesnitt, og administrasjon av selve tjenestene eksempelvis via RDP, API, SSH eller lignende. Dette kan utgjøre en risiko for sikkerheten i løsningen ettersom administrasjonsgrensesnitt for eksterne tjenester ofte er tilgjengelig via Internett.

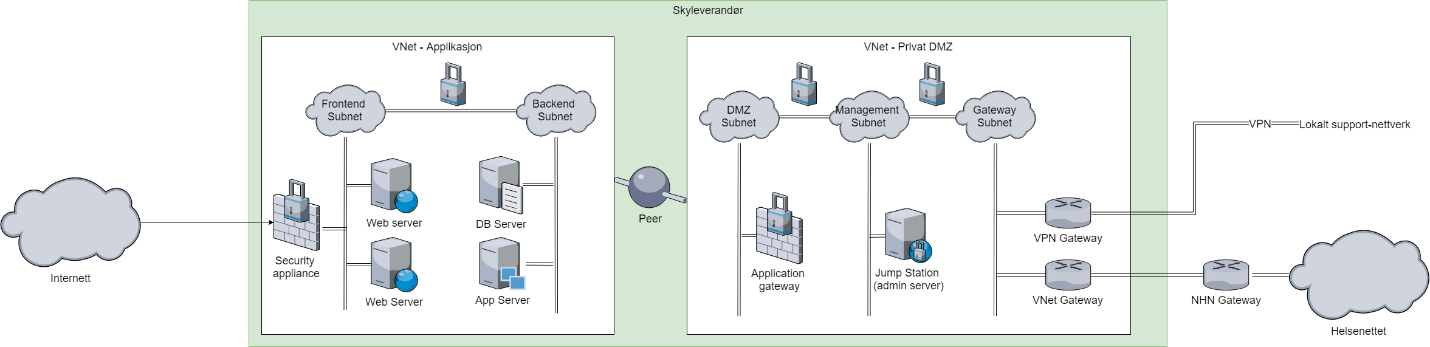
Slike administrasjonsgrensesnitt bør sikres slik at de ikke er tilgjengelig direkte fra internett, men kun fra en arbeidsstasjon som er sikret på samme måte som en arbeidsstasjon som håndterer sensitiv informasjon.

En mindre, konseptuell løsningsmodell illustreres i Figur 12



Figur 12: Konseptuell sikkerhetsmodell

I et mer komplisert design (se Figur 13) bør hver del av tjenesten segmenteres opp mot sensitivitet og bruksområde. Ved administrasjon av tjenestene bør man unngå direkte kommunikasjon mot tjenestene, men benytte VPN eller dedikerte virtuelle maskiner eller grensesnitt som er lokalisert sammen med de eksterne tjenestene.



Figur 13: Konseptuell sikkerhetsmodell med segmentering

Ved å etablere en slik løsning kan både kommunikasjonskontroll og autentisering utføres før tilgang til administrasjonsgrensesnitt tillates.

## Antatt nødvendige tekniske kapabiliteter

For å kunne realisere data- og analyseplattformen er det etablert ett forslag til tekniske kapabiliteter som Helsedataprogrammet tror er nødvendige for å realisere Helseanalyseplattformen. Under er en illustrasjon på disse:



Figur 14: Illustrasjon over viser 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 |
| Data1 | Lagring av strukturerte data | Den tekniske plattformen må inneholde kapabiliteter for lagring av strukturerte data i form av relasjonsdatabaser, NoSQL m.fl. |
| Data2 | Lagring av ustrukturerte data | Den tekniske plattformen må inneholde kapabiliteter for lagring av ustrukturerte data, som dokumenter, bilder, video, lyd m.fl. |
| Data3 | 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 registervariabler mot en eller flere informasjonsmodeller. |
| Data4 | 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. |
| Data5 | 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. |
| Data6 | Metadataforvaltningsverktøy | Den tekniske plattformen bør inneholde verktøy for forvaltning av metadata. Denne bør kunne samspille med HealthTerm, 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 Helseanalyseplattformen kan kobles med metadata. |
| Data7 | 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. |
| Data8 | 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. |

### Informasjonssikkerhet og personvern

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

|  |  |  |
| --- | --- | --- |
| ID | Kapabilitet | Beskrivelse |
| Sik1 | Sporing og logging | Den tekniske løsningen må tilby detaljerte sporingsmuligheter og logging for all bruk av plattformen.  Logg for personvernformål må skilles fra aksess logg/sikkerhetslogg, logger må sikres, og tilgang til logger må være kontrollert og basert på autorisasjon. |
| Sik2 | Tilgangsstyring | Den tekniske løsningen må ha mulighet for å skille mellom ulike brukergrupper, for eksempel ved å benytte rollebasert tilgangskontroll (RBAC) eller dynamiske modeller som attributt-basert (ABAC), for eksempel XACML.  Tilgangsrettigheter må kunne modelleres slik at tilgang kun gis for de som skal ha tilgang, uavhengig av autentiseringsmetode. |
| Sik3 | Sertifikat- og nøkkelhåndtering | Den tekniske løsningen må tilrettelegge for sikker administrasjon/håndtering av innloggingsdetaljer, sertifikater og krypteringsnøkler. |
| Sik4 | Kryptering av data | Den tekniske løsningen må kunne 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. Kryptering må kunne ivareta variert behov, inkludert kryptering av data som skal beskyttes i minst 50år. |
| Sik5 | Segmentering og soneinndeling | Den tekniske løsningen må 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. |
| Sik6 | Informasjonsklassifisering | Den tekniske løsningen må ha funksjonalitet for å klassifisere data og informasjon på ulike nivåer. |
| Sik7 | Datalekkasjebeskyttelse | Den tekniske løsningen må ha evne til å oppdage og forhindre både tilsiktet og utilsiktet datalekkasje(DLP – Data Loss Prevention/Data Leakage Prevention) |
| Sik8 | Sårbarhetshåndtering | Den tekniske løsningen må ha funksjonalitet for å oppdage, styre og håndtere tekniske sårbarheter og svakheter (Vulnerability management). |
| Sik9 | Detektere ondsinnet programvare | Den tekniske løsningen må ha kapabilitet til å oppdage, hindre og detektere ondsinnet programvare, og bør støtte både signatur, oppførsels- og anomalibaserte deteksjonsmekanismer. |
| Sik10 | Konfigurasjonskontroll | Den tekniske løsningen må tilby en oversikt over og kontroll over konfigurasjon av all maskinvare og programvare og sikre at innstillinger kun kan endres ved å følge et endringsregime, og at uautoriserte endringer i konfigurasjon detekteres og blokkeres.  Løsningen må fortløpende kunne produsere dokumentasjon som omhandler den tekniske konfigurasjonen av informasjonssystemene. |
| Sik11 | Sikkerhetskopiering og arkivering | Den tekniske løsningen må tilby funksjonalitet for sikkerhetskopiering og arkivering av data, informasjon, samt konfigurasjon av applikasjoner og tilhørende integrasjoner. Sikkerhetskopier må kunne tilgjengeliggjøres både logisk i form av speiling så vel som fysisk, dvs. fjernlagring av fysiske backupmedia. |

