Direktoratet for e-helse

Målarkitektur for datadeling i helse- og omsorgstjenesten

Versjon 0.8

HITR 1231 utkast 2020

Tittel:
Målarkitektur for datadeling i helse- og omsorgstjenesten

Rapportnummer:
HITR 1231 utkast 2020

Utgitt:
03/2020

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
www.ehelse.no

Innholdsfortegnelse

Sammendrag

Deling av strukturerte helseopplysninger mellom helsepersonell og med innbygger ved hjelp av datadeling er en ny samhandlingsform som gir helt nye muligheter for å digitalisere helse- og omsorgstjenesten og ta i bruk innovative løsninger. Samtidig stiller en slik digitalisering høye krav til sikkerhet og personvern.

Helse- og omsorgstjenesten har behov for bedre samhandling og løsninger som effektiviserer tjenesten. Plan for utvikling av felles grunnmur[1] peker på at det må legges til rette for innovasjon og næringsutvikling gjennom et økosystem med Felles grunnmur, e-helseløsninger og innovative aktører for å dekke samhandlingsbehovene til helsepersonell og innbygger, men samtidig sikrer at taushetsbelagte opplysninger ikke kommer på avveie.

Målarkitektur for datadeling beskriver behovet for felleskomponenter i Felles grunnmur for digitale tjenester i helse- og omsorgstjenesten som vil være en forutsetning for et levedyktig og sikkert økosystem. Felleskomponentene skal muliggjøre aktørenes etablering av datadeling hvor det skal være en lav terskel og lite byråkrati for dataansvarlige å dele sine helseopplysninger med andre helsepersonell og pasienten selv. I tillegg må aktørene ha tillit til at felleskomponentene ivaretar kravene til sikkerhet og personvern som er pålagt de dataansvarlige.

Realisering av målarkitekturen skal også gjøre det enkelt for leverandører å forstå kravene, få tilgang til dokumentasjon og testmiljøer samt ta i bruk felleskomponentene for enkelt å etablere sikker datadeling.

Målarkitektur for datadeling fokuserer i hovedsak på teknisk samhandlingsevne, men belyser også problemstillinger i det organisatoriske og juridiske laget. For å etablere datadeling som en standardisert samhandlingsform er det behov for å gjennomføre tiltak i alle lag av EIF-modellen, der det semantiske og organisatoriske laget er vurdert som spesielt viktig. Det vil være andre tiltak for datadeling som fokuserer på disse.

Hvilke felleskomponenter må et økosystem for datadeling bestå av? Gjennom arbeidet med målarkitekturen er behovene for felleskomponenter diskutert bredt med både arkitekter fra sektoren og fra nasjonale e-helseløsninger og eksisterende grunnmurskomponenter.

Dette dokumentet beskriver vurderingene som er gjort og de arkitekturvalgene som ligger til grunn for den beskrevne målarkitekturen. Målarkitekturen peker ut en fremtidig ønsket arkitektur og tar ikke for seg hvordan denne arkitekturen kan realiseres. Det er ikke gjennomført kvantitativ kost-/nytteanalyse for målarkitekturen og det forutsettes at dette gjøres før investeringsbeslutning og realisering av felleskomponentene. Målarkitekturen kan derfor sees på som en reguleringsplan for realisering av datadeling hvor hovedformålet er å beskrive nødvendige kapabiliteter og felleskomponenter som bør etableres for datadeling.

I arbeidet med målarkitekturen fremkom det at behovene for felleskomponenter for datadeling skilte seg basert på hvilken aktør og brukertyper som er involvert. Det er tatt utgangspunkt i behovene og de lovmessige rettigheter til innbyggere og helsepersonell. Helsedataområdet er holdt utenfor i denne omgang. Det er definert 4 bruksområder hvor behovene for felleskomponenter er behandlet adskilt for hvert av områdene. De fire områdene er:

1. Sektorens samhandling med grunnmur og nasjonale e-helseløsninger
2. Innbyggers behandling av sine helseopplysninger
3. Samhandling mellom helsepersonell i andre virksomheter

4. Samhandling med helsepersonell og innbyggere lokalt

Hvilke felleskomponenter har hvert bruksområde behov for? Gjennom arbeidet med referansearkitekturen for datadeling har vi identifisert sentrale byggeklosser. Vurdering av disse byggeklossene er i dokumentet inndelt i følgende kategorier:

1. Felles tillitsøkende tjenester inkludert autentisering, autorisering, sperringer, fullmakter og samtykker.
2. Felles API-katalog
3. Felles API managementløsning
4. Felleskomponent for lokalisering av pasientinformasjon
5. Felleskomponent for logging

I tillegg til å beskrive målarkitektur for datadeling beskriver dokumentet hvilke kapabiliteter som må etableres for realisering av datadeling. For de viktigste kapabilitetene er det beskrevet løsningsmønstre som beskriver forretningsprosessene og hvilke felleskomponenter som er involvert i disse prosessene. Løsningsmønstrene er basert på samme metode som Digitaliseringsdirektoratet benytter i sitt arbeid med å beskrive tverrsektoriell datadeling.

To av bruksområdene er i denne versjonen ikke beskrevet fullt ut, da disse områdene trenger mer koordinering med andre prosjekter. For bruksområdet "Samhandling mellom helsepersonell i andre virksomheter" vil forprosjekt for Akson samhandlingsløsning svare ut hvordan løse samhandling mellom virksomhetene i helsesektoren.

1 Innledning

"Den norske helse- og omsorgstjenesten må innrettes etter helsetilstanden i befolkningen. Ettersom befolkningen blir stadig eldre og har mer sammensatte sykdomsbilder sammenlignet med tidligere, må helsetjenesten tilpasse seg en ny hverdag og kravet til samhandling med andre aktører øker[2]."

1.1 Bakgrunn

Direktoratet for e-helse har et overordnet mål om å øke elektronisk samhandling mellom aktørene i helse- og omsorgssektoren. Det er startet en rekke tiltak innenfor området data- og dokumentdeling. Dette arbeidet er prioritert fordi data- og dokumentdeling er samhandlingsformer som tas i bruk på ulike måter innen stadig nye områder innen helse- og omsorgstjenesten. Hensikten er å sikre en koordinert utvikling av datadeling samt økt bruk i hele helse- og omsorgstjenesten. Med det ønsker man en raskere utvikling og gevinster for virksomheter, helsepersonell, innbyggere og leverandørmarkedet, samt unngå behovet om å omfattende opprydding i etterkant på grunn av fragmenterte løsninger med lav samhandlingsevne.

Arbeidet med data- og dokumentdeling startet som en del av program for Felles Infrastruktur og Arkitektur (FIA) og har blitt videreført i divisjon styring og samhandling, seksjon arkitekturstyring. I 2018 ble det publisert en referansearkitektur for datadeling som beskriver en beste praksis for realisering av løsninger som benytter datadeling [1]. Referansearkitekturen inneholder arkitekturprinsipper, begrepsmodell, brukstilfeller, aktører og generiske komponenter og deres sammenheng. Målarkitekturen er basert på dette arbeidet.

1.2 Forankring av arbeidet

Målarkitekturen for datadeling er utarbeidet av et leveranseteam bestående av representanter fra Helsenorge, Kjernejournal, Norsk Helsenett og Direktoratet for e-helse. I tillegg har personell fra relevante prosjekter deltatt i leveransetemaet. Sektoren har blitt involvert via en arbeidsgruppe som har bistått leveranseteamet med faglige og erfaringsbaserte vurderinger, samt anbefalinger i arbeidet med målarkitekturen. Rammene for målarkitekturen, bruksområder, arkitekturvalg med mer har blitt diskutert og vurdert i arbeidsgruppen. Se vedlegg 3 for liste over deltakende virksomheter i arbeidsgruppen.

Det har i 2019 vært gjennomført 7 videomøter og 3 heldagssamlinger med arbeidsgruppen.

1.3 Forvaltning av målarkitekturen

Målarkitekturen vil forvaltes videre av Direktoratet for e-helse. Det planlegges at målarkitekturen oppdateres jevnlig. Det er flere arkitekturtemaer som vi har valgt å utsette med bakgrunn i at arbeidet har avhengig til andre prosjekter eller utredninger som ikke var ferdige når arbeidet med dette dokumentet pågikk. Eksempel på tema som er utsatt er:

"Samhandling med helsepersonell i andre virksomheter" hvor Akson sin rolle i datadeling ikke var klar. Se også kapittel 8 - veien videre for nærmere beskrivelser av hva som det må jobbes mer med.

Gjennom erfaringer fra realiseringsprosjekter vil Direktoratet for e-helse jobbe videre med å utvikle felles krav og retningslinjer knyttet til datadeling i helsesektoren.

1.4 Målgruppe

Målgruppen for målarkitekturen er primært arkitekter og tekniske prosjektledere. Den er også relevant for beslutningstakere, prosjektledere og utviklere innen helse- og omsorgstjenesten.

1.5 Omfang

Målarkitekturen er en beskrivelse av en fremtidig ønsket situasjon, hvor helsesektoren kan dele strukturerte helseopplysninger på tvers mellom virksomheter og omsorgsnivå i et nasjonalt perspektiv. Det er tatt utgangspunkt i behovene og de lovmessige rettigheter til innbyggere og helsepersonell. Ut ifra dette er det beskrevet fire bruksområder for datadeling, se kapittel 3.5 for beskrivelse av disse. Målarkitekturen har fokus på samhandling mellom helsepersonell på tvers av virksomheter og samhandling med innbygger. Det betyr for eksempel at datadeling mellom systemer internt i en virksomhet ikke er en del av omfanget for målarkitekturen. Føringer til arbeidet med målarkitekturen er beskrevet i innledningen til kapittel 6.

Målarkitekturen er bare et av flere tiltak for å realisere datadeling som en samhandlingsform i helsesektoren. For å belyse at samhandlingsutfordringer trenger brede tiltak som dekker juridisk, organisatorisk, semantiske og tekniske problemstillinger har EU utarbeidet "European Interoperability Framework" (EIF) og Digitaliseringsdirektoratet (DigDir) har oversatt dette rammeverket til norsk [3].

Figur 1 viser DigDirs oversettelse av European Interoperability Framework

Målarkitektur for datadeling fokuserer i hovedsak på teknisk samhandlingsevne, men belyser også problemstillinger i det organisatoriske og juridiske laget. For å etablere datadeling som en standardisert samhandlingsform er det behov for å gjøre tiltak i flere lag av EIF modellen, hvor det semantiske og organisatoriske laget er vurdert som spesielt viktig.

Målarkitekturen kan sees på som en reguleringsplan for realisering av datadeling, og målarkitekturen sitt hovedformål er å beskrive nødvendige kapabiliteter og felleskomponenter som bør etableres for datadeling.

1.6 Normeringsnivå

Direktoratet for e-helse publiserer normerende dokumenter som gir rammer og retningslinjer for IKT-utviklingen i helse- og omsorgssektoren, se beskrivelse på ehelse.no [4].

Dette dokumentet har status som veileder, men deler av innholdet kan på sikt være aktuell for høyere grad av normering. Dette kan for eksempel inkludere hvilke funksjoner og data som helseinformasjonsystemer må gjøre tilgjengelig gjennom API, med nærmere spesifikasjon av tekniske og semantiske standarder. Det kan også stilles krav til bruk av nasjonale felleskomponenter ved deling av data. Dette ville da være krav for datadeling og API i e-helseløsninger tilsvarende dagens krav til meldingsutveksling i "Forskrift om IKT-standarder i helse- og omsorgstjenesten" [5].

2 Målbilde for datadeling

Utredningen av Én innbygger – én journal slo fast at *"[det] er behov for at korrekt, nødvendig og relevant informasjon, raskt og effektivt, gjøres tilgjengelig for helsepersonell med tjenstlig behov, uavhengig hvor pasienten har fått helsehjelp før"*. Tilgang til data om en bestemt pasient hos andre aktører og virksomheter er en viktig mulighet til å supplere eventuelle manglende opplysninger, samt å kunne se historikk over tidligere undersøkelser og behandlinger. Datadeling mellom aktører muliggjør overføring av kunnskap på tvers av virksomhetsgrenser og omsorgsnivåer, samt legger til rette for mer effektiv samhandling gjennom pasientforløpet. . Datadeling gjør det mulig å dele utvalgte og strukturerte data til helsepersonell, det vil si dele akkurat den informasjonen som relevant og nødvendig for å gi helsehjelp.

Innbyggere er helsetjenestens viktigste samarbeidspartnere og er en viktig brukergruppe for datadeling. Innbyggere og/eller individer med fullmakt (utover deres lovbestemte krav på innsyn i egne journalopplysninger) kan ha behov for innsyn i egne journalopplysninger og laboratoriesvar for blant annet å:

a) følge egen utredning,
b) kunne foreta selvvalg og samvalg rundt egen behandling,
c) repetere råd og beskjeder som er gitt under konsultasjoner,
d) søke fornyet vurdering, og
e) vurdere om innsyn i dele av journalen skal begrenses for utvalgte virksomheter/helsepersonell.

Innbyggere skal også kunne få tilgang til å se hvilke helsepersonell som har hatt innsyn i deres journalinformasjon. Dette vil bidra til at innbyggere blir tryggere på at deres helseopplysninger behandles på en forsvarlig måte.

Datadeling er deling av og samarbeid om strukturerte data gjennom felles ressurser/tjenester. Målet er at det skal være et felles rammeverk for standardisert deling av og samarbeid om strukturerte data som leverandører av e-helseløsninger kan benytte seg av for utvikling av nye tjenester.

2.1 Nasjonal e-helsestrategi

Dagens samhandling baserer seg først og fremst på sending av elektroniske meldinger. Samtidig er det et økende behov for å ta i bruk nye og andre samhandlingsformer for å styrke pasientbehandlingen, øke pasientsikkerheten og gi innbyggerne innsyn til egne helseopplysninger. Samhandlingsformen datadeling er forankret i Nasjonal e-helsestrategi 2017-2022 [6].

Et av de strategiske områdene i Nasjonal e-helsestrategi 2017-2022 er å bedre sammenhengen i pasientforløpet. Innsatsområde #2.1 i strategien omhandler:

- " Bidra til plan og kontinuitet i ansvarsoverganger".

Innenfor dette innsatsområdet er det definert tre mål:

1. *"Henvisning, saksbehandling og henvisningssvar skjer i én sammenhengende digital arbeidsprosess. Det gir bedre grunnlag for helhetlig administrativ oppfølging av helsehjelp, slik at pasienten får rett behandling til rett tid."*

2. *" Helsepersonell kan raskt, enkelt og sikkert gjøre nødvendige oppslag i pasientopplysninger fra andre behandlingssteder. Dette for å unngå feil, kunne gjenbruke prøvesvar og sikre raskere helsefaglige beslutninger."*

3. *"Pasienter og pårørende med samtykke har innsyn i egne helseopplysninger og kan ta del i administrasjon av forløp. Dette bidrar til mer effektiv planlegging av pasientforløp, og gir innbyggeren større mulighet til å være en informert og aktiv deltaker i behandling."*

De siste to målene er førende for målarkitekturen.

Nasjonal handlingsplan for 2017-2022 [6] omtaler også tiltak for å realisere målene beskrevet over. Følgende tiltak er en del av planen for 2017-2022:

1. Ta i bruk dokumentdeling basert på nasjonal referansearkitektur slik at helsepersonell med tjenstlige behov har mulighet for innsyn i journal i andre virksomheter.
2. Gi innbyggere innsyn i egen journal via Helsenorge og videreutvikle løsninger som setter pasient og pårørende i stand til å ta aktiv del i planlegging av forløp.
3. Prøve ut ulike former for digital dialog og digitale verktøy for felles planlegging av pasientforløp. Med mer dynamiske verktøy for kommunikasjon på tvers av omsorgsnivå får en raskt gjort helsefaglige avklaringer og lagt planer for helhetlige pasientforløp

Målarkitekturen skal understøtte de siste to tiltakene og beskrive den nasjonale arkitekturen for datadeling.

2.2 Plan for utvikling av Felles grunnmur for digitale tjenester i helse- og omsorgstjenesten

I 2018 ble Plan for Felles grunnmur for digitale tjenester i helse- og omsorgstjenesten [11] utarbeidet og publisert. Det overordnede målet for felles grunnmur er definert som:

"Felles grunnmur skal gi betydelig raskere, sikrere og mer kostnadseffektiv digitalisering av helse- og omsorgssektoren, og tilrettelegge for enkel og sikker samhandling på tvers av forvaltningsnivåene og bedre muligheter for innovasjon."

Plan for felles grunnmur definerer følgende resultatmål relatert til datadeling:

> Resultatmål 4: Et felles rammeverk for standardisert deling av og samarbeid om strukturerte data
>
> Resultatmål 7: Tilrettelegge for innovasjon og næringsutvikling

Målarkitektur for datadeling er ett av flere tiltak for å nå disse resultatmålene. Målarkitekturen skal blant annet legge til rette for et økosystem med e-helseløsninger og innovative aktører ved å beskrive hvilke felleskomponenter felles grunnmur må bestå av for å oppnå dette.

3 Datadeling som samhandlingsform

3.1 Hva er datadeling?

Datadeling er en term som tolkes forskjellig i ulike sektorer i Norge. DigDir benytter termen datadeling om alle typer deling av data hvor data ikke setter noen føringer om det er strukturert eller ustrukturert. I helse- og omsorgstjenesten beskriver datadeling en samhandlingsform hvor det benyttes API-er for å dele strukturerte data.

API betegner et grensesnitt i en programvare slik at spesifikke deler av programvaren kan aktiviseres fra en annen programvare (definisjon hentet fra [1]). Vi bruker API i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt i en programvare for andre aktører.

I mange av tjenestens anvendelser av datadeling kan databegrepet knyttes til ulike typer data: Persondata, helseopplysninger om en person, tilstandsdata, aggregerte data, grunndata, strukturerte data, historiske data, sanntidsdata. I dette dokumentet er det fokus på deling av helseopplysninger da dette er taushetsbelagte data hvor anvendelser med slike data trenger et rettslig grunnlag for at en aktør kan behandle dataene.

Innen helse- og omsorgstjenesten finnes det mange behov for å dele informasjon via bruk av API-er:

1. Deling av helseopplysninger for å yte, administrere eller kvalitetssikre helsehjelp
2. Deling av helseopplysninger til innbygger.
3. Deling av administrative grunndata, både felles offentlige grunndata og helsesektor spesifikke grunndata.
4. Deling av helseopplysninger med offentlige etater slik som (men ikke begrenset til) Nav, Helfo, Politiet, Vegvesen, Skatteetaten
5. Deling av helseopplysninger for forsknings- og kvalitetsforbedringsformål

I dette dokumentet dekker vi behovene punkt 1, 2 og 3 ved hjelp av deling av strukturert informasjon mellom ulike aktører gjennom felles ressurser eller tjenester i sanntid.

Aktører i helse- og omsorgstjenesten er i dette dokumentet definert som pasienten selv (eller noen som representerer pasienten) og aktører som er underlagt pasientjournalloven og har krav til å vedlikeholde et behandlingsrettet register. Det skilles i dette dokumentet ikke på private og offentlige aktører.