### 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 |
| An1 | 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 bør også være mulig å benytte analysepakker fra eksempelvis CRAN og Python Package Index. |
| An2 | Eksterne analyseverktøy | Den tekniske plattformen bør legge til rette for bruk av tredjeparts eksterne analyseverktøy iht. et økosystem tankegang der tredjeparts aktører kan tilby sine analyseverktøy eller –tjenester gjennom plattformen. |
| An3 | 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. |
| An4 | 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. |
| An5 | 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. |
| An6 | 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 |
| Int1 | 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, sikre og overvåke data pipelines. |
| Int2 | Verktøy for datakvalitetsregler | 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. |
| Int3 | 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. |
| Int4 | 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.  API management løsning bør støtte kryptering av trafikk, på transport og meldingsnivå.  API management bør støtte sikkerhetsfunksjonalitet. |
| Int5 | 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 |
| Adm1 | 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. |
| Adm2 | 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. |
| Adm3 | Beregne pris på analyserom | Den tekniske plattformen bør ha mulighet til å kunne beregne pris for de tjenestene som en sluttbruker ønsker å benytte. |
| Adm4 | 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. |
| Adm5 | Kundekatalog | Den tekniske plattformen bør ha mulighet for å kunne vedlikeholde en kundekatalog med de aktørene som benytter Helseanalyseplattformen sine tjenester. |
| Adm6 | Leverandør/ partnerkatalog | Den tekniske plattformen bør ha mulighet for å kunne vedlikeholde en leverandør katalog med de aktørene i økosystemet som tilbyr tjenester på Helseanalyseplattformen. |
| Adm7 | 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. |
| Adm8 | 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 Helseanalyseplattformen. Det må også være mulig for innbygger å be om å bli slettet. |
| Adm9 | 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. |
| Adm10 | 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. |
| Adm11 | 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). |
| Adm12 | Administrasjon av dataprodukter | Den tekniske plattformen må ha støtte for å administrere dataprodukter. Det må være mulig å knytte metadata til dataproduktet, og kunne publisere disse i en katalog som gjør det enkelt for potensielle konsumenter å finne relevante dataprodukter. Det bør være mulig for en dataleverandør å knytte dataprodukt mot en lisens som regulerer bruk av data, samt eventuelle kommersielle betingelser. |
| Adm13 | 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 dataprodukter og 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. |
| Adm14 | 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 |
| Inf1 | Kjøremiljø for containere | Den tekniske plattformen bør tilby kjøremiljø for containere som er tilgjengelig for sluttbrukere av analyserom. |
| Inf2 | Monitorering av infrastruktur og applikasjoner | Den tekniske plattformen må ha mulighet for å måle ytelse, responsivitet etc. |

### 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 |
| Utv1 | 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). |
| Utv2 | Integrasjon mot code repositories | Den tekniske plattformen bør ha mulighet for integrasjon mot kildekode repositories (for eksempel GitHub). |

# Kvalitetskrav

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

Vi har gruppert kvalitetskravene i følgende kategorier:

* Ytelse
* Kompabilitet
* Brukskvalitet
* Robusthet
* Informasjonssikkerhet og personvern
* Vedlikeholdbarhet
* Portabilitet

Disse er videre beskrevet i kapitlene under. Leverandøren skal besvare kravene under uavhengig av om kravene oppfylles av leverandøren selv, underleverandører og/eller tredjeparter.

## 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 |
| YT1 | Sluttbruker skal oppleve løsningen som rask og responsiv, og ha minst like god ytelse som tilsvarende løsninger innen samme løsningsområde. | Leverandøren bes beskrive forventet responstid for sentrale brukeraksjoner. Brukerinteraksjoner som normalt tar mer enn 1,5 sekunders ventetid skal listes opp. |
| YT2 | Elementer som påvirker ytelse i løsningen samt nødvendig kapasitet for å opprettholde stabil drift, skal være dokumentert | Leverandøren bes beskrive de ulike elementene som påvirker ytelse, samt kapasitet som løsningen er beregnet for å tåle – normalsituasjon og max. |
| YT3 | Ytelse skal testes og verifiseres i et egnet testmiljø for ytelsestesting | Ytelsestest skal innfri avtalt baseline for ytelse, i motsatt fall må tiltak iverksettes. Leverandøren bes beskrive metodikk, plan og infrastrukturbehov for gjennomføring av ytelsestest. |

## 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 |
| KOMP1 | Løsninger skal være i overensstemmelse med gjeldende lover, forskrifter, retningslinjer og ev. (bransje)bestemmelser | Leverandøren bes bekrefte at løsningen er i overstemmelse med relevante lover og forskrifter som for eksempel:  [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 |
| KOMP2 | Løsninger skal utformes, utvikles, driftes og forvaltes i overenstemmelse med rammeverk for sikker og effektiv elektronisk samhandling og datautveksling | Leverandøren bes beskrive hvordan løsningen utformes for å være iht. til følgende:  [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 |
| KOMP3 | Løsningen skal støtte integrasjon mot og eksponere grensesnitt som fortrinnsvis følger internasjonale og nasjonale standarder | Leverandøren bes beskrive hvordan løsningen tilrettelegger for bruk av grensesnitt som 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)[[9]](#footnote-10). |
| KOMP4 | Løsningen skal støtte nasjonale og internasjonale standarder for kodeverk og terminologi. | Leverandøren bes beskrive hvordan løsningen tilrettelegger for bruk av nasjonale og internasjonale standarder for kodeverk og terminologi. Dette inkluderer SNOMED CT[[10]](#footnote-11), og nasjonalt administrativt kodeverk på volven.no. |
| KOMP5 | 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 forretningslogikk som endret fra en versjon til en annen og dette må være dokumentert.  Leverandøren bes beskrive hvordan man sikrer bakoverkompabilitet ved endring i grensesnitt. |
| KOMP6 | 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  Leverandøren bes bekrefte at grensesnitt/integrasjoner og datautveksling dokumenteres iht. beskrivelsen over. |

## Brukskvalitet

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

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| BRU1 | 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)  Leverandøren bes beskrive hvordan løsningen utformes mtp. universell utforming og e-helses retningslinjer hvor dette er påkrevd. |
| BRU2 | 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.  Leverandøren bes beskrive hvordan løsningen uformes slik at brukeren får støtte til gjennomføring av oppgaver på en trygg og effektiv måte. |
| BRU3 | Kontekstuelt relevant informasjon | Informasjonen som presenteres i løsningene skal oppleves kontekstuelt relevant for brukerens oppgave, rolle og situasjon, og bidra til å redusere usikkerhet knyttet til valg.  Leverandøren bes beskrive hvordan løsningen uformes slik at brukeren får kontekstuell relevant informasjon. |
| BRU4 | 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.  Leverandøren bes beskrive hvordan løsningen uformes slik at informasjonens troverdighet ivaretas. |
| BRU5 | Løsninger skal kunne konfigureres og tilrettelegges for måling av avtalte måleindikatorer for brukskvalitet | Løsningen skal kunne konfigureres med analytiske måleverktøy for brukerbeteende. For eksempel skal brukerens evne til å gjennomføre sin oppgave og til å gjøre informerte og hensiktsmessige valg for sin situasjon kunne måles.  Leverandøren bes beskrive hvordan løsningen tilrettelegges for måling av avtalte måleindikatorer for brukskvalitet |
| BRU6 | Løsninger skal kvalitetssikres gjennom brukertest og/eller andre relevante metoder iht. E-helses retningslinjer, både i utviklingsfasen og løpende etter behov | Leverandøren bes beskrive metodeverk og plan for gjennomføring av brukertest. |

## Robusthet

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

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| ROB1 | 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.  Leverandøren bes lage ett utkast til en kontinuitetsplan for plattformen. |
| ROB2 | 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.  Leverandøren bes lage ett utkast til en gjenopprettingsplan for plattformen. |
| ROB3 | 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.  Leverandøren bes beskrive hvordan løsningen automatisk kan skalere på sentrale parameter ved behov. |
| ROB4 | Deploy uten nedetid | Det bør 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.  Leverandøren bes beskrive løsning for deploy uten nedetid. |
| ROB5 | 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. |
| ROB6 | 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 |
| ROB7 | Dokumentasjon på tilgjengelighet | Tilgjengelighet og responstid må kunne dokumenteres. For dette bør det logges jevnlig tilgjengelighet og responstid. Om det ikke følger med slik logging med plattformen eller andre softwarekomponenter bør det utvikles funksjonalitet for denne typen logging.  Målinger skal utføres fra brukerens lokasjon.  Leverandøren bes beskrive hvordan tilgjengelighet og responstid dokumenteres. |
| ROB8 | Feilhåndtering og logging | Løsningen skal ha innebygde mekanismer for feilhåndtering og logging. Dette gjelder både for funksjonalitet på selve plattformen og ved integrasjon med eksterne komponenter og datakilder. Alle feil skal logges i forhold til definert loggnivå og løsningen skal kunne presentere en oversiktlig logg over feil. Løsningen skal gi fornuftige og forståelig feilmeldinger  Leverandøren bes beskriv hvordan de håndterer og logger feil. |
| ROB9 | Sikkerhetskopiering | Sikkerhetskopering er en sentral komponent i en gjennomrettingsplan, og inkluderer:   * Plan for sikkerhetskopiering og gjennopretting * Test av plan * Hvor lagres sikkerhetskopier (off site) * Logisk og fysisk sikring av sikkerhetskopier * Kryptering av sikkerhetskopier og hvordan de håndtere langsiktig behov for oppbevaring av nøkler.   Leverandøren bes beskrive hvordan de håndterer sikkerhetskopering. |

## Informasjonssikkerhet og personvern

De ikke-funksjonelle kravene opplistet nedenfor omfatter informasjonssikkerhet og personvern. Overordnet innebærer dette krav til håndtering av risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Det innebærer også krav til å ivareta grunnleggende personvernprinsipper, innbyggers rettigheter og virksomhetens håndtering av konsekvenser for personvernet.

Kundens krav til informasjonssikkerhet baserer seg på Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 5.3 ("Normen"), som benyttes av alle aktører som er tilkoblet Helsenettet, og har meget store utbredelse i helsesektoren. Normen dekker områder som styringssystem, risikostyring, personvern og pasientlovgivning.

Ved behov har vi supplert med elementer fra Cloud Security Alliance Cloud Control Matrix (CSA CCM), Center of Information Security Critical Security Controls (CIS CSC), OWASP Application Security Verification Standard (OWASP ASVS).

### Risikostyring

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| RIS1 | Ansvar og organisering av personvern og informasjons-sikkerhet | Arbeidet med personvern og informasjonssikkerhet hos leverandøren skal organiseres og gjennomføres slik at det kommer klart frem hvem som er ansvarlig på ulike områder, og hva de er ansvarlig for.  Leverandøren bes redegjøre for hvorledes de organiserer ansvaret for personvern og informasjonssikkerhet i henholdsvis egen virksomhet og i tilbudt prosjektteam. |
| RIS2 | Sikkerhetsstrategi | Leverandøren skal ha tydelig definerte sikkerhetsmål, personvernerklæringer og strategier. Videre skal leverandøren ha dokumentasjon om internkontroll for sikkerhet og personvern for bruk i egen virksomhet, herunder instrukser, sjekklister og beredskapsplaner for å understøtte arbeidet med sikkerhet i virksomheten og mot kunder.  Leverandøren bes om en overordnet beskrivelse av sine sikkerhets- og personvernmål og strategier. |
| RIS3 | Risikostyring | Leverandøren skal regelmessig gjennomføre risikovurderinger for å evaluere risiko, samt beslutte sikringskrav og -tiltak. Risikovurderingene skal som minimum utføres årlig, og resultatet av disse, samt tilhørende tiltak for risikostyring og håndtering skal på forespørsel gjøres tilgjengelig for tilsynsmyndighet og Kunden.  Leverandøren bes beskrive hvorledes de gjennomfører risikovurderinger og implementerer risikoreduserende tiltak for løsningene de leverer. |
| RIS4 | Revisjon og attestasjon | Leverandøren skal tilby revisjonsmuligheter for Kunden, og bør som et minimum tilby revisjonsprodukter og/eller tredjepartsattestasjoner, eksempelvis basert på ISAE 3000, 3402 eller tilsvarende revisjonsstandarder.  Leverandøren bes beskrive hvorledes de tilrettelegger for at Kunden kan revidere de, samt hvilke revisjons- og attestasjonsprodukter de kan tilby for seg selv og aktuelle underleverandører. |