Begrepet datadeling blir ofte knyttet til API-operasjonen å lese data. DigDir kobler datadeling i første omgang kun til å lese data. Helse- og omsorgstjenesten har flere use case hvor det også er behov for å skrive til andre systemer via API. Tillatelse til å skrive helseopplysninger på tvers av virksomhetsgrenser er juridisk strengt og det må derfor foreligge et rettsgrunnlag for skrive-operasjoner. Eksempler på rettsgrunnlag er databehandleravtale og avtale basert på pasientjournalloven § 9. Teknisk sett har vi sett at behov for felleskomponenter er lik uavhengig av om det er snakk om å lese eller skrive.

3.1.1 Hva er status på elektronisk samhandling i helse- og omsorgstjenesten i dag?

Datadeling til samhandling på tvers av virksomheter benyttes i dag i svært liten grad i helse- og omsorgstjenesten. Hovedvekten av dagens elektroniske samhandling mellom aktørene i helse- og omsorgssektoren er basert på meldingsbasert samhandling. Dette er i stor grad et resultat av mange regionale og kommunale installasjoner av EPJ/PAS og andre fagsystemer. *Veikart for realiseringen av målbildet Én innbygger – én journal [2]* slår fast at samhandlingsbehovet er større enn tidligere antatt og dekkes ikke av meldingsutveksling. Videre skrives det at "*Så lenge ikke alle virksomheter som yter helsehjelp jobber i et felles kjernesystem, vil det være behov for utveksling og deling av data og dokumenter på tvers av virksomheter*". Direktoratet for e-helse forutser at en vesentlig del av samhandlingen mellom spesialisthelsetjenesten og kommunal helse- og omsorgstjeneste vil måtte basere seg på datadeling og dokumentdeling i tillegg til meldingsutveksling.

Meldingsutveksling har flere begrensninger i tilknytning til samhandlingsbehov som sektoren har i dag:

- Legger ikke til rette for oppdatert informasjon om en pasient
- Dårlig egnet for å møte innsynsbehovet for innbyggere
- Er en asynkron samhandlingsform hvor mottakere må være kjent ved sending

Selv om dokumentdeling bidrar til å løse opp i flere av begrensningene forbundet med meldingsutveksling finnes det en rekke behov som avhenger av gjenbruk og deling av strukturerte helseopplysninger gjennom bruk av datadeling.

3.2 Strukturerte data

I dagens elektroniske pasientjournalsystemer (EPJ-er) har det historisk vært benyttet mye fritekst. Fremtidige EPJ-er vil i større grad baseres på strukturerte data eller maskinell tolkning av ustrukturerte data (gjennom f.eks AI) og det vil være enklere å dele data gjennom API-er.

Gjennom standardisering av API-er vil strukturerte data kunne enklere gjenbrukes på tvers. I midlertidig kan strukturerte data ha forskjellig betydning i forskjellig kontekster og det er

behov for standardiserte grensesnitt. Direktoratet for e-helse har anbefalt FHIR som standard for å representere semantikken i datadelingsgrensesnitt på en internasjonalt standardisert måte. Det vil fortsatt være behov for å tilpasse FHIR ressurser til den konteksten de skal brukes i. Ofte snakkes det om at det er behov for tilpasninger på lokalt, regionalt, nasjonalt og internasjonalt nivå. Noen grunnleggende informasjonselementer bør allikevel være likt for alle nivåene. Gjennom standarden International Patient Summary (IPS – EN 17269) defineres et kjernesett av informasjonselementer som er relevant i all helsehjelp og er viktig for kontinuitetene i pasientbehandlingen.

IPS-datasettet ble fastsatt som en europeisk standard i november 2019 og består hovedsakelig av:

- Informasjon om pasienten (f.eks. navn, fødselsdato, kjønn)
- Sammendrag av kliniske pasientdata (f.eks. allergier, implantater, nylige kirurgiske inngrep)
- Informasjon om pasientens medisinbruk
- Metadata om journalen

FHIR beskriver også bruk av helsefaglig terminologi, administrative kodeverk og medisinske klassifikasjonskodeverk som vi omtaler som felles språk. Det er behov for en felles forståelse av informasjonen som deles mellom de som deler helseopplysninger om en pasient. Et felles språk kan bidra til at data kan forstås likt gjennom all helsehjelp som en pasient mottar.

Felles språk brukes derfor i den strukturert informasjonen knyttet til dokumentasjonen som helsepersonell er pliktig til å nedtegne i elektroniske pasientjournaler. Felles språk tar ikke stilling til hvilken informasjon som skal struktureres i EPJ, eller hvordan dette skal gjøres. Direktoratet for e-helse har utarbeidet et målbilde for et økosystem innen kodeverk og terminologi som sektoren har gitt sin tilslutning til [15].

3.3 Tilgang basert på tjenstlig behov og sperring av tilgang

Elektronisk deling av helseopplysninger mellom personell med tjenstlig behov i ulike virksomheter fordrer at man er i stand til å ta stilling til det tjenstlige behovet for tilgang på tvers av virksomhetene. Tilgangskontroll er den mekanismen som innvilger innsyn i helseopplysninger. For at tilgangskontroll på tvers av virksomheter skal kunne skalere til flere virksomheter må det være mulig å ta stilling til det tjenstlige behovet hos den virksomheten som brukeren er ansatt i. I den anbefalte tillitsmodell [10] for data- og dokumentdeling er dette den foreslåtte modell og som sektoren har sluttet seg til.

Å gi tilgang til helseopplysninger som er relevant og nødvendig for å yte helsehjelp til en pasient kan ikke utelukkende bestemmes av rollen til personellet i en gitt virksomhet. Tjenstlig behov kan også være avhengig av at den som ønsker tilgang er med i en behandlingsprosess, svarer på telefonforespørsler fra pasient eller lignende.

Tilgang til sensitive opplysninger kan styres ved at en person gir andre tilgang per område, eventuelt at en hel gruppe kollektivt blir autorisert for all sensitiv informasjon. Dette er en modell som ikke er tilstrekkelig i helse- og omsorgssektoren. Helsepersonells hverdag består av både planlagt arbeid og uforutsette situasjoner som må håndteres der og da. Det er derfor ikke praktisk gjennomførbart at en eksplisitt må autorisere helsepersonells tilgang til en pasients journal når uforutsette hendelser oppstår. Samtidig kan man ikke gi alt helsepersonell, normalt basert på rolle, tilgang til alle helseopplysninger, siden dette raskt vil medføre brudd på taushetsplikten. Internt i helseforetak løses dette ofte ved at det gis en

grunntilgang basert på roller, men at det før åpning av journalen for en spesifikk pasient må avklares hvorfor tilgang er nødvendig (det tjenstlige behovet).

Det er derfor behov for å etablere metoder og regler basert på flere parametere enn rolle slik at det er mulig å styre tilgang til helseopplysninger automatisk.

- ***Det ligger en beslutning til grunn for all helsehjelp***
  En slik beslutning kalles normalt for et besluttet tiltak [13] og er normalt opphavet til det tjenstlige behovet. Dette tiltaket kan være både eksplisitt (for eksempel kommunalt vedtak) og implisitt (for eksempel pasient bestiller time hos fastlegen sin).

  Før en beslutning om å yte helsehjelp kan tas, har helsepersonell behov for å vurdere pasientens helseopplysninger og må da ha tilgang til all relevant informasjon.
- ***Det skal kun gis tilgang til helseopplysninger i forbindelse med gjennomføring av besluttede tiltak***
  Det er i helse- og omsorgtjenesten et krav at det skal kun gis tilgang til helseopplysninger i forbindelse med gjennomføring av et besluttet tiltak.
- ***Enhver tilgang til helseopplysninger skal ha et uttrykkelig angitt og saklig begrunnet formål***
  Lovgivningen legger stor vekt på at enhver behandling av helseopplysninger skal ha et uttrykkelig angitt og saklig begrunnet formål, jf. GDPR art. 5 nr. i bokstav b. Et besluttet tiltak skal derfor alltid knyttes til et eller flere formål.
- ***Helsepersonell skal ikke gis tilgang til flere helseopplysninger enn det som er nødvendig***
  Ved all tilgjengeliggjøring av helseopplysninger gjelder at det ikke skal tilgjengeliggjøres flere opplysninger enn det som er nødvendig for formålet med tilgjengeliggjøringen.
- ***All tilgang skal være tidsbegrenset***
  Når et besluttet tiltak opphører, skal også tilgangen opphøre.
- ***En pasient har rett til å motsette seg helsepersonells tilgang til sine helseopplysninger***
  En pasient kan fremsette krav om sperring av innsyn i hele eller deler av sin journal. En sperring kan gjelde navngitte helsepersonell, grupper eller virksomheter. Alle pasientjournaler skal ha en journalansvarlig. Dersom pasienten har sperret visse journalopplysninger, skal helsepersonell varsles om dette og skal kunne be pasient om innsyn (be om samtykke for innsyn i sperret del). Før en slik innsynsforespørsel gjøres, kan man spørre journalansvarlig om sperrede opplysninger er relevante for det aktuelle tilfellet.

  En pasients rett til å motsette seg tilgang til sine helseopplysninger er i tillegg ikke absolutt. Det følger av pasient- og brukerrettighetsloven § 5-3 tredje ledd og helsepersonelloven § 23 nr. 4, at helseopplysninger kan utleveres tross pasientens motstand dersom tungtveiende grunner taler for dette, for eksempel dersom det er fare for liv eller alvorlig helseskade.

3.4 Åpne API-er

API-er har eksistert i flere titalls år. Når det snakkes om API-er, så kan det ofte misforstås hvor klare API-ene er for bruk av andre. I dette dokumentet omtales API-er som API-er som kan nås via http(s) og som kan benyttes av andre enn virksomheten som eier API-et.

Direktoratet for e-helse har valgt å benytte begrepet "åpne API" for å etablere en felles forståelse og forventninger til hverandre for et API som kan tas ibruk av en annen aktør. Åpne API må ikke forveksles med Åpne data, da helseopplysningene som tilbys gjennom åpne API må sikres for å ivareta krav til informasjonssikkerhet og personvern

Direktoratet har definert Åpne API som: *gjenbrukbare, sikre, godt dokumenterte og tilgjengelige programmeringsgrensesnitt som kan benyttes av alle relevante aktører uten diskriminerende og konkurransevridende vilkår.*

Direktoratet har definert noen retningslinjer for åpne API som skal gi følgende effekter:

1. forebygge delingsmotstand og redusere barrierer mot datadeling
2. legge til rette for forutsigbare, transparente og ikke-diskriminerende vilkår
3. legge til rette for lett tilgjengelig og gratis tilgang til dokumentasjon
4. overordnet å gi en samlet oversikt over grunnleggende rammebetingelser for deling av personopplysninger
5. gjøre det enklere å innføre datadeling som samhandlingsform

Hvordan skal målarkitekturen for datadeling bidra til å etablere et økosystem som tilrettelegger for innovasjon og næringsutvikling?

3.5 Tilrettelegge for innovasjon og næringsutvikling

Resultatmål 7 i Plan for utvikling av felles grunnmur [11] handler om å gjøre byggeklossene i Felles grunnmur tilgjengelige for et bredere utvalg av brukere og aktører, slik at innovasjon i norsk e-helse kan bidra til bedre helsehjelp og i tillegg kan bidra til at norske leverandører kan levere sine innovative løsninger i et internasjonalt marked.

Resultatmålet omfatter tilrettelegging av et økosystem bestående av felles grunnmur, e-helseløsninger og innovative aktører. Et levedyktig økosystem må involvere en hel rekke aktører og tjenester, og dette går ut over hva selve grunnmuren har ansvar for.

Et økosystem må bidra til økt forståelse for krav til datadeling, økt tillit mellom partene og enklere og åpne endringsprosesser for å få tilgang til data. Økosystemet må tilby tjenester og selvbetjeningsløsninger som er attraktive og reduserer tidkrevende involvering fra det offentlige.

Datadeling er i dag i liten grad tatt i bruk som en samarbeidsform i helse- og omsorgstjenesten. I andre sektorer har datadeling bidratt til en stor innovasjonstakt som har medført høy grad av digitalisering. I vårt arbeid med målarkitektur for datadeling har det derfor vært stort fokus på hvordan målarkitekturen kan tilrettelegge for innovasjon og næringsutvikling for å være i stand til å etablere et økosystem.

Målarkitekturen beskriver behovet for felleskomponenter som vil være grunnlaget for etablering av et økosystem.

Når målarkitekturen er realisert, skal det være en lav terskel og lite byråkrati for dataansvarlige å dele sine helseopplysninger med andre helsepersonell og pasienten selv. I tillegg skal det være enkelt for leverandører å forstå kravene, få tilgang til dokumentasjon og testmiljøer samt ta ibruk felleskomponentene som er en del av økosystemet.

En arkitektur kan ikke alene etablere et levedyktig økosystem. I tillegg til insentiver, finansiering, møteplasser for brukermedvirkning og felles styring må et levedyktig økosystem ha en organisasjon som er dedikert til å følge opp økosystemet slik at det blir tatt i bruk. Dette er utenfor scopet av målarkitekturen å beskrive.

4 Relevante lover og forskrifter

I dette kapittelet vil vi trekke frem relevante lover og forskrifter for deling av helseopplysninger mellom personell med tjenstlig behov samt for innbygger.

4.1 Hjemmelsgrunnlag for helsepersonell

Nødvendige helseopplysninger skal være tilgjengelig for den som yter, administrerer eller kvalitetssikrer helsehjelp. Pasientjournalloven § 19 gir derfor en plikt til tilgjengeliggjøring av opplysninger fra behandlingsrettede helseregistre (herunder EPJ etter pasientjournalloven § 8 og samarbeidsløsninger etter pasientjournalloven §§ 9 og 10).

Det fremkommer av pasientjournalloven § 19, 1 ledd at:

" [..] databehandlingsansvarlige [skal] sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte".

Helsepersonelloven § 25 har tilsvarende bestemmelse og det fremkommer at:

"*[…] taushetsbelagte opplysninger [kan] gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp"*.

Helsepersonelloven § 45 sier at:

"*Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient etter denne lov, gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger".*

I dette ligger en plikt for helsepersonell til å gjøre data om en pasient *tilgjengelig* for helsepersonell som skal utøve helsehjelp.

Det er opp til virksomheten selv å vurdere hvorvidt helseopplysningene som ligger lagret i virksomheten tilgjengeliggjøres via datadeling. Dette fremkommer av pasientjournalloven § 19, 2 ledd som sier at

"*det er den databehandlingsansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige"*.

Ny forskrift om pasientjournal har erstattet "Forskrift om tilgang til helseopplysninger mellom virksomheter". Dette innebærer at kravet om å inngå avtale for å kunne tilgjengeliggjøre helseopplysninger i behandlingsrettede helseregistre på tvers av virksomheter opphører. Det er i stedet lagt vekt på risikobasert tilnærming til tilgangsstyring, autorisasjon/autentisering og gode internkontrollrutiner for å avdekke avvik og uberettiget tilgang.

Datadeling legger til rette for informasjonsflyt som tilgjengeliggjør helseopplysninger på en annen måte enn det som er mulig i dag. Det bør derfor etterstrebes å gi tilstrekkelig

informasjon til pasienten om at helseopplysninger deles på tvers av virksomheter der det er nødvendig for å yte forsvarlig helsehjelp.

Pasienten bør også gjøres oppmerksom på retten til å motsette seg informasjonsdeling mellom helsepersonell og konsekvensene av dette. En pasient har etter Helsepersonelloven § 45 rett til å motsette seg informasjonsutveksling mellom helsepersonell, selv om opplysningene er nødvendige for å yte helsehjelp. Dette forutsetter at pasienten gir beskjed om at det ikke er ønskelig at informasjon deles. Krav om aktivitet fra pasienten for å forhindre informasjonsutveksling er begrunnet i at pasienten må kunne legge til grunn at det utveksles relevant informasjon mellom helsepersonell om vedkommende sin helsetilstand, og om hvilken helsehjelp som gis, jf. Prop. 89 L (2011-2012) kap. 3.1.

4.2 Hjemmelsgrunnlag for innbyggers innsynsrett

Innbygger har en lovfestet rett til innsyn i opplysninger som er registrert om seg. Dette følger av pasientjournalloven § 18, personopplysningsloven § 18 mfl. Denne retten videreføres – og forsterkes i artikkel 15 i ny personvernforordning (GDPR).

Innbygger har innsynsrett overfor primærkilden som har registrert opplysningene (sykehus, fastlege) på grunn av deres dokumentasjonsplikt ifm. ytelse av helsehjelp, jfr. helsepersonelloven § 39. Retten til innsyn i disse dokumentene følger direkte av helsepersonelloven § 41.

4.3 Dataansvaret

Alle virksomheter som kobler seg til Norsk Helsenett forplikter seg til å følge Norm for informasjonssikkerhet i helse- og omsorgssektoren ("Normen"). Retningslinjene i Normen gjenspeiler Personvernforordningens krav som stilles til dataansvarlig og databehandler i forbindelse med behandling av personopplysninger med elektroniske hjelpemidler. I en arkitektur der strukturerte data som er lagret hos hver enkelt aktør i sektoren kun vises gjennom datadeling, vil primærkilden for opplysningene (den enkelte helsevirksomhet) være dataansvarlig for opplysningene som gjøres tilgjengelig gjennom løsningen. De dataansvarlige bestemmer formålet med behandlingen og hvilke virkemiddel som skal benyttes for å nå formålet.

Det er dataansvarliges ansvar å sikre ivaretakelse av krav til konfidensialitet, integritet og tilgjengelighet i forbindelse med tilgjengeliggjøring av personopplysninger fra den aktuelle virksomhets systemer. Dette følger av pasientjournalloven § 22 som sier at *"en databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene [...]."*

4.4 Databehandler

Dersom virksomheten som er dataansvarlig benytter en databehandler, kan denne gis tilgang/behandle opplysninger i tråd med hva den dataansvarlige bestemmer i databehandleravtale. Det kan gis både lese- og skrivetilgang via datadeling. En databehandler behandler opplysninger på vegne av den dataansvarlige og vil altså ikke ha noe selvstendig formål med behandlingen. Databehandleren er som sådan underlagt den dataansvarliges instruksjonsmyndighet, og vil i denne sammenheng ikke regnes som en ekstern virksomhet.

Den databehandlingsansvarlige og databehandleren skal i alle tilfeller sørge for tilfredsstillende informasjonssikkerhet, jf. pasientjournalloven § 22.