### Personvernprinsipper

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| PER1 | Lovlig, rettferdig og gjennomsiktig | Løsningen skal tilrettelegge for lovlig, rettferdig og gjennomsiktig behandling av personopplysninger.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om lovlighet, rettferdighet og gjennomsiktighet blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER2 | Formålsbegrensning | Leverandøren skal tilrettelegge for at personopplysninger samles inn for spesifikke, uttrykkelige angitte og berettigede formål, og ikke viderebehandles på en måte som er uforenlig med disse formålene.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om formålsbegrensning blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER3 | Dataminimering | Løsningen skal tilrettelegge for at det er mulig å begrense behandlingen av personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om dataminimering blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER4 | Riktighet | Løsningen skal tilrettelegge for at det kan kontrolleres at personopplysninger som behandles er korrekte og at de kan oppdateres om nødvendig. Videre må det være mulig å rette og/eller slette personopplysninger er uriktige.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om riktighet blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER5 | Lagrings-begrensning | Løsningen skal tilrettelegge for at personopplysninger kan anonymiseres eller slettes når formålet de ble behandlet for er oppfylt.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om lagringsbegrensning blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER6 | Konfidensialitet, i og tilgjengelighet | Løsningen skal tilrettelegge for at personopplysninger kan behandles på en sikkerhetsmessig forsvarlig måte slik at opplysningenes konfidensialitet, integritet og tilgjengelighet ivaretas.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om integritet og tilgjengelighet blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |
| PER7 | Ansvarlighet | Løsningen skal tilrettelegge for at den dataansvarlige (Kunden) kan påvise at personvernprinsippene overholdes.  Leverandøren bes beskrive og eksemplifisere hvordan prinsippet om ansvarlighet blir ivaretatt i løsningen, herunder organisatoriske og tekniske tiltak. |

### Den registrertes rettigheter

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| RET1 | Retten til informasjon | Den registrerte har rett til å få informasjon om at det behandles personopplysninger og hvordan disse behandles. Løsningen skal tilrettelegge for at Kunden kan ivareta den registrertes rett til informasjon.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til informasjon kan ivaretas gjennom løsningen. |
| RET2 | Rett til innsyn | Den registrerte har rett til innsyn i hvilke personopplysninger som behandles, herunder logg over bruk. Løsningen skal tilrettelegge for at Kunden kan gi innsyn etter forespørsel.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til innsyn kan ivaretas gjennom løsningen. |
| RET3 | Retten til retting | Den registrerte kan ha rett til å få uriktig personopplysninger rettet. Løsningen skal tilrettelegge for at Kunden kan rette etter forespørsel.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til retting kan ivaretas gjennom løsningen. |
| RET4 | Retten til sletting | Den registrerte kan ha rett til å kreve personopplysninger slettet. Løsningen skal tilrettelegge for at Kunden kan slette personopplysninger når påkrevd.  Leverandøren bes beskrive hvordan den registrertes rett til sletting ivaretas i løsningen, herunder særlig;   * Tekniske løsninger for fysisk og logisk sletting av personopplysninger * Prosessen for sletting * Eventuell funksjonalitet i løsningen som identifiserer når personopplysninger blir behandlet ulovlig * Håndtering av feilaktige slettemeldinger * Hvordan det sikres at permanent sletting er autorisert * Hvordan det sikres at sletting/destruksjon gjennomføres i alle lagringsmedier og dokumenter som inneholder personopplysninger, herunder sikkerhetskopier * Hvordan det sikres at gjenoppretting ikke er mulig. |
| RET5 | Retten til begrensning | Den registrerte har rett til å kreve at behandlingen av personopplysninger begrenses. Dette innebærer at personopplysningene kan lagres, men ikke brukes.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til begrensning kan ivaretas gjennom løsningen. |
| RET6 | Underrettingsplikt | Løsningen skal tilrettelegge for at Kunden kan underrette mottakere som har fått utlevert personopplysninger som er rettet, slettet eller begrenset.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal gjøre det mulig for Kunden å underrette mottakere. |
| RET7 | Retten til dataportabilitet | Kunden kan ha rett til å motta personopplysninger om seg selv i et strukturert, alminnelig anvendt og maskinlesbart format. Løsningen skal tilrettelegge for at persondata kan flyttes fra Helseanalyseplattformen til en ekstern mottaker på en sikker måte.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til dataportabilitet kan ivaretas gjennom løsningen. |
| RET8 | Retten til å protestere | Den registrerte kan ha rett til å protestere mot behandlingen av personopplysninger med den konsekvens at behandlingen må stanses. Løsningen skal tilrettelegge for dette.  Leverandøren bes beskrive tekniske og organisatoriske tiltak som skal sikre at retten til å protestere kan ivaretas gjennom løsningen. |
| RET9 | Samarbeid ved forespørsler fra den registrerte | Leverandøren skal bistå Kunden ved henvendelser fra den registrerte, knyttet til dennes rettigheter.  Leverandøren bes beskrive hvordan slikt samarbeid kan gjennomføres. |

### Ansatte, kompetanse og holdningsarbeid

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| ANS1 | Vilkår og betingelser for ansatte | Leverandøren skal sette vilkår og betingelser for egne ansattes behandling av Kundens personopplysninger.  Som et minimum må slike vilkår og betingelser inkludere en sikkerhetsinstruks, taushetserklæring og virksomhetens sanksjonsmuligheter ved brudd.  Taushetserklæringen må innebærer en absolutt taushetsplikt knyttet til alle helse- og personopplysninger som den ansatte har tilgang til i kraft av sin stiling, samt konfidensiell informasjon om Kundens øvrige virksomhet.  Leverandøren bes beskrive sine vilkår og betingelser, samt de rutiner og prosesser som ivaretar dette. |
| ANS2 | Opplæring, kompetanse og holdningsarbeid | Leverandøren skal iverksette tiltak og beskrive prosesser som ivaretar at alle som har tilgang til og/eller drifter informasjonssystemene og tilhørende informasjon, har tilstrekkelig kunnskap til å bedre bruke systemene for sin rolle og til å ivareta personvernet og informasjonssikkerheten.  Leverandøren skal iverksette tiltak og beskrive prosesser som ivaretar at alle som har tilgang til helse- og personopplysninger behandler disse i samsvar med til enhver tid gjeldende regelverk.  Videre skal leverandøren sikre kontinuerlig kompetansebygging og holdningsarbeid som er tilpasset den ansattes rolle og nivå.  Leverandøren bes beskrive de rutiner, prosesser og tiltak som virksomheten har i tilknytning til opplæring, kompetansebygging og holdningsarbeid. |
| ANS3 | Konsekvenser og sanksjoner ved brudd på taushetsplikten og/eller ulovlig tilegnelse | Leverandøren skal ha rutiner, prosesser og iverksette tiltak for å avdekke brudd på taushetsplikten, herunder ulovlig tilegnelse og utlevering og annen uautorisert bruk.  Leverandøren skal ha retningslinjer som beskriver konsekvenser og sanksjoner ved brudd på taushetsplikten.  Leverandøren bes beskrive hvilke rutiner og prosesser som ivaretar ovennevnte samt hvilke tiltak som iverksettes ved mistanke om brudd på taushetsplikten.  Leverandøren bes beskrive hvilke konsekvenser og sanksjoner virksomheten opererer med ved brudd på taushetsplikten og/eller ulovlig tilegnelse av helse- og personopplysninger. |
| ANS4 | Opphør av ansettelse | Ved opphør av ansettelse eller der ansatte trer ut av prosjektet, skal leverandøren sikre at den ansatte leverer tilbake alle medier (herunder digitalt, papir etc.) som kan inneholde personopplysninger som denne har fått tilgang til i egenskap av sin stilling.  Leverandøren bes beskrive rutiner, prosesser og tiltak som sikrer at ansatte leverer tilbake slike medier. |

### Tilgangsstyring

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| TS1 | Autorisasjon | All tilgang til løsningen, inkludert system-til-system og brukertilgang, skal kun tillates av en autorisert part som har blitt godkjent gjennom en autorisasjonsprosess.  Dette kan være en prosess der en person i en bestemt rolle gis bestemte rettigheter til for eksempel lesing, registrering og sletting, eller der teknisk personell med særskilt behov for tilgang autoriseres for nødvendig tilgang basert på sin rolle.  Leverandøren bes beskrive hvordan løsningen legger til rette for ivaretagelse av prosessen for autorisasjon for både brukere og teknisk personell (admin/support). Beskrivelsen må også dekke hvordan slik autorisasjon kan delegeres til den enkelte eier av analyserommene i løsningen. |
| TS2 | Autorisasjonsregister | All tildeling av autorisasjon skal registreres i et autorisasjonsregister som viser autorisasjon som er gitt og historiske endringer minimum 5 år tilbake i tid. Registeret skal dekke alle tilganger for brukere og administrator eller annet teknisk personell.  Leverandøren bes beskrive hvordan de legger til rette for et autorisasjonsregister som følger gjeldende krav iht. Normens kapittel 5.2.1.1 |
| TS3 | Autentisering | Løsningen skal støtte autentisering via tredjeparts identitetsløsninger (Identity Providers – IdP) som baserer seg på åpne standarder som OpenID Connect og SAML. Eksempler på dette er HelseID og FEIDE.  Autentisering skal utføres på nivå 3 eller 4, og leverandøren bes beskrive hvordan løsningen kan integreres med f.eks. HelseID, FEIDE eller andre basert på OpenID Connect eller SAML og evt. andre standarder. |
| TS4 | Autentisering med utvidede rettigheter | Brukere med utvidede rettigheter og spesiell tilgang som administrator/teknisk personell må også autentiseres for å få tilgang til løsningen.  Leverandøren bes beskrive hvordan de sikrer god autentisering av brukere og roller som ikke vil benytte standard nivå 3 / nivå 4-autentisering. Dette kan inkludere servicepersonell, administratorer eller andre med tilgang til løsningen eller informasjonen som behandles i løsningen |
| TS5 | Rolle- og/eller attributtbasert tilgangsstyring | For å skille på brukere med ulike rettigheter forventes det at leverandøren implementerer og vedlikeholder en fleksibel tilgangsstyring, for eksempel rollebasert tilgangsstyring (RBAC) eller attributtbasert tilgangsstyring.  Løsningen skal også støtte at samme person kan ha flere roller i løsningen og bør også støtte tilgangsstyring basert på brukerinformasjon (attributter eller roller) som oversendes fra en identity provider (IdP) ved autentisering  Leverandøren bes beskrive hvordan løsningen kan støtte slik tilgangsstyring, for eksempel basert på roller som saksbehandler, forsker, registereier og administratorbrukere (teknisk personell/admin) eller basert på attributter fra en ekstern kilde. |
| TS6 | Logging | All tildeling av autorisasjon og tilgang i løsningen skal logges. Det skal være mulig å verifisere disse loggene opp mot autorisasjonsregisteret for å verifisere om tilgangen er autorisert.  Leverandøren bes beskrive hvordan løsningen logger all tilgang til informasjon og hvordan dette kan sjekkes mot autorisasjonsregisteret. Leverandøren må også beskrive hvordan denne informasjonen kan hentes ut av eksterne systemer eller personell hos Kunden som skal ha innsyn i og analysere tilgangsloggene. |
| TS7 | Informasjonssystemer og informasjon skal kategoriseres og klassifiseres | Det er behov for å klassifisere informasjonen i løsningen. Eksempler kan være klassifiseringsnivåer som Åpen, Intern, Skjermet og Sterkt Skjermet.  Dette kan angi sikkerhetsnivået for informasjonen og hvilke tiltak som kreves utenom grunnsikring for å behandle den. Dette kan være for eksempel krav til Data Loss Prevention (DLP) eller andre tiltak.  Leverandøren bes beskrive hvordan løsningen legger til rette for klassifisering av informasjon og hvordan løsningen kan forenkle/automatisere hvilke tiltak som kreves for behandling av informasjon innenfor en klassifisering |