4.5 Hovedgruppene for hjemmelsgrunnlag for datadeling

Oppsummert kan man dele datadeling i fem hovedgrupper, hvor datadeling mellom virksomheter er knyttet til tre av hovedgruppene, mens de to siste hovedgruppene er koblet til deling av data med innbyggere. De tre første gruppene skiller seg fra ved at virksomheter deler data basert på ulike hjemmelsgrunnlag som igjen setter ulike krav til hva en virksomhet kan få tilgang til:

1. Tilgang til helseopplysninger mellom virksomheter hvor en av virksomhetene tilgjengeliggjør helseopplysninger fra sitt lokale behandlingsrettede helseregister (jf. definisjonen i pasientjournalloven § 2 d) ved hjelp av datadeling basert på pasientjournallovens §19.
2. Tilgang til og oppdatering av helseopplysninger mellom virksomheter hvor det eksisterer en databehandleravtale eller samarbeid om felles journal etter pasientjournalloven § 9 hvor datadeling benyttes som metode for deling.
3. Tilgang til og oppdatering av helseopplysninger mellom virksomheter og en nasjonal løsning basert på egen forskrift eller forskrift etter pasientjournalloven §10.

Deling av data med innbyggere dekkes i de to siste gruppene hvor den ene gruppen dekker der hvor innbygger får tilgang til sine helseopplysninger via datadeling. I lovverket finnes det generelle krav om å gi pasienter innsyn i egne data (pasient- og brukerrettighetsloven § 5-1, helsepersonelloven § 41, pasientjournalloven § 18 samt i artikkel 15 i GDPR). Den andre gruppen er der hvor innbygger oppdaterer sine helseopplysninger via bruk av datadeling hvor innbygger rapporterer inn informasjon om eget helseforhold, for eksempel via velferdsteknologi eller skjemainnrapportering.

5 Brukstilfeller for datadeling

Å ta i bruk datadeling er et av flere tiltak for å bedre samhandlingen i helse- og omsorgstjenesten.

Datadeling som samhandlingsform kan overordnet løse innbyggers forventning om:

- å delta mer i behandlingsforløpet sitt og få innsyn i behandlingen
- at de involverte helseaktører er koordinert og informert seg imellom.

For helsepersonell kan datadeling løse:

- Behovet for økt koordinering og oppgaveløsning på tvers av virksomheter ,
- Større behov for å kunne fordele oppgaver mellom virksomheter og sikre at oppgavene blir fulgt opp for å dekke behovene for mer spesialisering av oppgaver og generelt større etterspørselen etter helse- og omsorgstjenester.

En større grad av samordning vil kreve mer dynamisk deling av informasjon i motsetning til dagens mer statiske utlevering av informasjonskopier til enkelte parter på bestemte tidspunkter. Det forventes også at en aktør tar mer av hovedansvaret for behandlingsforløpet og at behandlingen er mer forutsigbar og er basert på en plan. Dette gjør at det er behov for å ta i bruk datadeling i mye større grad enn i dag. Økt mobilitet blant pasienter og helsepersonell setter også nye krav til samhandling og til tilgang og deling av informasjon ved hjelp av datadeling.

Med mer deling av informasjon må også personvernet ivaretas og balanseres med behovet for nødvendig tilgang til informasjon.

5.1 Bruksområder for datadeling

Deling av person- og helseopplysninger har mange ulike bruksområder i helse- og omsorgstjenesten hvor datadeling benyttes som samhandlingsform. Hvert av bruksområdene har særegne behov som påvirker arkitekturen for datadeling. Bruksområdene vil benyttes ved beskrivelse av målarkitekturen slik at de særegne behovene blir håndtert adskilt og i tilknytning til det bruksområdet som har behovet. Følgende bruksområder hvor datadeling benyttes er identifisert:

1. Sektorens samhandling med grunnmur og nasjonale e-helseløsninger
2. Innbyggers behandling av sine helseopplysninger
3. Samhandling mellom helsepersonell i andre virksomheter
4. Samhandling med helsepersonell og innbyggere lokalt

I tillegg har sektoren behov for samhandling med andre offentlige etater og tjenester utenfor helse- og omsorgstjenesten. Dette området er holdt utenfor.

Et annet bruksområde som er holdt utenfor er innbyggers behov for å samhandle med andre innbyggere samt innbyggers bruk av utstyr på eget initiativ som samler inn og lagrer helseopplysninger.

5.1.1 Sektorens samhandling med grunnmur og nasjonale e-helseløsninger

Dette bruksområdet dekker brukstilfeller hvor personell med tjenstlig behov har behov for å gjøre oppslag eller oppdatere/registrere person- og helseopplysninger i nasjonale e-helse tjenester slik som for eksempel Kjernejournal hvor datadeling benyttes som samhandlingsform. I tillegg dekker bruksområdet oppslag i register og tjenester for grunndata.

5.1.1.1 Oppslag, oppdatering/registrering i nasjonal e-helsetjeneste

Nasjonal e-helsetjeneste benyttes som samhandlingsløsninger hvor hovedformålet er å unngå mange til mange samhandlingsformer. Kritisk info i Kjernejournal er et eksempel hvor kopi av kritisk info om en pasient blir registrert i Kjernejournal av helsepersonell og blir tilgjengelig for oppslag for annet helsepersonell. Reseptformidleren er et annet eksempel på en sentral tjeneste som benyttes for samhandling rundt rekvirering og utlevering av legemidler.

Både Kjernejournal og Reseptformidleren støtter flere samhandlingsformer hvor datadeling er en av disse.

Felles for nasjonale e-helsetjenester er at de normalt krever egen forskrift for å behandle og lagre helseopplysninger uten at det hentes inn pasientens samtykke på forhånd.

5.1.1.2 Tilgang til grunndata

Tilgang til grunndata er viktig slik at helsepersonell og systemer har oppdatert og korrekt informasjon.

Dette innebærer tilgang til administrative grunndata som ikke er helseopplysninger eller knyttet til en pasient, herunder data fra helseadministrative registre.

Det er behov for å søke etter tjenester, enheter og annen informasjon i ulike registre og søketjenester som:

- Adresseregisteret (AR)
- Helsepersonellregisteret (HPR)
- Legestillingsregisteret (LSR)
- Fastlegeregisteret
- Register for enheter i spesialisthelsetjenesten (RESH)
- Personregisteret (PREG), helse- og omsorgssektorens kopi av det sentrale folkeregisteret
- Medisinske kodeverk og klassifikasjoner (FinnKode, med mer)
- Administrative kodeverk (Volven)

5.1.2 Innbyggers behandling av sine helseopplysninger

Dette bruksområdet dekker brukstilfeller der hvor det benyttes datadeling for å gi innbygger tilgang til å delta og få innsyn i sine helseopplysninger.

Eksempler på brukstilfeller hvor datadeling kan benyttes som samhandlingsform:

Med Innbygger	Beskrivelse	Eksempler
Innsyn i egne helseopplysninger i sentrale registre	Innbygger ønsker lovfestet innsyn i egne helseopplysninger som finnes registrert i ulike helseregistre eller en gitt tjeneste.	Helsenorge.no (kjernejournal), sentrale helseregistre
Innsyn i egen journal og bruk	Innbygger ønsker lovfestet innsyn i egne journalopplysninger. En pasient kan ha flere ulike journaler hos ulike virksomheter.	Helsenorge.no benytter datadeling mot helseaktører
Selvbetjeningsløsning	Innbygger kan benytte selvbetjeningsløsninger der opplysninger behandles automatisk.	Bytt fastlege, endre timer og pasientreiser benyttes av pasientens app på sin mobil og benytter datadeling
Skjemaregistrering	Innbygger skal fylle ut skjemaer laget av helsevesenet, som en engangshendelse eller repetert. Skjemaene kan være en del av jevnlig medisinsk oppfølging av primær- eller spesialisthelsetjeneste, helseundersøkelser over tid, enkel innrapportering av medisinske måledata, brukerundersøkelser med mer.	Medisinsk oppfølging, velferdsteknologi, helseundersøkelser (som HUNT)

5.1.3 Samhandling mellom helsepersonell i andre virksomheter

Dette bruksområdet dekker brukstilfeller som i hovedsak dekker behovet for at helsepersonell i ulike virksomheter har behov for samhandling for å yte best mulig helsehjelp

Virksomheter som yter helsehjelp har en plikt til å samarbeide om behandling og forebygging av sykdom hos innbyggere. Det ligger som en forutsetning for godt samarbeid at aktørene må samarbeide om behandlingsplaner og andre helseopplysninger. Samarbeidet kan inkludere deling av dokumentasjon ved hjelp av datadeling fra den ene virksomheten til den andre, og kan også inkludere digitalisert samarbeid om pasientforløp på tvers av virksomheter. For mer avanserte samarbeidsformer rundt en pasient vil ikke meldings- og dokumentutveksling være tilstrekkelig for å kunne lage fleksible og gode samarbeidsløsninger. Her vil samarbeidsprosesser og arenaer kreve datadeling der aktørene kan samarbeide om både strukturerte dokumenter og mindre informasjonselementer.

Dette bruksområdet må sees i sammenheng med de nasjonale tiltakene som for eksempel Akson og Helseplattformen som skal løse hoveddelen av behovet for samhandling ved å ha en felles journal. Disse tiltakene vil redusere antall løsninger som det må lages samhandlingsfunksjoner som benytter datadeling på tvers.

Det er i midlertidig langt frem før disse løsningene er realisert og tatt i bruk. Det vil derfor være behov for å ta i bruk datadeling også frem til disse løsningene er realisert og tatt i bruk.

Behovsanalysen til konseptvalgutredningen for nasjonal journalløsning for kommunal helse- og omsorgstjeneste beskriver behovene for samhandling i detalj [7].

5.1.4 Samhandling med helsepersonell og innbyggere lokalt

Dette bruksområdet dekker brukstilfeller hvor helsepersonell og innbyggere benytter mobile applikasjoner samt velferdsteknologi for å samarbeide om helsehjelp og som kan benyttes internt i mange virksomheter. Bruk av slike løsninger kalles ofte lettvekts-IT og har behov for å få tilgang til pasientens helseopplysninger gjennom API-er i journalløsningene som ofte refereres til å være tungvekts-IT.

Bruksområdet skal dekke leverandørmarkedets behov for å utvikle løsninger som kan gjenbrukes av mange virksomheter i sektoren, men også for at nye leverandører skal kunne enklere konkurrere med etablerte leverandører hos den enkelte virksomhet.

Eksempler på brukstilfeller:

- Oppslag i ulike tjenester: Oppslag for helsepersonell i en virksomhet sine tjenester der det ligger relevant informasjon om pasient
- Sammendrag. Gi et relevant sammendrag av helsetilstanden eller om en behandling gitt til en pasient.
- Samarbeid om pasient. Et behandlingsteam som skal samarbeide om behandlingen av en pasient hvor pasienten selv også skal bidra.
- Innrapportering av medisinske måledata som pasient får utplassert for at helse- og omsorgstjenesten kan følge opp hjemmeboende pasienter.
- Skjemaregistrering knyttet til oppfølging av pasient hvor for eksempel pasient får med seg en Ipad hjem etter et sykehusopphold og som må rapportere opplevd tilstand eller andre opplysninger.

6 Målarkitektur for datadeling

6.1 Innledning

En målarkitektur er en fremtidig, ønsket tilstand. Det er naturlig å ha en stegvis, behovsprøvd tilnærming til realisering av målarkitekturen. Samtidig er det viktig at de første stegene forholder seg til en fremtidig målarkitektur for å unngå arkitekturvalg som senere vil være kostbare å endre på. Målarkitekturen beskriver ikke hvordan arkitekturen skal realiseres og kan derfor sammenlignes med en reguleringsplan.

Behovene som ligger til grunn for målarkitekturen vil endres og modnes over tid. Derfor må målarkitekturen beskrevet i dette dokumentet ikke sees på som en endelig arkitektur.

6.1.1 Føringer

Datadeling kan løses på svært mange måter. I arbeidet med målarkitekturen har det vært nødvendig å utarbeide noen føringer for arbeidet med målarkitekturen. Disse føringene er ble utarbeidet i samarbeid med sektoren ved oppstart av arbeidet med målarkitekturen.

1. Målarkitekturen skal beskrive datadeling med bruk av felleskomponenter og følgende felleskomponenter skal vurderes:
    a. HelseID for identifisering av helsepersonell og sikring av API-er for helsepersonellbruk.
    b. Innbygger-STS for identifisering av Innbyggere og sikring av API-er for innbyggerbruk.
    c. Felles API management løsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter.
    d. Felleskomponenter for håndtering av samtykke, reservasjoner, sperringer og fullmakter, for logging og innsyn i brukslogg dersom dette er hensiktsmessig.
    e. Felleskomponent for oppslag av hvilke virksomheter som har helseopplysninger lagret om en gitt pasient.
    f. Felles API-katalog.
2. Målarkitekturen skal legge til grunn anbefalt tillitsmodell hvor tjenstlig behov skal håndheves av anvendende virksomhet heretter kalt brukerorganisasjonene. Målarkitekturen skal i tillegg legge til grunn at fingranulert tilgangsstyring av brukere kan håndheves av API-eier (tjenestetilbyder). Dette forutsetter at informasjon om bruker, organisasjon og tjenstlig behov distribueres i en sikkerhetsbillett til API-eier som spesifisert i " *Krav til sikkerhetsbillett ved deling av helseopplysninger*" [17].

6.1.2 Hovedmålsetninger

For målarkitektur for nasjonal datadeling er det utarbeidet følgende hovedmålsetning*:*

> Målarkitekturen for datadeling anbefaler hvordan en umiddelbar, sikker deling og oppdatering av strukturert informasjon på tvers av aktører i helse- og omsorgstjenestene og med innbyggere skal realiseres.
>
> Det skal være enkelt for aktører å etablere deling og oppdatering av person- og helseinformasjon på en strukturert og standardisert måte.

Målarkitekturen har i tillegg følgende målsetninger:

- Muliggjøre arkitekturstyring på flere nivåer: nasjonalt, regionalt og for andre grupperinger av dataansvarlige slik at arkitekturvalg kan gjennomføres mest mulig uavhengig av nivåene, men samtidig sørge for at valg som berører alle nivåer gjelder for hele helse- og omsorgstjenesten.
- Oppnå fleksibilitet i arkitekturen som dekker behov til både store og små aktører.

6.1.3 Bruksområder for datadeling

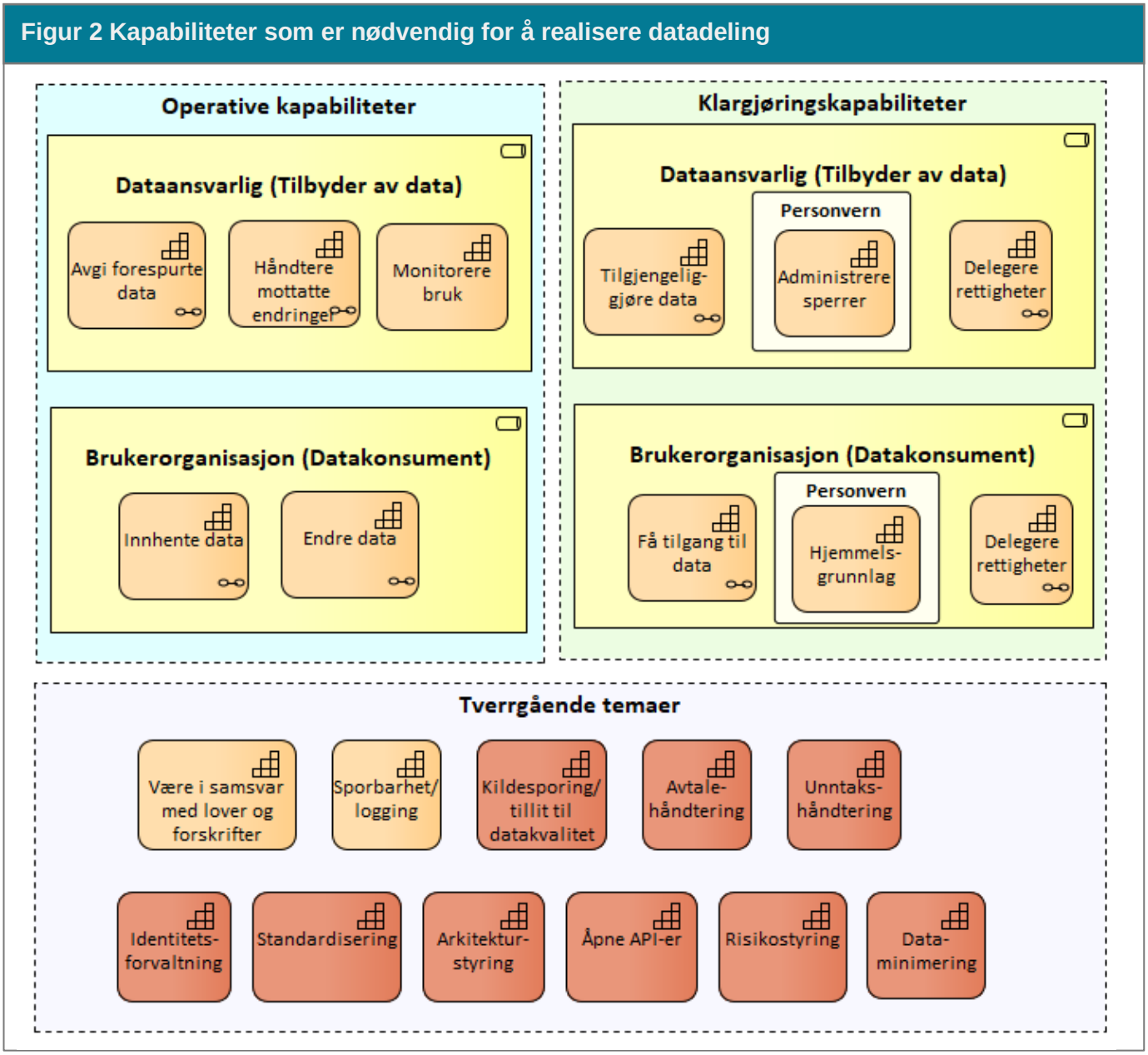
Ulike bruksområder for datadeling setter ulike krav til målarkitekturen. Dokumentet vil behandle arkitekturen for de bruksområdene som er identifisert i kapittel 5.1 adskilt.

6.2 Kapabiliteter nødvendig for å realisere datadeling

DigDir har sammen med andre offentlige virksomheter utarbeidet en referansearkitektur for datautveksling. I dette arbeidet har de identifisert kapabiliteter som må være på plass for å ta i bruk datadeling [12]. Vi har tatt utgangspunkt i denne modellen og tilpasset temaene behov og begreper som helse- og omsorgstjenesten har. Dette er vist i Figur 2 og hver kapabilitet er beskrevet i **Feil! Fant ikke referansekilden.** . Kapabilitetene benyttes senere til å beskrive hvordan helse- og omsorgssektoren kan realisere kapabilitetene ved bruk av felleskomponenter og vil være grunnlaget for hvilke ansvar som de enkelte felleskomponentene vil ha i målarkitekturen. Vi har valgt å gruppere kapabilitetene i klargjørings-, operative og tverrgående kapabiliteter:

- Klargjøringskapabiliteter: kapabiliteter knyttet til forberedende aktiviteter før to parter er i stand til å dele
- Operative kapabiliteter: kapabiliteter knyttet til aktiviteter som foregår i sanntid ved deling av data mellom to parter.
- Tverrgående kapabiliteter: Kapabiliteter som angår alle aktørene innen datadeling

Figur 2 Kapabiliteter som er nødvendig for å realisere datadeling



Tabell 1 Beskrivelse av kapabilitetene

Kapabilitet	Ansvarlig aktør	Beskrivelse
Tilgjengeliggjøre data	Dataansvarlig	Evnen til å gjøre data tilgjengelig for aktører utenfor egen virksomhet med eller uten krav til innlogget bruker ved hjelp av datadeling.
Få tilgang til data	Brukerorganisasjon	Evnen til å skaffe seg tilgang til tilbudte data fra annen aktør ved hjelp av datadeling.
Administrere sperrer	Dataansvarlig	Evnen til å håndtere mottak og registrering av ønsker fra pasienter som vil motsette seg deling.