### Fysisk sikkerhet, kryptografi og håndtering av utstyr

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| FY1 | 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.  Leverandøren bes beskrive den fysiske sikkerheten i datasentre som benyttes av løsningen. |
| FY2 | Separasjon av data fra forskjellige kunder | Leverandøren må separere data som tilhører forskjellige kunder og Leverandørens egne data skal separeres fra kundenes data.  Leverandøren bes beskrive sin sikkerhetsarkitektur med hensyn til separasjon av data som tilhører forskjellige kunder. |
| FY3 | Skille mellom person- og helsedata | Ved behandling av helse- og personopplysninger bør løsningen skille ut direkte personidentifiserende kjennetegn fra andre personopplysninger og kryptere disse separat.  Leverandøren bes beskrive hvordan de sikrer et slikt skille. |
| FY4 | Separasjon av test miljø og data fra produksjonsdata | Leverandøren skal ha et separat testmiljø og benytte separate testdata.  Leverandøren bes beskrive hvordan de håndterer testmiljø og testdata. |
| FY5 | Bruk og sletting av Kundens testdata | I enkelte tilfeller kan det oppstå behov for å benytte produksjonsdata til testformål i begrensede perioder. Dette kan eksempelvis forekomme under håndtering av kritiske feil, m.m.  Produksjonsdata skal kun benyttes i slike tester etter avtale. Der det benyttes produksjonsdata til testformål, skal disse slettes etter at test er utført.  Leverandøren bes beskrive sine policyer, prosesser, rutiner, tiltak og sikkerhetsmekanismer for bruk og sletting av kundens produksjonsdata når disse er brukt til testformål. |
| FY6 | Administrasjon av krypteringsnøkler og algoritmer | Leverandøren må sikre at bruk av krypteringsalgoritmer er i henhold til den etablerte NSM standarden[[11]](#footnote-12).  Leverandøren bes redegjøre for hvordan løsningen legger til rette for administrasjon av krypteringsalgoritmer og nøkler. Leverandøren bør også beskrive om de benytter anbefalinger og standarder som for eksempel OWASP ASVS, FIPS 140-2. NSM Cryptographic Requirements 3.1, NIST SP 800-57 eller lignende. |
| FY7 | Bytte av krypterings-algoritmer og -nøkler | Dersom det påvises svakheter i krypteringsalgoritmer eller krypteringsnøkler lekker eller ikke lenger er innenfor gyldighetsperioden, må Leverandøren rekryptere informasjonen med ny og sikker algoritme og/eller nøkler..  Leverandøren bes beskrive hvordan løsningen støtter rekryptering av informasjonen basert på nye algoritmer og nøkler |
| FY8 | Leverandørens oppbevaring og bruk av kryptonøkler | Løsningen må stille sikkerhetsmessig krav til generering, oppbevaring og behandling av nøkler som benyttes for kryptering eller tilgangsstyring.  Løsningen må håndtere at:   * Nøkler generert av Leverandøren opprettes og oppbevares sikkert, for eksempel via en Hardware Security Module (HSM). * Nøkler generert av Kunden som skal benyttes av løsningen skal lagres sikkert (for midlertidig eller permanent bruk i løsningen) * Tilbaketrekking / invalidering / utbytting og nyoppretting av nøkler må støttes * Tilgangskontroll ved bruk av nøkler – det bør være mulig å bestemme hvilke applikasjoner/programmer som får lov til å hente ut spesifikke nøkler fra HSM.   Leverandøren bes beskrive hvordan de vil opprette, motta, og behandle nøkler som benyttes for kryptering eller tilgangsstyring og hvordan de kan håndtere forskjellige type nøkler uten at disse er tilgjengelig for Leverandørens eller underleverandørers personell. Beskrivelsen skal også vise hvordan Kunden og/eller Leverandøren kan trekke tilbake nøkler. |
| FY9 | Kryptering av data som har behov for langsiktig beskyttelse | Helsedata som behandles i løsningen vil kunne ha behov for langsiktig beskyttelse, for eksempel i 50 år. Fordi utvikling i teknologi som kvantedatamaskiner[[12]](#footnote-13) kan medføre at informasjon som er beskyttet med dagens krypteringsmetoder ikke nødvendigvis er trygge innenfor en tidshorisont på 10-30 år.  Leverandøren bes beskrive hvordan de vurderer at en slik 50-års langsiktig sikring av lagret informasjon kan realiseres mot forventet teknologiutvikling innenfor kryptografiområdet, som for eksempel kvantedatamaskiner. |
| FY10 | Krav til fysisk lokasjon på datasentre og supportpersonell | Leverandørens datasentre hvor løsningen skal bygges, samt supportpersonell skal være lokalisert innenfor EU/EØS, og i enkelte tilfeller kan det også stilles krav til at informasjon skal kunne lagres i Norge.  Leverandøren bes beskrive hvilke lokasjoner det er aktuelt å levere løsningen fra, og hvilke funksjoner som leveres fra hver enkelt lokasjon. |