Kapabilitet	Ansvarlig aktør	Beskrivelse
Delegere rettigheter	Både dataansvarlig og Brukerorganisasjon	Evnen til å delegere rettigheter til databehandler som utfører oppgaver på vegne av dataansvarlig.
Hjemmelsgrunnlag	Brukerorganisasjon	For at en aktør skal behandle helseopplysninger må den ha et hjemmelsgrunnlag. Et hjemmelsgrunnlag er knyttet til hjemmel i lov, forskrift, rettspraksis eller annen rettskilde.
Avgi forespurte data	Dataansvarlig	Evne til å avgi data på forespørsel. Kan omfatte tilgangsstyring på brukernivå.
Håndtere mottatte endringer	Dataansvarlig	Evnen til å behandle endringer (opprettelse, oppdatering, sletting) av helseopplysninger mottatt fra en annen aktør ved hjelp av datadeling.
Monitorere bruk	Dataansvarlig	Evnen til å ha kontroll på andre aktørers datadelingsbruk for å holde oversikt over hvem som har fått tilgang til hva når og hvorfor.
Innhente data	Brukerorganisasjon	Evnen til å innhente data fra en annen aktør ved hjelp av datadeling
Endre data	Brukerorganisasjon	Evnen til å gjøre dataendringer hos en annen aktør ved hjelp av datadeling
Være i samsvar med lover og forskrifter	Tverrgående	For at to aktører skal dele helseopplysninger med hverandre må begge parter være i samsvar med lover og forskrifter
Sporbarhet/logging	Tverrgående	Evne til å etterprøve tjenstlig behov.
Kildesporing	Tverrgående	Å kunne ha sporing til hvem som har forfattet/opprettet helseopplysninger er svært viktig for tilliten til dataene og dens kvalitet, spesielt ved datadeling mellom aktører hvor kildesporing er lett å utelate.
Avtalehåndtering	Tverrgående	Evne til å håndtere avtaler om tilgang til og bruk av data. Det er et mål å unngå behov for bilaterale avtaler mellom aktørene og benytte et tillitsanker som håndterer avtaler og/eller bruksvilkår.
Unntakshåndtering	Tverrgående	Evne til brukerorganisasjoner til å gjennomføre sine helsetjenester ved nedetid hos tilbydere av data.

Kapabilitet	Ansvarlig aktør	Beskrivelse
Standardisering	Tverrgående	Evne til å utarbeide, enes om og ta ibruk standarder på tvers av mange aktører
Arkitekturstyring	Tverrgående	Evne til å koordinere og beslutte arkitekturvalg og andre arkitekturrelaterte problemstillinger på tvers av mange aktører .
Åpne API-er	Tverrgående	Evne til å tilby gjenbrukbare, sikre, godt dokumenterte og tilgjengelige programmeringsgrensesnitt som kan benyttes av alle relevante aktører uten diskriminerende og konkurransevridende vilkår.
Risikostyring	Tverrgående	Evne til å styre risiko ved deling av helseopplysninger mellom aktører
Dataminimering	Tverrgående	Evne til å tilby kun relevant og nødvendig helseopplysninger til andre aktører.

6.3 Felleskomponenter for datadeling

Kapabilitetene beskrevet i forrige kapittel beskriver ikke hvem som har hvilket ansvar. Når to virksomheter skal dele helseopplysninger med hverandre, må alle de beskrevne kapabilitetene være på plass. "peer"-to-"peer" deling skalerer i liten grad når hele helse- og omsorgstjenesten skal dele (mange til mange). Det bør derfor etableres felleskomponenter for datadeling som håndterer kapabilitetene på vegne av virksomhetene som deler.

Virksomhetene må etablere tillit til hverandre for å kunne dele helseopplysninger. Gjennom en felles tillitsmodell som virksomhetene slutter seg til, kan en slik tillit etableres på en enhetlig måte gjennom bruk av felleskomponenter som støtter opp under felles tillitsmodell.

Direktoratet for e-helse har beskrevet en anbefaling til en overordnet tillitsmodell for data- og dokumentdeling [10] som helse- og omsorgstjenesten har tilsluttet seg. Anbefalingen dekker helsepersonellbruk av datadeling og er lagt til grunn i arbeidet med målarkitekturen.

Felleskomponenter for datadeling vil kunne øke utbredelse av datadelingsløsninger og de skal legge til rette for at virksomheter raskere kan være i stand til å oppfylle kravene til personvern og informasjonssikkerhet.

Brukerorganisasjoner vil normalt benytte et fagsystem som en klient for å få tilgang til helseopplysninger gjennom et API. Helseopplysninger kan kun overføres til brukerorganisasjoner som har et behandlingsgrunnlag for dette. De behandlingsgrunnlagene vi dekker i målarkitekturen er:

1. Innbyggers rett til innsyn i egne helseopplysninger, jmf GDPR artikkel 15.
2. Personell med tjenstlig behov basert på lovhjemmel, slik som § 19 i pasientjournalloven, kjernejournalforskriften osv.
3. Samtykkebasert tilgang hvor personell gis tilgang basert på eksplisitt samtykke fra innbygger.

Hvilke felleskomponenter har vi behov for? Dette er et sentralt spørsmål som målarkitekturen må svare ut. Gjennom arbeidet med referansearkitekturen for datadeling er det identifisert flere kandidater. Vi vil i dette kapittelet gjøre en behovsvurdering av disse kandidatene. Vurdering av felleskomponent-kandidater er inndelt i følgende kategorier:

6. Felles tillitsøkende tjenester
7. Felles API-katalog
8. Felles API managementløsning
9. Felleskomponent for lokalisering av pasientinformasjon
10. Felleskomponent for logging

Felleskomponenter defineres som komponenter som kan sambrukes i flere IT-løsninger og dekker felles behov. Felleskomponenter kan brukes på tvers av e-helseløsninger, virksomheter og forvaltningsnivå. Vi legger i dette dokumentet ingen føringer om en felleskomponent er frivillig eller påkrevd å bruke.

6.3.1 Felles tillitsøkende tjenester

Ved bruk av datadeling som involverer deling av helseopplysninger, må det etableres tillit mellom konsumenten av API-et og API-et. Målarkitekturen baseres på at dette sikres gjennom bruk av felles tillitsøkende tjenester.

6.3.1.1 Hvilke tjenester eksisterer i dag?

I dag (2020) er følgende etablert:

1. En tjeneste for behandlingsgrunnlag knyttet til innbyggers rett til innsyn (nr 1): Helsenorges sikkerhetstjeneste (Innbygger-STS) sammen med personvernkomponenten
2. En tjeneste for behandlingsgrunnlag knyttet til lovhjemmel i helselovgivningen (nr 2): HelseID.
3. For behandlingsgrunnlag basert på samtykke fra pasient (nr 3) er det ikke etablert en felleskomponent for håndtering av samtykker som kan benyttes av hele sektoren. Dette kan realiseres ved en utvidelse av en eller begge de nevnte løsningene i punkt 1. Helsenorge innhenter samtykke for sine tjenester og benytter personvernkomponenten for lagring av samtykker. Andre innbyggertjenester (eksempel pasientreiser) innhenter også samtykke fra pasient i dag, men benytter ikke personvernkomponenten for dette.

6.3.1.2 Bør samme løsning dekke både behandlingsgrunnlag nr 1 og 2?

Behovene som helse- og omsorgstjenesten har, knyttet til innbyggers rett til innsyn, er svært like behovene andre offentlige virksomheter har for innbyggers innsyn i sensitiv informasjon. Basert på disse felles behovene er det stor sannsynlighet at det i fremtiden vil komme en felles tverrsektoriell løsning som dekker felles behov knyttet til løsning for innbyggers rett til innsyn ved bruk av datadeling. Vi anbefaler derfor at dagens løsning videreutvikles som en egen felleskomponent som dekker behandlingsgrunnlaget knyttet til innbyggers rett til innsyn og det må tas høyde for at enten hele eller deler av dagens løsning må på sikt byttes ut eller integreres med en felles tverrsektoriell løsning.

For behandlingsgrunnlag knyttet til lovhjemmel er vurderingen at lovhjemlene som ligger til grunn for dette, er helsespesifikke. Lover og forskrifter som gjelder ved yting av helsehjelp inneholder spesielle krav som gjelder kun for helsesektoren. Vår anbefaling er at det må legges til grunn at HelseID videreføres som en sektorløsning tilpasset helse- og omsorgstjenesten behov.

Basert på disse to vurderingene anbefales det i målarkitekturen å videreføre Innbygger-STS og HelseID som separate løsninger for de respektive behandlingsgrunnlaget.

6.3.1.3 Felles forutsetninger til bruk av felleskomponenter

Referansearkitektur for datadeling [1] beskriver arkitekturprinsipper som gjelder ved utvikling av datadelingsgrensesnitt. Vi har videre sett på de viktigste forutsetninger som ligger til grunn for bruk av felleskomponenter tilknyttet datadeling. Følgende forutsetninger ligger til grunn i arbeidet med vurdering av felleskomponentene:

1. Alle brukerorganisasjoner og API-eiere må akseptere bruksvilkårene til en felleskomponent for datadeling for å bruke den.
2. Iht Helsepersonelloven § 45 skal det fremgå av journal at helsepersonell utenfor sin egen virksomhet har mottatt helseopplysninger. Tjenestetilbyder setter derfor krav til at det finnes en innlogget sluttbruker på klienten. Det er lite hensiktsmessig at sluttbruker er registrert hos tjenestetilbyder og tjenestetilbyder må derfor kunne stole på at en felleskomponent sikrer at en sluttbruker er innlogget med en elektronisk identitet på et tilstrekkelig avtalt tillitsnivå.
3. Brukerorganisasjoner må kunne velge hvilken eID tilbyder den benytter for et avtalt tillitsnivå. Sluttbruker må være i stand til å velge innlogging fra en liste over aksepterte elektroniske identiteter for et gitt tillitsnivå. Dersom sluttbruker allerede er innlogget med en akseptert identitet, skal tjenestetilbyder kunne stole på dette slik at sluttbruker slipper å logge inn på nytt.
4. Tjenestetilbyder må motta en signert sikkerhetsbillett fra en felleskomponent som et bevis på at sluttbruker er innlogget med riktig sikkerhetsnivå.
5. Alle API-er (eller den de har delegerte ansvaret til) må ha tillitt til de sikkerhetsbilletter som er utstedt av felleskomponenten.
6. Alle klienter av et API må kunne entydig kobles til en registrert klientkonfigurasjon gjennom autentisering av klienten og kobling til en organisasjon og/eller en leverandør.
7. Siden behandlingsgrunnlaget til brukerorganisasjonen må være avklart før deling av helseopplysninger kan starte. Må en klient være gitt en forhåndstillatelse for å kalle et API. Behandlingsgrunnlaget vil også bestemme hva den kan utføre på en gitt ressurs(typisk lese eller skrive). Det er lagt til grunn i målarkitekturen at Tjenestetilbyder overlater håndtering av forhåndstillatelser til en felles tillitsøkende tjeneste, men skal kunne, om ønskelig, selv godkjenne brukerorganisasjonene.
8. Sikkerhetsmodellen som legges til grunn i målarkitekturen skal sikre at elektronisk identitet og sikkerhetskontekst overføres på en sikker måte fra kallende klient til utførende API slik at API-et kan overholde lovmessige krav til logging samt muligheten til å implementere brukertilgangskontroll dersom behov for det.

6.3.1.4 Detaljering av de tillitsøkende tjenestene

Tillitsøkende tjenester er et bredt begrep og kan dekke mange sikkerhetsfunksjoner. Vi vil her beskrive de mest aktuelle felles tillitsøkende tjenester som er nødvendig for å etablere datadeling som en samhandlingsform i helse- og omsorgstjenesten. Vi har valgt å ikke beskrive mer generiske tillitsøkende tjenester som sertifikatutstedelse, identitetstilbydere, signaturtjenester og andre mer generiske tillitsøkende tjenester.

Følgende behov for felles tillitsøkende tjenester er vurdert:

1. En portal hvor godkjente tilbydere av digitale identiteter kan tilby sine digitale identiteter
2. En felles autentiseringsløsning for applikasjoner som bruker portalen i punkt 1
3. Felles klientautentisering – en sikker autentisering av forhåndsgodkjente klienter
4. Felles klientautorisering – håndheving av autorisasjoner som en klient har blitt godkjent for å benytte.
5. Sentral fullmaktsløsning - hvor de en innbygger har gitt tilgang til å representere seg, kan få tilgang på vegne av innbygger.
6. Felles samtykkeløsning - hvor de applikasjoner eller personell en innbygger har delegert tilgang til et begrenset sett av sine helseopplysninger får tilgang til disse helseopplysninger.
7. Felles sperretjeneste – hvor de en innbygger ønsker å sperre innsyn for er registrert. (Sperre innsyn = motsette seg deling av sine helseopplysninger)
8. Felles reservasjonsløsning – Reservasjon mot registrering av helseopplysninger. Hvor en innbygger kan reservere seg mot behandling av sine helseopplysninger i en løsning basert på rettigheter i en lovhjemmel.

6.3.1.5 Portal over godkjente tilbydere av digitale identiteter

Deling av helseopplysninger krever brukerpålogging med digitale identiteter med tilstrekkelig høyt sikkerhetsnivå/tillitsnivå. Målarkitekturen legger til grunn at det ikke skal være nødvendig å etablere nye digitale identiteter for å benytte datadeling, men gjenbruke de som finnes. Det må i tillegg tilrettelegges for at virksomheter kan etablere sine egne digitale identiteter med tilstrekkelig høyt tillitsnivå for sitt personell. Det er viktig at brukeren kan velge digitale identiteter slik at brukere kan benytte kjente digitale identiteter. I tillegg kan dette tilrettelegge for engangspålogging ("single sign-on").

6.3.1.6 Sentral autentiseringsløsning

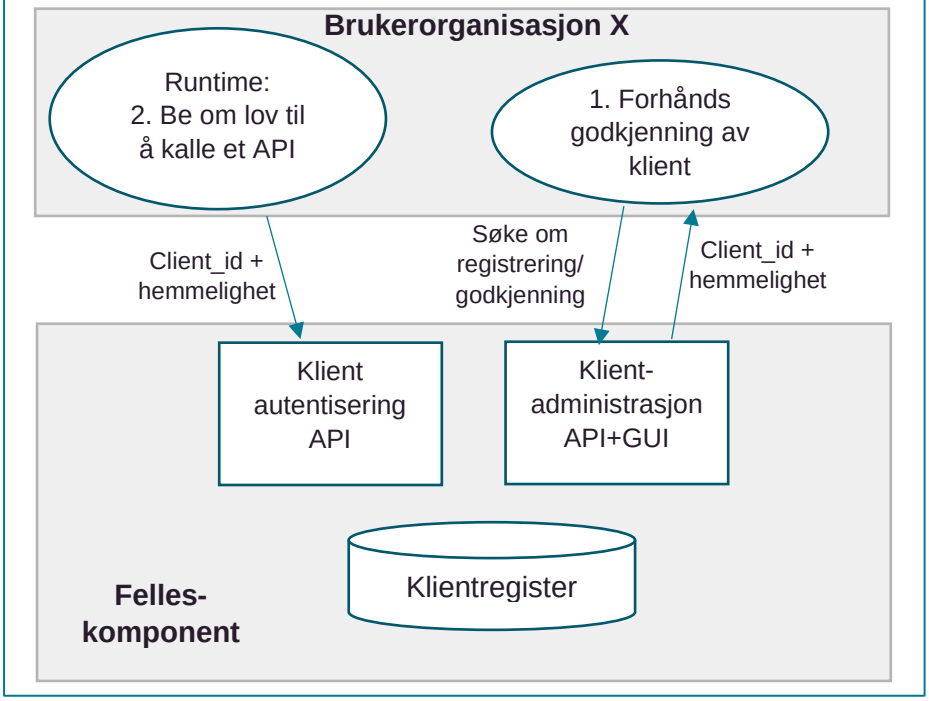
Det er behov for å ha en sentral autentiseringsløsning som fungerer som en tillitstjeneste for hele helse- og omsorgstjenesten og tilrettelegger for single sign-on. Sentral autentiseringsløsning må fungere slik at alle API-eiere må stole på påloggінger gjennomført via denne løsningen. Siden det legges opp til at brukere kan velge tilbyder av digitale identiteter ved pålogging, så er det hos den valgte tilbyderen brukeren må logge seg på.

6.3.1.7 Klientautentisering – autentisering av brukerorganisasjon

For at en API-eier skal kunne tillate en annen virksomhet tilgang til sitt API har API-eier behov for å autentisere brukerorganisasjonen. Teknisk sett autentiseres klienten og klienten kobles til brukerorganisasjonen gjennom en klientkonfigurasjon. Følgende behov må dekkes av klientautentisering:

- En klient må kunne knyttes til en virksomhet
- Alle klienter må være forhåndsregistrert før de kan få tilgang til et API. Her kan det være krav om at det etableres avtaler, krav til godkjenning/sertifisering av klientene og andre krav som stilles til brukerorganisasjoner og deres klienter.
- Ved forhåndsregistrering må en klient kunne unikt identifiseres og autentiseres
- Autentiseringen av klienten må gjøres på en sikker måte (eksempler: virksomhetssertifikat, API nøkler osv).

Figur 3 Konseptuell arkitektur for Klientautentisering



Figur 3 viser konseptet bak klientautentisering. En brukerorganisasjon må kunne registrere og få godkjent sine klienter. Prosess for å få godkjent en klient kan inneholde flere tillitsøkende steg. Et eksempel på et slik steg kan være at virksomheten må inngå en privatrettslig avtale som forplikter virksomheten til å følge visse krav. Et annet kan være at det må være sertifiserte driftspersonell som setter opp klientene.

Når en klient eller en brukerorganisasjon er godkjent, så kan klienten starte med å søke om å ta i bruk API-er som krever at klientene eller brukerorganisasjonene er forhåndsgodkjente av tillitstjenesten. Ved kall til API-ene må tillitstjenesten autentisere klienten før klientautoriseringen kan gjøres.