### Sikker utvikling og forvaltning

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| SUF1 | Innebygget personvern og sikker utviklingsprosess | Løsningen skal ha innebygd personvern og personvern som standardinnstilling.  Ved utvikling eller endring av løsningen må Leverandøren følge en anerkjent utviklingsmetodikk som sørger for god sikkerhet og innebygd personvern.  En slik metodikk kan for eksempel inkludere:   * Opplæring * Sikkerhetskrav * Risiko- og personvernvurderinger * Designkrav * Trusselmodellering * Statisk og dynamisk sikkerhetstesting inkludert operativsystem, kode og biblioteker * Overvåkning av konfigurasjon * Oppdatering av beredskapsplaner   Leverandøren bes beskrive hvordan kravet til innebygd personvern, personvern som standardinnstilling og sikker utviklingsprosess ivaretas gjennom utvikling, videreutvikling og bruk av løsningen. Dette omfatter metodikk, tekniske og organisatoriske tiltak, prosesser og rutiner. |
| SUF2 | Revisjon av utviklingsprosjekter | Leverandøren må legge til rette for at kunden kan revidere sikkerhet og personvern i utviklingsløpet og løsningene som utvikles eller endres. Eksempel er vurdering av krav og oppfyllelse mot anbefalingene i OWASP ASVS.  Leverandøren bes beskrive hvordan de tilrettelegger for revisjon av sikkerhet og evt. automatisering av dette i utviklingsløpet |
| SUF3 | 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, både ved etablering og mens løsningen er i drift. |
| SUF4 | 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. |
| SUF5 | Endringsstyring | Endringer i Kundens systemer eller i Leverandørens systemer som berører Kunden må være forankret i en formell endringsprosess som inkluderer alle berørte aktører. Dette skal sikre at endringer skjer på en kontrollert og forutsigbar måte, og er forankret på relevant ledelsesnivå.  Endringsprosessen skal inkludere:   * Identifisering av vesentlige endringer * Planlegging og testing av endringer * Godkjennelsesprosedyre for endringer * Kommunikasjon av plan til aktuelle personer/roller * Reserveprosedyrer om endringen må avbrytes, feiler eller at uønskede hendelser oppstår * Endringslogg med relevante opplysninger * Nød-endring/Håndtering av ekstraordinære endringer hvor endringer må utføres raskt, for eksempel pga. en kjent sårbarhet som medfører akutt risiko, og må fjernes raskt. * Utfasing av tjenester eller komponenter eller erstatning med nye komponenter hos Leverandøren eller underleverandører   Leverandøren bes beskrive hvordan endringsregimet ivaretar sikkerhet og stabilitet, og hvordan Kundens involvering og varsling av endringer kan oppfylles. |
| SUF6 | Konfigurasjonsendring og kontroll | Selve endringen av løsninger, dvs. endringer i utstyr og/eller programvare og tjenester, skal ikke settes i drift før risikoreduserende tiltak er gjennomført.  Eksempler kan være:   * 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, programvare, tjenester eller plattformen generelt. |
| SUF7 | Kontroll på bruk og endringer utført av administratorer / teknisk personell | Bruk av privilegerte brukerkontoer bør begrenses sterkt og overvåkes for å forhindre misbruk og sikre at endringer skjer kontrollert og iht. gjeldende prosedyrer. Endringer som utføres av slike brukere må også logges for senere kontroll. Slike privilegerte kontoer bør også kun benytte godkjente klienter og utsyr som er spesielt godkjent for dette  Leverandøren bes beskrive hvordan tilganger med forhøyede rettigheter håndteres og logges, og hvordan de sikrer arbeidsstasjoner og administrasjonsgrensesnitt som benyttes for slike tilganger. |
| SUF8 | Sikring av Kontainermiljø | Løsningen skal støtte opplasting av kontainere med for eksempel analyseverktøy. Løsningen må derfor sikre at slike kontainere er godkjent sikkerhetsmessig før tilgang til informasjon tillates.  Leverandøren bes beskrive hvordan de sikrer at kontainere som importeres og benyttes på plattformen kan sjekkes for skadelig kode eller andre svakheter og holdes oppdatert før det gis tilgang til løsningen. |
| SUF9 | Jevnlig sikkerhetstesting av løsningen | Før en løsning settes i produksjon eller endres er det viktig at den testes for sårbarheter og svakheter som kan medføre risiko.  Leverandøren bes beskrive hvilke rutiner, prosesser og tiltak de vil benytte for å planlegge og gjennomføre jevnlige sikkerhetstester av løsningen. |
| SUF10 | Sikkerhetsrevisjon av informasjons-systemer | 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 av sin løsning for å sikre at sikkerhetsnivået opprettholdes over tid i drift. |
| SUF11 | Overvåking og logging | Som del av sikker forvaltning er det viktig at løsningen overvåkes for å se på mulige sikkerhetsbrudd eller unormal aktivitet. Alle tilganger som utøves i løsningen skal også logges. Videre skal informasjon fra slik overvåking være tilgjengelig for eksterne analyseverktøy hos Kunden. Logger skal beskyttes med hensyn til Integritet og Konfidensialitet, og skal ikke kunne slettes/manipuleres.  Leverandøren bes beskrive hvordan de vil overvåke løsningen for å sikre stabil og sikker drift, samt hvordan de vil tilgjengeliggjøre informasjonen fra overvåkingen for Kundens analyseverktøy. Beskrivelsen bør også dekke hvordan tilgangslogger kan verifiseres opp mot autorisasjonsregisteret. |

### Kommunikasjonssikkerhet

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| KOM1 | Beskyttelse av informasjon under transport, lagring og prosessering | 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. |
| KOM3 | Sikker tilkobling til Helsenett (registre) | Løsningen skal behandle og overføre informasjon som i dag kun er tilgjengelig innenfor Helsenettet. Dette krever at løsningen sikres for å unngå at uønsket trafikk kan nå andre tjenester på helsenettet.  Leverandøren bes beskrive hvordan en sikker tilkobling til Helsenettet kan implementeres, herunder:   * Sikker overføring og tilkobling mot Helsenettet * At kun godkjent kommunikasjon kan nå Helsenettet via løsningen * Unngå at andre kunder på en delt plattform kan få tilgang til helsenettet * Kapasitet ved overføring av store filer |
| KOM5 | Sikkert datamottak | Løsningen må støtte mottak av store datafiler i et sikkert data mottak. Dette kan for eksempel være store datafiler på 100GB. Ved mottak av slike filer er det viktig at løsningen analyserer og vurderer sikkerheten ved filen eller informasjonen som overføres før den sendes videre inn i løsningen eller til et analyserom.  Leverandøren bes beskrive hvordan de kan realisere et sikkert datamottak. |
| KOM6 | Transportrute for datatrafikk | Ved bruk av geografiske distribuerte datasenter kan det i noen tilfeller være nødvendig å kjenne til detaljer om hvorledes datatransporten skjer, eksempelvis for å sikre redundante oppkoblinger ikke deler samme fysiske transportrute, eller for å sikre at data ikke transporteres via uønsket tredjepart.  Leverandøren bes beskrive hvordan de tilgjengeliggjør informasjon om fysiske og logiske transportruter for datatrafikk. |