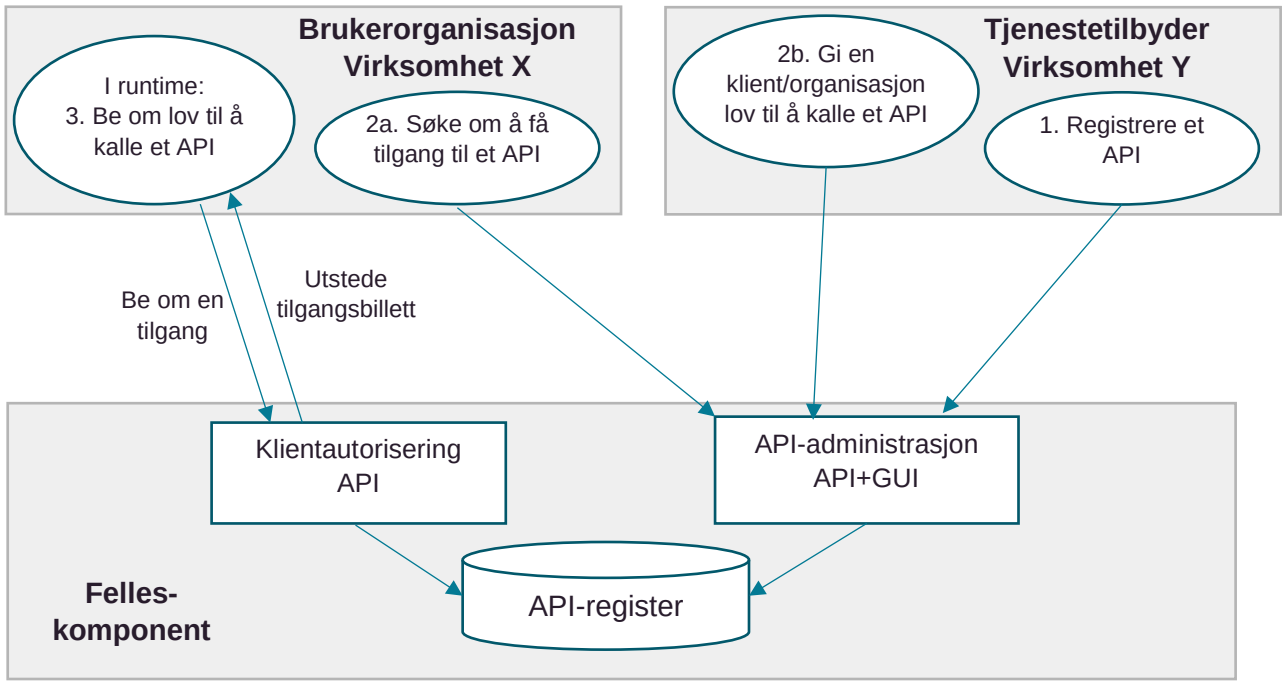
6.3.1.8 Klientautorisering – autorisering av brukerorganisasjonenes tilgang til API

En API-eier må kun akseptere forespørsler fra brukerorganisasjoner som er forhåndsgodkjente til å motta eller endre deres helseopplysninger. Klientene må autoriseres for få lov til å kalle API-ene til API-eier. Dette ansvaret kan overlates til en felles tillitsøkende tjeneste. API-eier må da inngå en avtale med tjenesten og registrere sine API-er og hvilke tilgangsregler som skal gjelde for API-ene. Eksempler på tilgangsregler:

- Alle godkjente klienter i tillitstjenesten som oppfyller API-eiers krav til klienter skal få automatisk tilgang til API-eiers API.
- Kun klienter fra virksomheter som API-eier har inngått avtale med skal få tilgang

API-eier må for hver klient angi en autorisasjon (scope) som bestemmer hva klienten får lov til å gjøre, for eksempel hvilke ressurser den får lov til å lese, opprette eller endre.
NB: et API kan i tillegg ha tilgangsregler knyttet til brukeren som er logget inn, men dette dekkes ikke av klientautoriseringen. Figur 4 viser konseptet bak felles klientautorisering hvor API-eier må først registrere API-et sitt. Deretter må virksomheten som eier klienten søke om

Figur 4 Konseptuell arkitektur for felles klientautorisering



å få tilgang til å kalle API-et. API-eier må godkjenne søknaden før klienten kan få tilgang til å kalle API-et.

6.3.1.9 Fullmaktsløsning

Det må ved bruk av datadeling legges til rette for at forespørsler om tilgang til helseopplysninger kan gjøres av personer som innbygger har eksplisitt gitt tilgang til å representere seg. I tillegg må de som har foreldreansvar eller er verge kunne få tilgang.

Tillit til slike representasjoner krever at en tillitstjeneste kan beskrive godkjente representasjoner som API-eiere har tillit til. I tillegg må innbygger kunne administrere sine representasjoner digitalt. Mulighet til å representere en innbygger er kun knyttet til innbyggers rett til innsyn i sine egne helseopplysninger.

6.3.1.10 Samtykkeløsning

Å få pasientens samtykke er en mulig lovhjemmel for å behandle, dele og/eller lagre helseopplysninger. Vi omhandler i målarkitekturen samtykke relatert til deling.

Mange tjenester på Helsenorge krever samtykke fra pasient for å behandle pasientens helse- og personopplysninger. Et eksempel er tjenesten Pasientreiser som krever at pasienten samtykker til at Pasientreisetjenesten kan innhente informasjon fra besøksregistrene for å få bekreftet at pasienten har vært på en behandling den dagen pasienten søker om refusjon. Samtykket registreres i dag i personverntjenesten til Helsenorge.

Pasientreiser-eksempelet er et eksempel hvor innbygger benytter en applikasjon som ikke har et behandlingsgrunnlag for å innhente innbyggers helseopplysninger via datadeling. Det vil være behov for en slik samtykkeløsning også for andre tilbydere av innbyggerbaserte applikasjoner som for eksempel en mobil applikasjon som tilbyr nye, innovative tjenester til innbyggere.

I eksempelet om pasientreiser ber applikasjonen om samtykke når innbyggeren benytter applikasjonen. Det vil også være behov for at personell som mangler et behandlingsgrunnlag skal kunne be om et digitalt samtykke til tilgang til en innbyggers helseopplysninger for et bestemt formål. En slik samtykkeprosess vil være annerledes enn når en applikasjon ber om samtykke. Prosessene vil være at helsepersonell må be en samtykkeløsning om at det innhentes samtykke om et bestemt formål. Innbygger må så varsles og må gjennomføre en vurdering om det skal gis et samtykke innen en gitt tidsfrist.

6.3.1.11 Sperretjeneste

Iht. lovgivningen kan en pasient motsette seg deling av sine helseopplysninger ved å be om at deler eller hele journalen sperres for enkeltpersonell, en gruppe av helsepersonell eller virksomheter. Opplysningene kan heller ikke tilgjengeliggjøres eller utleveres dersom det er grunn til å tro at pasienten ville motsette seg det ved forespørsel.

Når en pasient benytter seg av denne retten, må virksomheten nedtegne ønsket fra pasienten i journalen, heretter kalt sperringer, og håndheve sperringen når pasientens journal aksesseres.

Ved bruk av datadeling må løsningene som deler helseopplysninger kunne ivareta at bestemte deler eller hele journalen er sperret for enkeltpersonell, en gruppe av helsepersonell eller virksomheter.

En sperretjeneste må kunne administrere sperringer samt sørge for at de håndheves.

6.3.1.12 Reservasjonsløsning

Flere nasjonale e-helsetjenester har en lovhjemmel for å behandle og lagre helse- og personopplysninger digitalt uten at pasienten må samtykke på forhånd. For disse løsningene har, iht. lovverket, pasienten rett til å reservere seg mot en slik behandling og lagring. En løsning for å administrere og håndheve reservasjoner kaller vi reservasjonsløsning.

6.3.1.13 Oppsummering av behov for tillitsøkende tjenester

I Figur 5 er det gjort en overordnet vurdering av hvilke bruksområder som har behov for de ulike tillitstjenesten. I denne figuren er det brukt fargekoder for ulike kategorier av behovsvurderingen og de ulike fargekodene er forklart i Tabell 2.

Tabell 2 Symbolforklaring på behovsvurdering

Kategori	Forklaring
	Stort felles behov og vil gi stor kost/nytteverdi å etablere som fellesfunksjonalitet
	Finnes behov, men det er mer usikkert om det vil gi noe kost/nytteverdi å etablere som fellesfunksjonalitet da samme funksjonalitet kan dekkes andre steder
	Ikke relevant

Figur 5 Behovsvurdering av tillitstjenestene				
Fargeforklaring: se Tabell 2	Sektorens samhandling med grunnmur og nasjonale e-helseløsninger	Innbyggers deltagelse og innsyn i sin helsehjelp	Samhandling mellom helsepersonell i ulike virksomheter	Samhandling mellom helsepersonell gjennom bruk av ny teknologi
Behov for å støtte valg av mange digitale identiteter				
Behov for felles autentiseringsløsning for personell				
Behov for felles klientautentisering				
Behov for felles fullmaktsløsning				
Behov for felles samtykkeløsning				
Behov for felles sperretjeneste				
Behov for felles reservasjonsløsning				

6.3.2 Vurdering av felles tillitsøkende tjeneste for helsepersonell bruk

HelseID er allerede etablert som en felles tillitsøkende tjeneste som virksomhetene kan benytte når virksomhetene skal dele helseopplysninger. Dette er videreført i målarkitekturen. Vi har i arbeidet med målarkitekturen vurdert hvilke tillitsøkende tjenester som HelseID må ha og hvilke av disse tillitstjenestene som brukerorganisasjonene og API-eiere er påkrevd eller valgfrie.

I Figur 6 er HelseID sine 3 hovedtjenester beskrevet og som legges til grunn for HelseID som en felleskomponent i målarkitekturen.

Figur 6 HelseID sine tillitsøkende tjenester

a) En portal hvor brukerorganisasjoner kan tilby sine digitale identiteter
b) Sentral autentiseringsløsning for applikasjoner som bruker portalen i punkt a
c) Klientautentisering og – autorisering. Sikring av API hvor sluttbrukers identitet transporteres i sikkerhetsbilletter

Basert på vurderingene som er gjennomført har vi kommet frem til følgende arkitekturvalg:

Arkitekturvalg 1

Målarkitekturen legger til grunn at HelseID skal være en felles tillitsøkende tjeneste for å:

1a) autentisere personell med tjenstlig behov som alle API-eiere **må** benytte.

1b) autentisere og autorisere klienter som en API-eier **kan** velge å benytte.

6.3.3 Vurdering av Helsenorge sin sikkerhetstjeneste som felles tillitsøkende tjeneste for innbygger

I dag har Helsenorge en egen sikkerhetstjeneste kalt Innbygger-STS. Denne har som funksjon å være en tillitstjeneste for interne og eksterne API-er hvor innbygger eller en som representerer innbygger er pålogget via ID-porten. I tillegg har den støtte for single sign-on mellom Helsenorge og andre eksterne webbaserte tjenester som er linket til i Helsenorge.

Sikkerhetstjenesten er i dag designet til å dekke Helsenorge sitt behov for datadeling:

- Helsenorge sitt bruk av interne API-er hvor Helsenorge er klient
- Helsenorge sitt bruk av eksterne API-er hvor Helsenorge er klient
- Andre e-helseløsningers bruk av Helsenorge sine API-er hvor de kan lagre informasjon om innbygger som de selv administrerer

Sikkerhetstjenesten fungerer allerede i dag som en tillitstjeneste for å gi innbygger tilgang til sine helseopplysninger via API-er hos andre virksomheter.

Tjenesten bør utvides til å også støtte samtykkebasert tilgang hvor en applikasjon ber om samtykke fra innbygger til å behandle innbyggers helseopplysninger via API-er som Helsenorge eller andre e-helseløsninger tilbyr. Dette vil si at tjenesten må støtte følgende tillitsøkende tjenester:

1. En felles autentiseringsløsning for applikasjoner som bruker ID-porten for å få tilgang til API-er på vegne av innbygger
2. Felles klientautentisering – en sikker autentisering av forhåndsgodkjente klienter

3. Felles klientautorisering – håndheving av autorisasjoner som en klient har blitt godkjent for å benytte (inkludert håndtering av samtykke fra innbygger).

I tillegg må den ha integrasjon med sentral fullmaktsløsning og felles samtykkeløsning

I "Plan for utvikling av felles grunnmur" [11] er denne komponenten identifisert som en mulig fellestjeneste for helse- og omsorgstjenesten.

Arkitekturvalg 2

Målarkitekturen legger til grunn at Helsenorge sin sikkerhetstjeneste skal være en felles tillitstjeneste for å:

2a) autentisere innbyggere eller en som representerer han/hun via ID-porten

2b) autentisere og autorisere klienter som en API-eier **kan** velge å benytte for å tilby API-er til innbyggerbenyttede applikasjoner.

6.3.4 Vurdering av personvernkomponenten som en felles tillitsøkende tjeneste for fullmakt, samtykke, sperringer og reservasjon

Helsenorgeplattformen har etablert en personvernkomponent som dekker tillitstjenestene fullmakt, samtykke, sperringer og reservasjon. I "Plan for utvikling av felles grunnmur" [11] er denne komponenten identifisert som en mulig fellestjeneste for helse- og omsorgstjenesten. For hver tillitstjeneste vil vi vurdere behovet for å etablere en fellestjeneste for grunnmuren basert på personvernkomponenten.

6.3.4.1 Fullmakt

Behov for håndtering av fullmakter er avgrenset til bruksområdet "Innbyggers deltagelse og innsyn i sin helsehjelp". I dag kan en innbygger på Helsenorge bruke tjenestene på andres vegne. Hvem en innbygger kan representere hentes fra fullmaktsløsningen i personvernkomponenten til Helsenorge. Samme løsning har også funksjonalitet hvor en innbygger kan administrere hvem som kan representere en selv. I tillegg er det støtte for fullmakt regulert av foreldreansvar hvor folkeregisteret er autoritativ kilde. Når folkeregisteret får støtte for informasjon om verge, kan også personvernkomponenten innføre støtte for representasjon knyttet til verge.

Det pågår også et arbeid nasjonalt om å lage en felles offentlig fullmaktsløsning hvor målet er at det skal for innbyggeren oppleves som en helhetlig håndtering av fullmakter på tvers av offentlige sektorer. Altinn er valgt som felles løsning hvor innbygger skal kunne få en oversikt over alle fullmakter som innbygger har gitt uavhengig av sektor. I tillegg skal det lenkes til løsningene hvor innbygger kan administrere de enkelte fullmakter.

Vi legger dette arbeidet til grunn for målarkitekturen. Personvernkomponenten skal benyttes som kilde for representasjon av innbyggere og API-eiere må stole på denne (via Innbygger-STS)

Innbygger har rett til innsyn i hva en fullmaktshaver har fått tilgang til av sine helseopplysninger og det er derfor et krav om at alle API-eiere må logge representasjonsforholdet når det gis tilgang til en innbyggers helseopplysninger.

6.3.4.2 Samtykke

Av behovsvurderingen kom det frem at behovet for en samtykkeløsning er gjeldende for alle bruksområdene og det bør derfor vurderes å etablere en fellestjeneste for håndtering av samtykke som en del av grunnmuren. I dag dekker samtykketjenesten til Helsenorge kun tjenester som er tilgjengelig gjennom Helsenorge og den mangler støtte for samtykkeprosesser som er knyttet til datadeling.

Behovet for en samtykkeløsning ved deling av data er også gjeldende for tverrsektoriell samhandling og det bør derfor tilstrebes at helse- og omsorgstjenesten ikke etablerer egen sektoriell løsning, men benytter en nasjonal løsning.

Altinn har i dag en løsning for håndtering av samtykke ved deling gjennom API. Et eksempel på dette er samtykkebasert lånesøknad hvor banker henter inn samtykke via Altinn fra låneøker om å innhente skattedata fra Skatteetatens API. Forutsetningen for denne tjenesten er at du som API-eier er en offentlig virksomhet og at alle API-er må registreres som en lenketjeneste i deres tjenesteutviklingsplattform. Foreløpig dekker ikke denne løsningen helse- og omsorgstjenesten sine behov og det anbefales i målarkitekturen at helse- og omsorgstjenesten inntil videre etablerer egen løsning, men at den på et senere tidspunkt kan enten integreres eller byttes ut med en nasjonal samtykketjeneste.

Arkitekturvalg 3

Målarkitekturen legger til grunn at det etableres en felles samtykkeløsning for helse- og omsorgstjenesten, basert på samtykkeløsningen etablert på Helsenorge.

Løsningen må på sikt kunne enten integreres eller byttes ut med en nasjonal samtykkeløsning.

6.3.4.3 Sperringer

Når en pasient ønsker å sperre sin journal for et navngitt helsepersonell, bør det forutsettes at pasienten ønsker å sperre alle sine journaler for denne personen, ikke bare i virksomheten som pasienten kontakter. Et helsepersonell kan jobbe i flere virksomheter og i tillegg kan helsepersonell bytte arbeidsgiver. Vi har diskutert om målarkitekturen bør inkludere et nasjonalt sperreregister hvor alle sperringer blir lagret og distribuert til den enkelte virksomhet som har lagret helseopplysninger for gjeldende pasient. Dette vil også kreve implementering av felles struktur og nivå på sperringer i de enkelte løsningene. I dag kan ikke en virksomhet kreve at en sperring også blir nedtegnet og overholdt av andre virksomheters EPJ-er. Et nasjonalt sperreregister kan da ikke inneholde offisielle sperrer, dette må i henhold til dagens praksis nedtegnes i den enkeltes pasientjournal. Dette medfører at et slik nasjonalt sperreregister ikke anbefales etablert nå.

I dag kan man gjennom Helsenorge sin personverntjeneste legge inn sperringer på opplysninger i Kjernejournal og resepter på Reseptformidleren.

Arkitekturvalg 4.1 og 4.2

1. Målarkitekturen legger til grunn at det IKKE etableres et nasjonalt sperreregister for helse- og omsorgssektoren for sperrer. Sperrer anses som en del av journal og må håndheves av den enkelte dataansvarlig/API-eier.
2. Målarkitekturen legger til grunn at alle grunnmurskomponenter og nasjonale e-helseløsninger benytter Helsenorge sin personverntjeneste for administrasjon av sperringer.

Selv om pasienten har motsatt seg deling, har helsepersonell etter helsepersonelloven § 45 mulighet for å overstyre dette dersom det er påkrevd ut fra kravet til forsvarlig helsehjelp. Dette følger av lovkommentarene til bestemmelsen. Det må derfor også etableres mekanismer i datadeling hvor dette kan gjennomføres.

6.3.4.4 Administrasjon av sperringer

Siden det i målarkitekturen ikke etableres et nasjonalt sperreregister for offisielle sperrer, må løsning for administrasjon av sperringer forenkles. Det bør legges til rette for at det lages en nasjonal tjeneste hvor pasient kan sende anmodninger om å legge inn/fjerne en sperre for deling av sine helseopplysninger direkte til virksomhetene selv. Dette kan gjøres ved at det lages en løsning på Helsenorge hvor pasienten får opp en liste over hvilken virksomhet som har en journal (forutsetter etablering av en pasientinformasjonslokalisator) og hvor pasienten kan sende en anmodning om sperring til de virksomheter som pasienten ønsker skal legge inn en sperring. Hver virksomhet må da etablere et mottak for håndtering av sperreanmodninger. Konseptet kan også utvides med bruk av standardiserte API-er som Helsenorge kan benytte for å hente ut registrerte sperringer hos den enkelte virksomhet. Det bør også vurderes om kopier av offisielle sperringer hos en virksomhet kan lagres i Personlig Helsearkiv på Helsenorge.

Ønsker pasienten å gjøre unntak fra sperringen, skal dette også være mulig. Det må da være mulig å registrere at pasienten har samtykket til at det gis tilgang til sperrede opplysninger og at kravet om sperring midlertidig er trukket tilbake.

6.3.4.5 Reservasjoner

I dag har Helsenorge sin personverntjeneste støtte for behandling av reservasjoner. Denne støtten går ut på at pasienter kan elektronisk reservere seg mot enkelte nasjonale e-helsetjenester, slik som Kjernejournal og automatisk frikort for helsetjenester.

Behovet for å håndtere reservasjoner er nært knyttet til nasjonale e-helsetjenester som har egne lovhjemler for behandling av helseopplysninger. Det er i liten grad behov innen datadeling for en felles tjeneste for håndheving av reservasjoner.

Arkitekturvalg 5

Målarkitekturen legger til grunn at nasjonale e-helseløsninger som må ha støtte for håndtering av reservasjoner må, ved bruk av datadeling, håndtere dette i sin egen løsning eller benytter Helsenorge sin tjeneste for dette og at det ikke er behov for å etablere en felles nasjonal tjeneste i helse- og omsorgstjenesten for håndtering av reservasjoner.

6.3.5 Felleskomponent for API-katalog

Det er viktig at de som har behov for API-er lett kan søke og finne relevante API-er samt forstå bruken av API-ene. Det må derfor tilrettelegges for å publisere slik informasjon.

Dette kan gjøres gjennom en API-katalog. En slik katalog jobbes det med å etablere nasjonalt. Gjennom et samarbeid mellom Brønnøysundregistrene, DigDir og øvrige SKATE-etater etableres det en felles offentlig API katalog på felles datakatalogportalen.

Figur 7 Behovsvurdering av felles API-katalog				
Fargeforklaring: se Tabell 2	Sektorens samhandling med grunnmur og nasjonale e-helseløsninger	Innbyggers deltagelse og innsyn i sin helsehjelp	Samhandling mellom helsepersonell i ulike virksomheter	Samhandling mellom helsepersonell gjennom bruk av ny teknologi
Behov for felles API-katalog				

Arkitekturvalg 6

Målarkitekturen legger til grunn at alle API-eiere i helse- og omsorgstjenesten publiserer informasjon om sine API-er i API katalogen til felles datakatalog som forvaltes av Brønnøysundregistrene.

6.3.6 API managementløsning

API management er en sentral del av målarkitekturen for datadeling i helse- og omsorgstjenesten. I dette kapittelet ser vi nærmere på hvilket bruk av API management som har størst nytteverdi for helse- og omsorgstjenesten.

Wikipedia definerer API management som: "*The process of creating and publishing web APIs, enforcing their usage policies, controlling access, nurturing the subscriber community, collecting and analyzing usage statistics, and reporting on performance. API Management components provide mechanisms and tools to support developer and subscriber community."*

Produktleverandører som leverer API managementprodukter fokuserer normalt på at en API managementløsning skal dekke en virksomhet sine behov for å forvalte og drifte sine eksponeringer av API-er eksternt og internt. I målarkitekturen tenker vi at API management skal dekke felles behov som flere API-eiere har, ikke bare for en virksomhet.

6.3.6.1 Felles API managementløsning

I arbeidet med målarkitekturen har vi diskutert hvordan felles API management-behov skal løses. Skal vi etablere en felles sektorløsning som alle virksomheter må tilby sine API-er i eller skal hver virksomhet ha ansvar for å etablere sin egen API management løsning?

Konklusjonen av diskusjonen var at helsesektorens virksomheter vil ha forskjellige behov som gjør det vanskelig å etablere kun en felles løsning for hele sektoren. Det var enighet i at det bør i første omgang gjøres en anskaffelse av en felles API managementløsning som dekker behovene til de nasjonale e-helseløsninger og grunnmurskomponenter med mulighet for at andre virksomheter også kan benytte samme løsning.

Det ble videre konkludert med at målarkitekturen i dette dokumentet skal avgrense felles API managementløsning til minimum å dekke :

- Bruk av API-er til grunnmurstjenester og nasjonale e-helseløsninger
    - Både helsepersonell og innbyggers bruk
- Andre virksomheter med API-er skal kunne benytte felles API managementløsning dersom de ikke ønsker selv å etablere egen API managementløsning

Som en konsekvens av denne konklusjonen må komponentene i en felles managementløsning både kunne produksjonssettes som en felles komponent dersom dette er hensiktsmessig eller som distribuerte komponenter. I en API managementløsning er API gateway en viktig komponent. Det er for eksempel anbefalt at denne komponenten bør etableres så nære API-ene som mulig og det vil derfor være behov for å produksjonssette en eller flere slike komponenter per API-eier.

Selv om realiseringen av en felles managementløsning vil medføre produksjonssetting av mange distribuerte komponenter vil vi omtale felles API managementløsningen som en løsning og som en grunnmurskomponent videre i dette dokumentet.

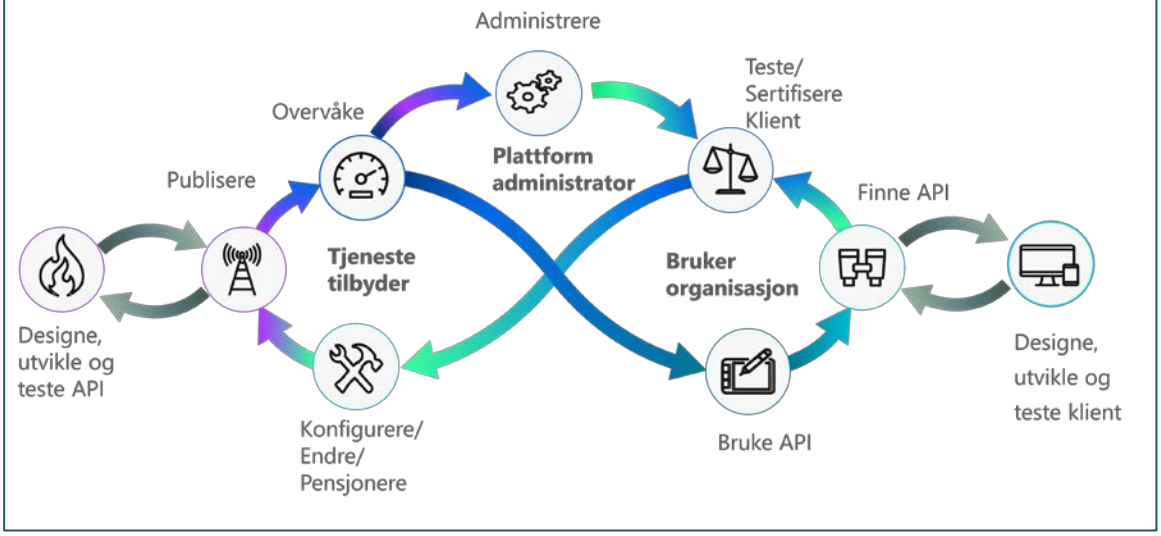
I diskusjonene kom det også innspill på at anskaffelsen av et felles managementprodukt bør gi mulighet for at andre virksomheter bør kunne avrope fra samme avtale for å etablere sin egen API managementløsning. Svaret på dette innspillet er holdt utenfor dette dokumentet.

6.3.6.2 Prosess for bruk av felles API managementløsning

En felles API managementløsning må støtte prosesser hvor ulike tjenestetilbydere kan publisere, overvåke, forvalte sine eksponerte API-er og brukerorganisasjoner kan finne, teste, sertifisere og bruke API-er fra tjenestetilbydere i sine klienter. I tillegg er det behov for prosesser for overvåking og analyse, administrasjon og teste/sertifisere klienter som en plattformadministrator har ansvaret for. Funksjonalitet for design, utvikle og teste selve API-ene og klientene er ikke en del av en felles API managementløsning.

Figur 8 viser en oversikt over rollene og funksjonalitet som de ulike rollene har behov for på overordnet nivå.

Figur 8 Prosess for bruk av felles API managementløsning



6.3.6.3 Komponenter i en felles API managementløsning

I "Referansearkitektur for datadeling" [1] er det beskrevet hvilke generiske komponenter en API managementløsning består av. Dette er gjengitt i Figur 9.

Figur 9 Byggeklosser og deres ansvar (ikke uttømmende)

API gateway	• Hoste API-proxyer som vil være første kontaktpunkt for publiserte API-er • Beskytte mot inntrenging og andre trusler • Håndtere volumbegrensninger og andre abonnementsordninger • Håndheve tilgangsstyring • Samle inn data om bruken av API-er
API manager	• Sentralisert API administrasjon og forvaltning av API-katalogen • Håndtering av registrerings- og introduksjonsprosesser for API utviklere • Håndtere livssyklusen til et API
API monitorering og analyse	• Monitorere bruken av API-er • Generere rapporter og analyser over bruk som eventuelt kan kobles til eventuelt fakturering av bruk • Konsekvensutrede versjonsendringer (oppdatere, utfase osv)
API utviklingsportal	• Håndtere abonnement og avtaler • API-katalog • Info om dagens bruk • Dokumentasjon av API-ene • Diskusjonsfora, support og testmiljøer

6.3.6.4 Bruksområdene for datadeling sine behov for en felles API-managementløsning

Bruksområdene definert i kapittel 5.1 har alle behov for API-management. Men ikke alle har behov for en sektorfelles API managementløsning. Vurderingen er vist i Figur 10.

Figur 10 Bruksområdene sine behov for en felles API-managementløsning		
Sektorens samhandling med grunnmur og nasjonale e-helseløsninger		• Eiere av nasjonale tjenester har behov for felles governance av bruk av API-er • Det er en stor gevinst å samordne behovene i en felles løsning. • Sektoren får «one stop shopping» av API-er mot nasjonale tjenester. • Leverandørmarkedet får større mulighet til innovasjon
Innbyggers deltagelse og innsyn i sin helsehjelp		• Markedet har behov for tilgang til å utvikle mot sektorens API-er, fellestjenester/nasjonale løsningers API-er og API-er til innbyggertjenestene på Helsenorge • Hensiktsmessig og innovasjonsfremmende å ha felles håndtering av API-er på tvers av alle regioner og kommuner (avtaleverk, felles plattformadministrator, sikkerhet og personvern)
Samhandling mellom helsepersonell i ulike virksomheter		• Mindre behov for en felles API-managementløsning • Kan gjenbruke samme produkt for å dekke egne behov • Enkelte delkomponenter er det allikevel behov for å ha felles slik som API-katalog
Samhandling mellom helsepersonell gjennom bruk av ny teknologi		• Behov for at "inhouse" og eksterne leverandører får tilgang til å utvikle mot en virksomhet eller en gruppe av virksomheter sine interne/eksterne API-er. • Mindre behov for en felles API-managementløsning • Kan gjenbruke samme produkt for å dekke egne behov • Enkelte delkomponenter er det allikevel behov for å ha felles slik som API-katalog

Arkitekturvalg 7

Målarkitekturen legger til grunn at:

7a) det må etableres en felles API-managementløsning som tilbyr sektoren tilgang til API-ene til grunnmurskomponenter og nasjonale e-helseløsninger.

7b) det må etableres en felles API-managementløsning som tilbyr leverandørmarkedet tilgang til sektorens API-er, fellestjenester/nasjonale løsningers API-er og API-er til innbyggertjenestene på Helsenorge

7c) andre virksomheter etablerer, sammen med andre eller egen, API managementløsning.

6.3.7 Samspill mellom Felles API managementløsning og HelseID/Innbygger-STS

I arbeidet med målarkitekturen er det identifisert ansvarsoverlapp mellom hva HelseID eller Innbygger-STS kan ha av ansvar kontra hva en felles API managementløsning kan ha av ansvar. Konkret går dette på tillitstjenestene klientautentisering og – autorisering som beskrevet i 6.3.1.4 heretter kalt STS-tjeneste.

Et av spørsmålene vi har diskutert er om det er mulig å bli enige generelt om hvilken felleskomponent har hvilket ansvar.

Vi har sett på følgende alternativer:

6.3.7.1 Alternativ 1: STS-tjeneste har ansvaret for både klientautentisering og –autorisering

Dette forutsetter at STS-tjenesten må ha et forhold til alle klientene og API-er som registreres i Felles API managementløsning. I tillegg kreves det en kobling mellom klientkonfigurasjoner i STS-tjenesten og Felles API managementløsningen slik at en godkjent klient i STS-tjenesten kan kobles til en konfigurasjon i API managementløsningen.
I en API managementløsning er det normalt å ha støtte for funksjonalitet til å søke API-eier om tilgang til sitt API. Siden tilgang til API må angis i STS-tjenesten, må også API-eiers godkjennelse av en søknad registreres i STS-tjenesten. Dette må enten løses med integrasjon mellom løsningene, dvs at API managementløsningen må oppdatere STS-tjenesten via et API eller ved at det manuelt registreres i selvbetjeningsløsningen til STS-tjenesten. Oppsummert må *administrasjon* av hvilken klient som har tilgang til hvilket API da håndteres i begge løsningene.
Dette alternativet kan også dekke andre scenarioer hvor API-eier ikke benytter en API managementløsning hvor da søknad om tilgang til API må gjøres på annen måte.

6.3.7.2 Alternativ 2: Felles API management har ansvaret for både klientautentisering og –autorisering

STS-tjenesten benyttes da som en identitetstilbyder og Felles API managementløsningen må selv ha funksjonalitet for klientautentisering og –autorisering og å utstede sikkerhetsbilletter. Dette krever at løsningen må ha en egen lokal STS-tjeneste som utsteder sikkerhetsbilletter. Dette alternativet medfører at klientene med stor sannsynlighet må ha en klientkonfigurasjon hos sentral STS-tjenesten i tillegg for at den skal kun utstede sikkerhetsbilletter til forhåndsgodkjente klienter.
Dette alternativet vil også kreve at andre API-eiere som ikke benytter Felles API managementløsning må etablere sin egen klientautentisering og –autorisering. Et eksempel på dette kan være helseregioners opprettelse av egne regionale løsninger for API management og STS-tjeneste.

Konklusjonen på diskusjonen er at det begge alternativene må kunne støttes i målarkitekturen.

6.3.8 Felleskomponent for oppslag av hvilke virksomheter/løsninger som har helseopplysninger lagret om en gitt pasient

Primærbehovet for datadeling er knyttet til bruk av API-er hvor brukere/klienter har behov for å behandle helseopplysninger for en gitt pasient.

Med over 17000 aktører er det ikke enkelt å vite hvem av disse som har lagret helseopplysninger for en gitt pasient. Det er i en rekke situasjoner tilknyttet datadeling behov for å kunne fremskaffe en liste over hvilke systemer som har en pasientjournal for en gitt pasient. For innbygger er det fire sentrale problemstillinger som har et behov for å vite i hvilke systemer som har en pasientjournal for en gitt pasient:

Problemstilling	Beskrivelse	Mulig løsning
Hvor er data lagret om meg?	Innbyggere har i dag ikke oversikt over dette og det er ingen mulighet for å skaffe en slik oversikt	Dersom alle virksomheter med plikt til å føre pasientjournaler meldte om dette til en grunnmurskomponent, kunne vi presentert dette for innbygger og personell med tjenstlig behov.
Jeg vil se hva som er lagret om meg	Innbyggere ønsker digitalt innsyn. Skal dette tilbys via Helsenorge, så krever det at Helsenorge må ha tilgang til en oversikt over hvem som har helseopplysninger om den innloggede innbygger.	I dokumentdeling er dette tenkt løst gjennom nasjonale søk etter metadata om journaldokumenter Men vi trenger dette også for FHIR ressurser når dette blir mer utbredt. For å få til dette må hver virksomhet registrere hvilke pasienter de har lagret info om (eventuelt også tilby et API som beskriver hvilke ressurser som er tilgjengelig for en gitt pasient).
Hvem har sett på mine data?	Innbyggere har rettmessig krav om å se hvem som har behandlet dataene sine. Innbyggere ønsker digitalt innsyn i dette. Helsenorge bør vise denne oversikten.	Det vil finnes mange løsninger som har brukslogg over hvem som har fått tilgang til en pasients helseopplysninger. Med standardiserte API-er for å uthente dette, kan Helsenorge hente og vise denne informasjonen. Men det krever at Helsenorge har en oversikt over hvem som har lagret helseopplysninger om aktuell pasient.
Jeg vil motsette meg deling av mine data	Innbyggere har rett til å motsette seg deling av sine data til navngitte personer, grupper eller virksomheter (sperrer). Dersom Innbygger ikke vet hvor det er lagret helseopplysninger, så er innbygger i mindre grad i stand til å ivareta sine rettigheter. Helsenorge bør tilby muligheter for å søke om sperringer hos de virksomheter som har lagret informasjon om en innbygger	Dersom Helsenorge kan få en oversikt over hvilke virksomheter som har informasjon om en innbygger, så kan den tilby funksjonalitet for en innbygger hvor den kan velge til hvilke virksomheter innbygger kan sende forespørsler om sperringer.

Et slikt register bør etableres som en felleskomponent hvor alle behandlingsrettede helseregistre må være registrert. Vi har valgt å kalle denne felleskomponenten for pasientinformasjonslokalisator, forkortet til PIL.

Ved en realisering av PIL må det tas stilling til om lagring av slik informasjon krever eget behandlingsgrunnlag i form av en forskrift. En lignende komponent for helseregisteret er tidligere prøvd etablert, kalt Oppføringsregisteret. Dette registeret hadde som formål å kunne gi oversikt over hvilke helseregistre en innbygger er oppført i. Siden Oppføringsregisteret ikke hadde behandlingsgrunnlag for å lagre helsedata, så måtte løsningen designes slik at den hentet all informasjon fra helseregistrene.