### Håndtering av personvern- og informasjonssikkerhetsbrudd

|  |  |  |
| --- | --- | --- |
| ID | Kvalitetskrav | Beskrivelse |
| HPI1 | Avvikshåndtering | Leverandøren skal ha rutiner for å sikre at ansatte rapporterer oppdagede avvik til nærmeste leder eller annet utpekt person/organ. Ved rapportering skal det foretas innsamling av fakta om hendelsesforløp, og gjennomføres en vurdering av korrigerende tiltak. Ved gjentatte avvik skal det gjennomføres en ny risikovurdering.  Leverandøren bes beskrive sitt system for avvikshåndtering for personvern og informasjonssikkerhet. |
| HPI2 | Overvåkning av trusselnivå | Leverandøren bør sørge for at informasjon om aktuell sikkerhetsstatus samt mulige endringer i risikonivået Kontinuerlig gjøres tilgjengelig for Kunden, slik at kan oppfylle sitt behov for sikkerhetsstyring.  Leverandøren bes beskrive hvordan de overvåker trusselnivået. |
| HPI3 | 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 uautorisert bruk.   Leverandøren bes beskrive hvordan de vil etablere hendelsesregistrering i løsningen, og hvorledes disse sikres. |
| HPI4 | Kontinuerlig deteksjon av sikkerhetstruende hendelser | Leverandøren bør sørge for kontinuerlig deteksjon av sikkerhetshendelser, evne til å varsle/integrere med hendelseshåndteringsprosesser og varslingsrutiner hos leverandør og kunde. Leverandøren må kunne følge de nødvendige lovkrav, inkludert bevissikring og uttrekk/eksportering av logger, samt mulighet til å utføre gransking etter hendelser.  Leverandøren bes beskrive hvordan de støtter deteksjon av sikkerhetshendelser, samt hvordan de legger til rette for hendelseshåndtering. |
| HPI5 | Beskyttelse mot tjenestenektangrep | Den tekniske plattformen må ha mekanismer for å beskytte mot applikasjonsbaserte- og nettverks-baserte tjenestenektangrep.  Leverandøren bes beskrive hvordan de kan håndtere tjenestenekt-angrep mot plattformen. |
| HPI6 | Klassesikring | For å tilpasse sikkerhets-nivået til den type informasjon som skal ligge i (f.eks.) et analyserom må det finnes sikkerhetsmekanismer tilpasset klassifisering. For rom som kan inneholde SKJERMET eller STERKT SKJERMET informasjon vil for eksempel Normen ikke tillate direkte kommunikasjon mot internett baserte tjenester.  Leverandøren bes beskrive hvordan sikkerhetstiltak i for eksempel et analyserom kan tilpasses klassifisering av informasjon som skal tilgjengeliggjøres i rommet. |
| HPI7 | Datalekkasje-beskyttelse | Leverandøren må sørge for at det er mulig å blokkere og/eller detektere om data sendes ut fra plattformen uautorisert.  Leverandøren bes beskrive hvordan deteksjon av data lekkasje kan oppdages og/eller stoppes. |
| HPI8 | Samarbeid mellom leverandør og kunde ved brudd på personvernet | Ved brudd på personvernet som har medført konsekvenser for den registrerte skal Kunden varsles om bruddet øyeblikkelig, slik at Kunden kan melde avviket til Datatilsynet innen 72 timer.  Leverandøren bes beskrive sine rutiner for underretting til Kunden. |
| HPI9 | Underretting til den registrerte | Den registrerte skal varsles så raskt som mulig dersom et avvik, personopplysninger på avveie, medfører en høy risiko for den registrertes rettigheter og friheter.  Leverandøren bes beskrive sine rutiner for underretting av den registrerte. |

## 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 |
| VH1 | 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. |
| VH2 | 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. |
| VH3 | 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. |
| VH4 | 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)   Leverandøren bes bekrefte at løsningens system- og driftsdokumentasjon utarbeides iht. god praksis. |
| VH5 | 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   Leverandøren bes bekrefte at løsningens forvaltningsdokumentasjon utarbeides iht. god praksis. |
| VH6 | Løsningen skal tilrettelegges for automatisert verifisering/testing | Automatisert testing gjør det lettere og raskere å utvikle ny kode.  Leverandøren bes bekrefte at løsningens tilrettelegges for automatisert verifisering/testing. |
| VH7 | 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.  Leverandøren bes beskrive metode og plan for utfasingsregime. |

## 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 |
| PORT1 | Løsningens krav til teknisk plattform og arkitektur og bruk av ulike miljøer, skal være dokumentert | Leverandøren bes beskrive krav til teknisk plattform og arkitektur. Dette inkluderer avhengigheten i oppsett av test- og driftsmiljøer eller komponenter i disse slik som bruk av database, fysisk/virtuelt infrastruktur, mellomvare og lisenser. |
| PORT2 | Bruk av proprietært utstyr, tilbehør og/eller programvare bør unngås | Valg skal begrunnes og dokumenteres. Plattformen som skal etableres bør begrense "vendor lock-in".  Leverandøren bes beskrive i hvilken grad løsningen baserer seg på proprietært utstyr, tilbehør og/eller programvare. |



**Besøksadresse**

Verkstedveien 1

0277 Oslo

**Kontakt**

postmottak@ehelse.no

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. Difis veileder for informasjonsforvaltning i offentlig sektor (orden i eget hus) <https://doc.difi.no/data/veileder-orden-i-eget-hus/> [↑](#footnote-ref-4)
4. <https://www.force11.org/group/fairgroup/fairprinciples> [↑](#footnote-ref-5)
5. <https://ehelse.no/programmer/helsedataprogrammet/bakgrunn-og-organisering-av-helsedataprogrammet/_/attachment/download/848177e4-2daa-444d-a7b3-ce50f9397906:a0c7bb98442d07cf0ede5eed3a66d9129a366b6e/Referansearkitektur%20og%20fellestjenester%20for%20helseregistre%20-%20Sluttrapport.pdf> [↑](#footnote-ref-6)
6. https://lovdata.no/dokument/NL/lov/1992-12-04-126?q=Arkivloven [↑](#footnote-ref-7)
7. For ytterligere informasjon se: <https://www.arkivverket.no/for-arkiveiere/skylagring-og-skanning-i-utlandet?q=skytjenester> [↑](#footnote-ref-8)
8. <https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet> [↑](#footnote-ref-9)
9. <https://www.hl7.org/fhir/> [↑](#footnote-ref-10)
10. <http://www.snomed.org/> [↑](#footnote-ref-11)
11. https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf [↑](#footnote-ref-12)
12. <https://www.nsm.stat.no/globalassets/rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf> [↑](#footnote-ref-13)