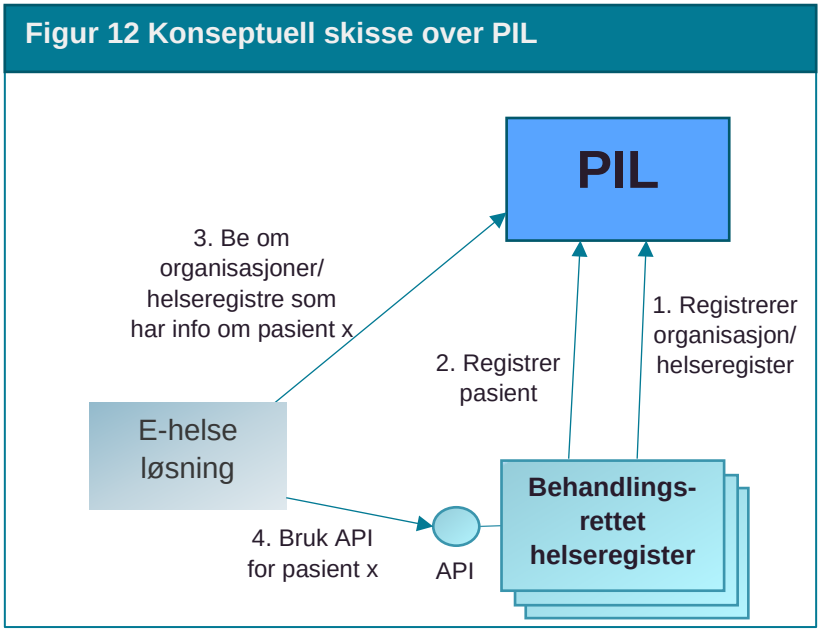
Kjernejournal har hjemmel for å lagre en pasients besøkshistorikk i helse- og omsorgstjenesten med begrensninger i hvor lenge ulike besøk skal kunne lagres. Vår vurdering er at denne historikken ikke vil gi en tilstrekkelig oversikt over hvor det ligger helseopplysninger om en pasient.

Figur 11 Behovsvurdering av PIL

Fargeforklaring: se Tabell 2	Sektorens samhandling med grunnmur og nasjonale e-helseløsninger	Innbyggers deltagelse og innsyn i sin helsehjelp	Samhandling mellom helsepersonell i ulike virksomheter	Samhandling mellom helsepersonell gjennom bruk av ny teknologi
Behov for felles pasientinformasjons-lokalisator				

Figur 12 viser konseptet bak PIL hvor e-helseløsninger kan bruke PIL til å skaffe en oversikt over hvilke virksomheter som har lagret helseopplysninger om en gitt pasient. Dette forutsetter at virksomhetene registrerer alle pasienter de har journaler på.

Figur 12 Konseptuell skisse over PIL



Arkitekturvalg 8

Målarkitekturen legger til grunn at det etableres en pasientinformasjonslokalisator (PIL) som en felleskomponent i grunnmuren hvor alle virksomheter som eksponerer API-er registrerer hvilke pasienter API-ene har data. Dette gjelder også aktuelle grunnmurskomponenter og nasjonale e-helseløsninger.

6.3.9 Felleskomponent for logging og innsyn i brukslogg

I "Retningslinjer for logging ved data- og dokumentdeling"[9] er det beskrevet ulike formål og behov for logging ved bruk av datadeling. Flere av disse formålene må dekkes av den enkelte virksomhet, slik som "teknisk feilsøking". Men for flere av formålene er det nødvendig å se alle involverte parter i en sammenheng og bestemme hvilken part har hvilke ansvar. I tillegg kan det være behov for å etablere noen felleskomponenter.

Følgende formål er vurdert dekket med felleskomponenter i målarkitekturen:

1. **Etterprøve tjenstlig behov:**
   Som dataansvarlig skal jeg ha tilgang til informasjon om hvilket personell som har hatt tilgang til eller forsøkt å få tilgang til helseopplysninger om pasienter slik at jeg kan vurdere om de har hatt tjenstlig behov for innsynet.
2. **Innsyn til innbygger:**
   Som innbygger skal jeg elektronisk kunne lese og forstå hvem som har hatt tilgang til helseopplysninger om meg, eller en jeg har fullmakt for, og hvorfor, slik at jeg kan vurdere om noen har hatt urettmessig tilgang.
3. **Revisjon av sikkerhetsmekanismer:**
   Som sikkerhetsansvarlig for en data- eller dokumentdelingsløsning skal jeg kunne få informasjon om alle tilgangsbeslutninger som er gjennomført slik at jeg kan se at disse er overens med de formelle avtalene som er gjort mellom de partene vi deler informasjon med.

Når datadeling benyttes, er det mange aktører og systemer involvert. Hver av systemene har krav til logging for å dekke formålene over. Det kan være hensiktsmessig å vurdere om disse kravene kan løses mer i felleskap. En felleskomponent som er vurdert er et felles loggarkiv. Alle systemer som har krav til å logge, må uansett logge til et loggarkiv uavhengig om dette er en del av systemet eller eksternt for systemet. Et slikt loggarkiv må for eksempel beskyttes mot innsyn, har samme krav til lagring av loggmeldinger som helseopplysninger og det må ikke kunne gjøres endringer på registrerte loggmeldinger. I tillegg er det krav om å gi tilgang til pasienter (ref formål 2 over) som vi ønsker å løse digitalt gjennom standardiserte API-er til loggarkivene.

Et nasjonalt loggarkiv for bruk i helse- og omsorgstjenesten vil ikke være hensiktsmessig pga mengden loggmeldinger. Derimot anbefaler vi at aktører går sammen om å samarbeide om å etablere felles loggarkiv for å forenkle ibruktakelsen av datadeling. Det er for eksempel naturlig at grunnmurskomponenter og nasjonale e-helseløsninger som tilbyr API-er bør vurdere å etablere et felles loggarkiv eller om forskriftene de er basert på regulerer krav til logging på en måte som vanskeliggjør et felles loggarkiv.

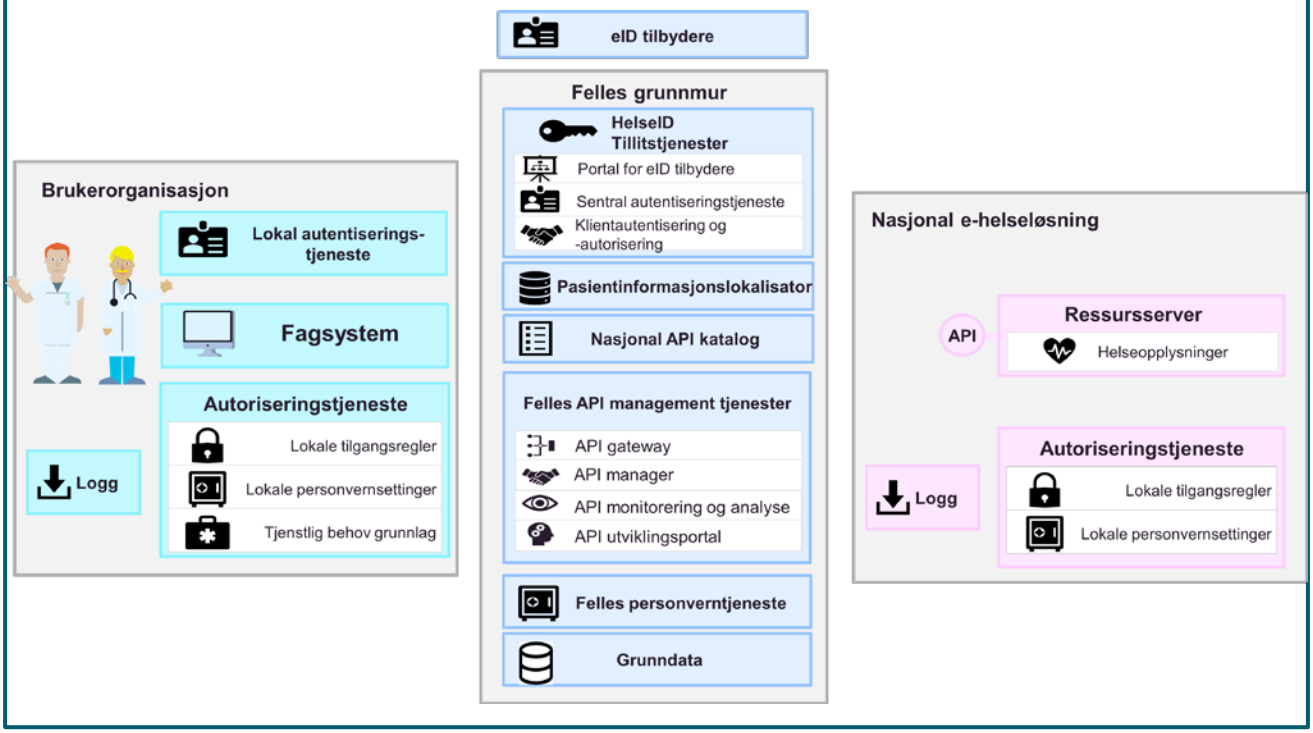
Arkitekturvalg 9

Målarkitekturen legger til grunn at det ikke etableres et nasjonalt loggarkiv for datadeling, men det anbefales at samarbeidspartnere eller andre grupperinger går sammen om å etablere egne felles loggarkiv.

6.4 Målarkitektur for sektorens samhandling med grunnmur og nasjonale e-helseløsninger

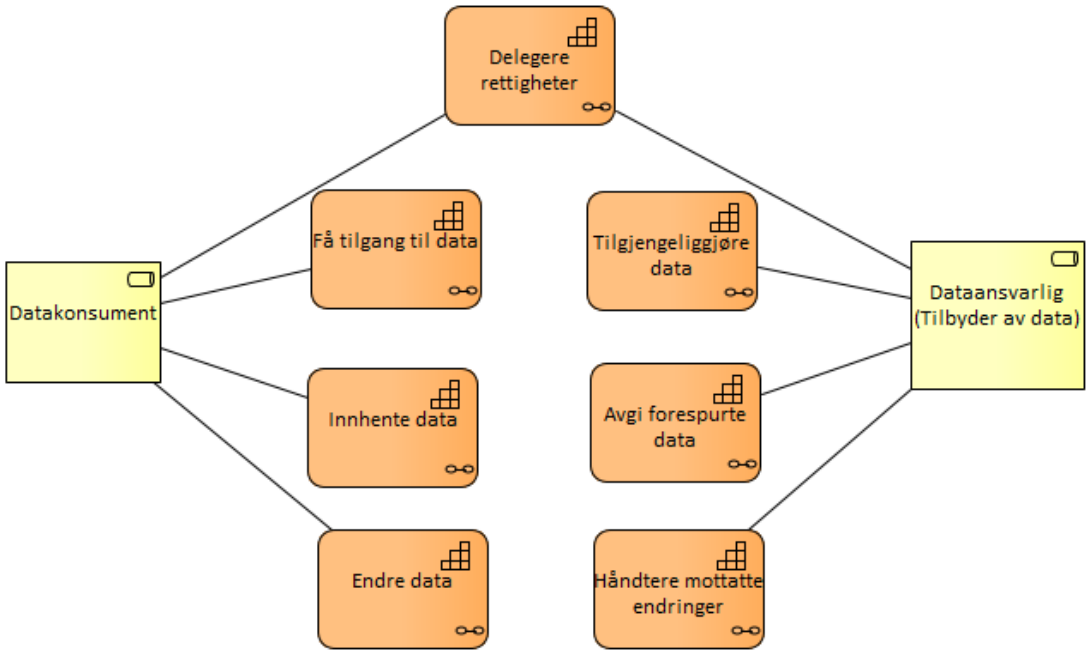
Dette bruksområdet er avgrenset til at brukere er personell (eller systemer) med tjenstlig behov og har behov for å samhandle med helse- og personopplysninger som er lagret i grunnmurskomponenter og/eller i nasjonale e-helseløsninger.

Figur 13 Målarkitektur for sektorens samhandling med grunnmur og nasjonale e-helseløsninger



Figur 13 viser målarkitektur for datadeling for dette bruksområdet med oversikt over involverte løsninger og felleskomponentene som ble introdusert i kapittel 6.3. Vi skal beskrive hvilke roller og ansvar som disse systemene har ved å knytte bruken av systemene til kapabilitetene introdusert i kapittel 6.2.

Figur 14 Hovedkapabiliteter for datadeling

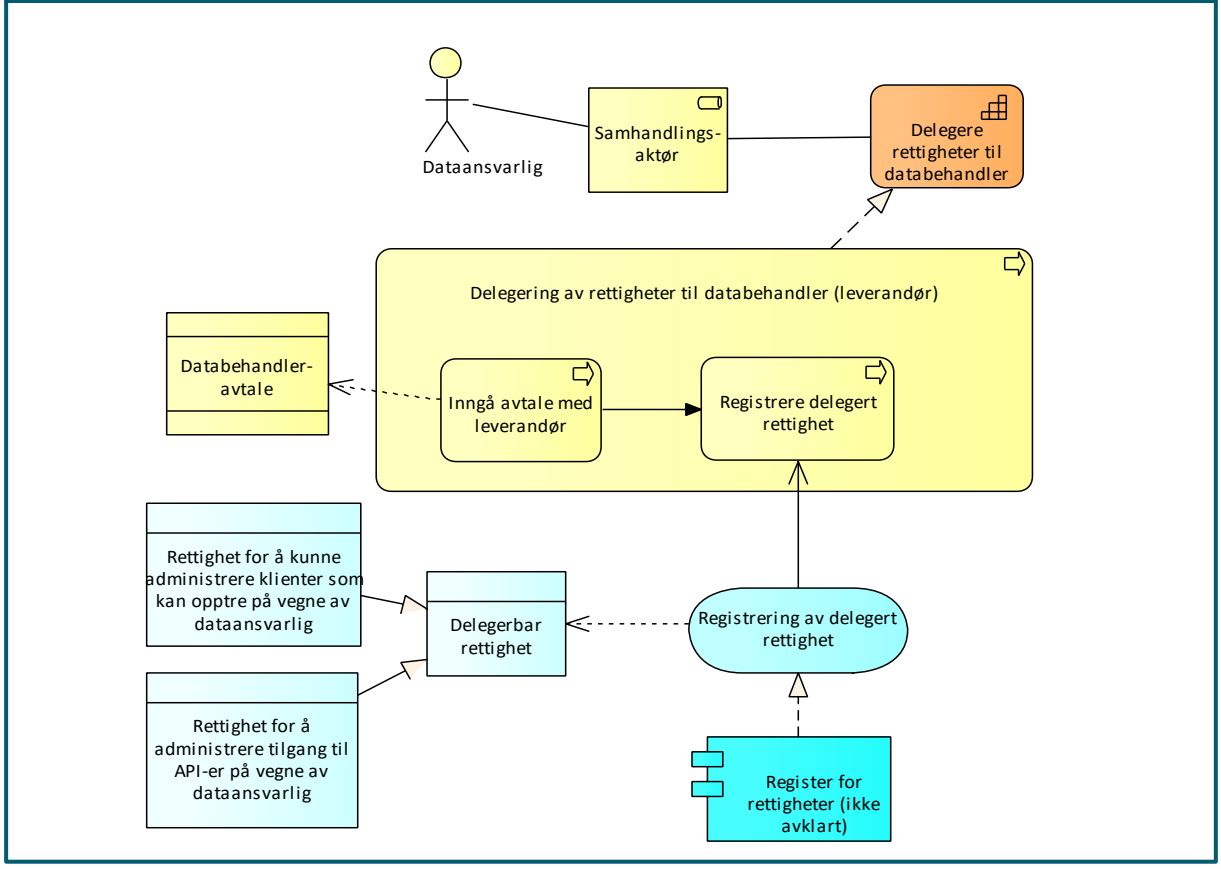


6.4.1 Delegere rettigheter

I mange tilfeller vil det ikke være dataansvarlige som er involvert i den operative delen av datadeling. Dette delegeres ofte til leverandører som inngår databehandlingsavtale med dataansvarlig. Disse delegeringen bør være kjente for enkelte av felleskomponenter for at de skal kunne ha støtte for slike delegeringer.

Figur 15 viser valgt løsningsmønster for målarkitekturen for håndtering av delegerte rettigheter. Når avtale med en databehandler er inngått, må den dataansvarlige registrere de delegerte rettighetene som den ønsker å gi til databehandler slik at dette er tilgjengelig for felleskomponenter som har behov for denne informasjonen. Det vurderes å benytte Altinn Autorisasjon til å administrere slike delegeringer. Løsningsmønsteret dekker delegering av både rettigheter som tilbyder av data og som datakonsument.

Figur 15 Delegering av rettighet til databehandler (leverandør)



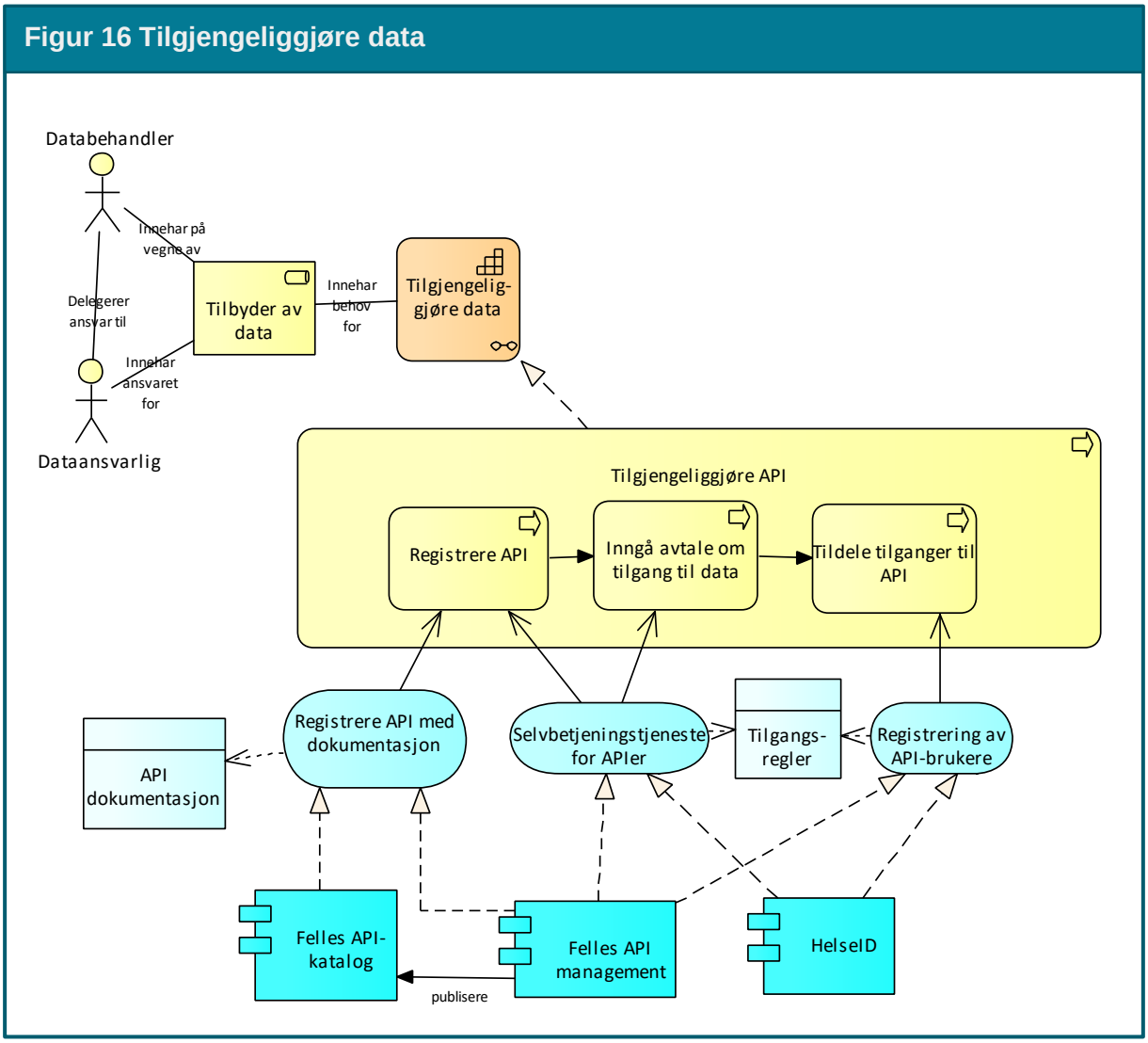
Element	Beskrivelse
Register for rettigheter	Komponent som gir muligheter til å delegere rettigheter til andre organisasjoner eller personer. Rettigheter til bruk av autorisasjonskomponenten må baseres på registrerte roller i Enhetsregisteret. Ikke endelig avklart hvilken løsning som velges. Altinn Autorisasjon er det mest aktuelle valget.
Registering av delegert rettighet	Tjeneste for å registrere en delegert rettighet som gir leverandør mulighet til å opptre på vegne av en dataansvarlig
Delegere rettigheter til databehandler	Evnen til å delegere rettigheter til databehandler som utfører oppgaver på vegne av dataansvarlig.
Samhandlingsaktør	Den som inngår i en samhandlingsprosess og samhandler med en annen samhandlingsaktør. Kan være en tilbyder av data, datakonsument, leverandør etc.
Delegering av rettigheter til databehandler (leverandør)	Prosessen med å delegere rettigheter til databehandler/leverandør.
Inngå avtale med leverandør	Prosessen med å inngå en avtale med leverandør. En slik avtale vil normalt være inngått tidligere og uavhengig av om man skal ta i bruk et nytt API. En tjenesteavtale med leverandør er en forutsetning for å kunne delegere en rettighet.

Element	Beskrivelse
Registrere delegert rettighet	Prosessen med å delegere rettigheter. I tilknytning til datadeling vil formålet være: 1. å gi leverandør tilgang til å representere datakonsument overfor et API, 2. å gi leverandør tilgang til å representere tilbyder av data overfor datakonsumenter. Registreringen vil potensielt også kunne gjelde for andre områder.
Delegerbar rettighet	Beskrivelse av ressurs, f.eks. et API, som det kan gis rettigheter til gjennom et representasjonsforhold.

6.4.2 Tilgjengeliggjøre data

Figur 16 viser valgt løsningsmønster for å tilgjengeliggjøre data for andre virksomheter gjennom bruk av datadeling. For dette bruksområdet vil tilbyder av data være dataansvarlige for nasjonale e-helseløsninger.

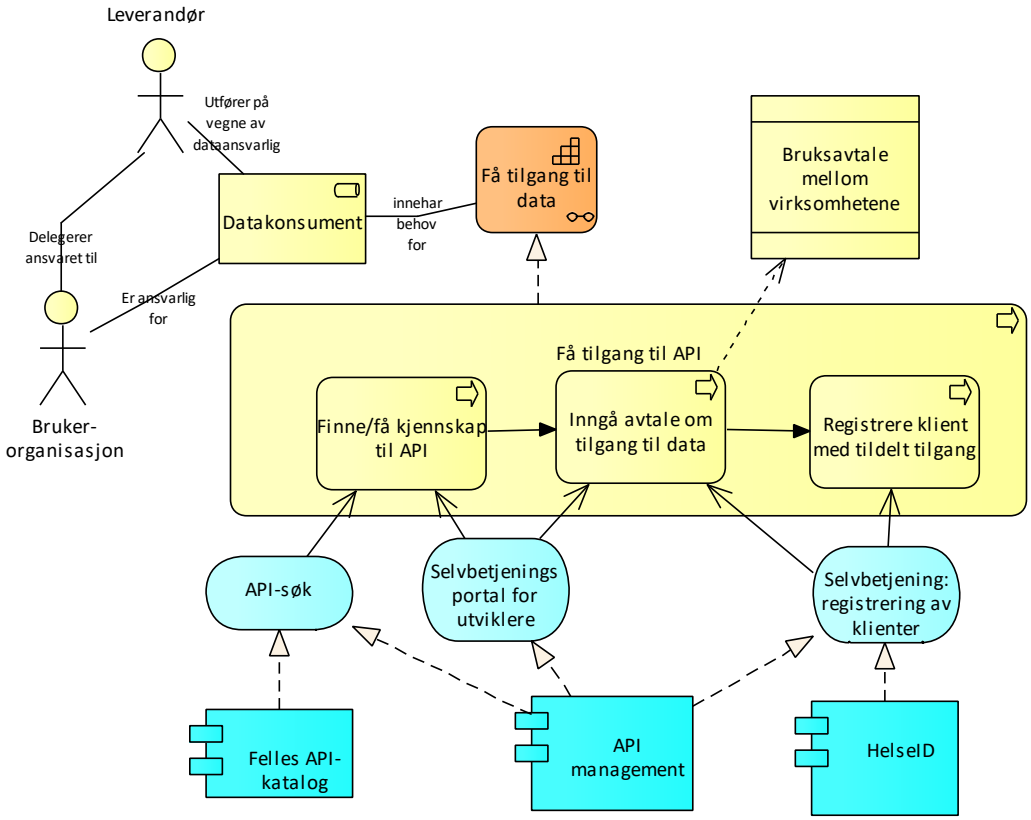
Figur 16 Tilgjengeliggjøre data



Element	Beskrivelse
Tilgjengeliggjøre data	Evnen til å gjøre data tilgjengelig for aktører utenfor egen virksomhet.
Tilbyder av data	En nasjonal aktør som tilbyr data til eksterne parter , enten på vegne av andre, som forvalter av data eller som dataansvarlig.
Tilgjengeliggjøre API	Prosessen med å tilby data gjennom et API til aktører utenfor egen virksomhet.
Registrere API	Prosessen med å registrere et API i relevante tjenester, Felles API-katalog, Felles API management og HelseID.
Inngå avtale om tilgang til data	Prosess for å inngå avtale om tilgang til og bruk av data.
Tildele tilganger til API	Prosessen med å registrere hvilke datakonsumenter som skal få tilgang til å kalle et API.
Registrere API med dokumentasjon	Tjeneste i Felles API-katalogen og i Felles API managementløsning for å registrere API og dets dokumentasjon. Bruk av tjenesten forutsetter at rettigheter til å gjøre dette på vegne av tilbyders virksomhet.
Selvbetjeningstjeneste for APIer	Tilbyder av API-et må konfigurere sikkerhet og andre operasjonelle forhold. En databehandler kan ha rettigheter til å administrere på vegne av tilbyder.
Registrering av API-brukere	Selvbetjeningstjeneste for å registrere og vedlikeholde tilgangene som datakonsumenter skal ha til API-et
Tilgangsregler	Regler for et API som beskriver hvilke tilganger en datakonsument (representert ved organisasjonsnummer) og deres klienter skal ha tilgang til (utstedt token for).
HelseID	Fellesløsning for API-sikring for helsesektoren. Den tilbyr selvbetjening av API-er og utstedelse av OAUTH2-tokens som gir forhåndsgodkjente klienter tilgang til å kalle et API.
Felles API-katalog	Del av Felles datakatalog som gir mulighet for å registrere API-er og dens dokumentasjon via enten et selvbetjeningsgrensesnitt eller via API-er som en API managementløsning kan benytte. https://fellesdatakatalog.brreg.no/apis
Felles API management	Fellesløsning løsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter.
API dokumentasjon	Dataobjekt som dokumenterer et API inkludert adresse og operasjoner som tilbys.

6.4.3 Få tilgang til data

Figur 17 Få tilgang til data

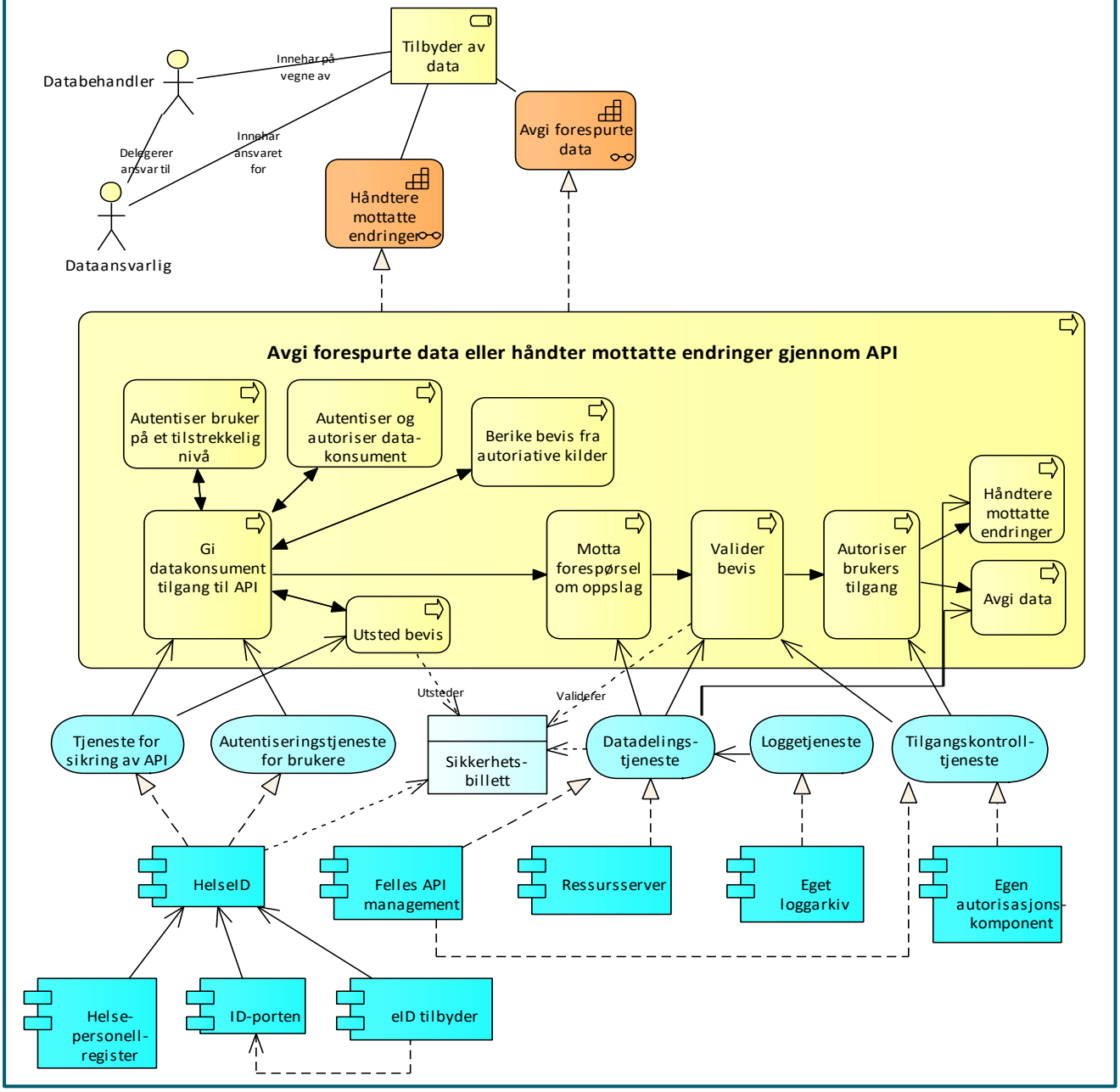


Element	Beskrivelse
Få tilgang til data	Evnen til å skaffe seg tilgang til tilbudte data fra annen aktør.
Datakonsument	Virksomheten som konsumerer data gjennom bruk av API.
Få tilgang til API	Hovedprosessen med å skaffe seg tilgang til tilbudte data fra annen aktør. Omfatter å finne API-er, inngå nødvendige avtaler og få tilganger.
Finne/få kjennskap til API	Prosessen med å finne eller få kjennskap til tilgjengelige API-er gjennom relevante kataloger og søkeløsninger.
Inngå avtale om tilgang til data	Prosess hvor konsumenten inngår eventuell avtale med tilbyder om tilgang til data.
Registrer klient med tildelt tilgang	Prosess for konsument å registrere (provisjonering av) den klienten som skal ha tilgang til API-et ved bruk av sikkerhetsbillett. Dette forutsetter at konsumenten har avtale om bruk av sikkerhetsbillettjenesten og at tilbyder har gitt konsumenten tilgang.

Element	Beskrivelse
	Dersom det er en leverandør som har blitt delegert rettigheter som databehandler på vegne av konsument er det leverandøren som registrer sin klient.
Felles API management	Fellesløsning løsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter.
Felles API-katalog	Del av Felles datakatalog som gir mulighet for å søke etter API-er og lese API-spesifikasjoner https://fellesdatakatalog.brreg.no/apis
HelseID	Fellesløsning for API-sikring for helsesektoren. Den tilbyr selvbetjening av API-er og utstedelse av OAUTH2-tokens som gir forhåndsgodkjente klienter tilgang til å kalle et API.
API-søk	Tjeneste for å søke etter og finne tilgjengelige API-er
Selvbetjening: registrering av klienter	Tjeneste for å registrere klienter som skal ha tilgang til et gitt API som kan opptre på vegne av datakonsumenten.
Selvbetjeningsportal for utviklere	Tjeneste for utviklere som skal utvikle klienter som benytter de registrerte API-ene. Portalen må beskrive bruk av API-ene inkludert adresse og operasjoner som tilbys.

6.4.4 Avgi forespurte data eller håndter mottatte endringer

Figur 18 Avgi forespurte data eller håndter mottatte endringer



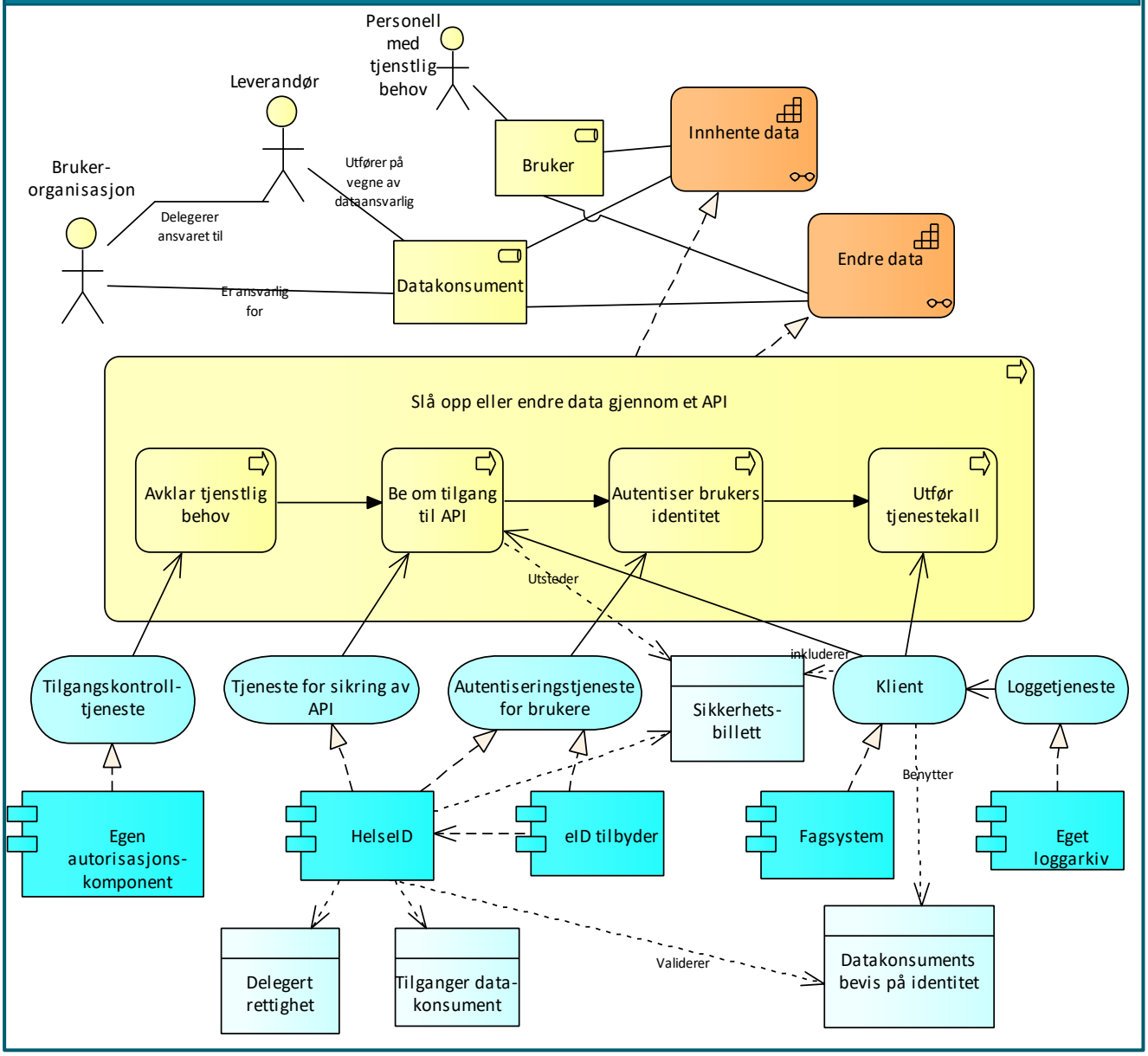
Element	Beskrivelse
Avgi forespurte data	Evne til å avgi data på forespørsel ved hjelp av datadeling.
Håndtere mottatte endringer	Evne til å motta endringer for å opprette, oppdatere eller slette data som er lagret hos den dataansvarlig (NB krever bestemte avtaleforhold)
Tilbyder av data	En aktør som tilbyr data til eksterne parter, enten på vegne av andre, som forvalter av data eller som dataansvarlig.

Element	Beskrivelse
Avgi forespurte data eller håndter mottatte endring gjennom API	Prosessen med å avgi data på forespørsel gjennom et egnet API.
Gi datakonsument tilgang til API	Prosess for å sikre at bruker er autentisert på et tilstrekkelig nivå, datakonsument er autentisert og kontrollert at har tilgang til API-et
Autentiser brukers identitet på et tilstrekkelig nivå	Prosess for å autentisere brukeren basert på en selvvalgt eID på et tilstrekkelig nivå
Autentiser og autoriser datakonsument	Prosess for å sikre at datakonsument er autentisert og har tilgang til API-et
Berike bevis fra autoritative kilder	Prosess for å koble identitet med annen informasjon i andre autoritative kilder som kan benyttes av dataansvarlige til tilgangskontroll av bruker og/eller datakonsument.
Utsted bevis	Prosess for å opprette og gi ut et bevis for at bruker er innlogget, datakonsument er autentisert og autorisert.
Motta forespørsel om oppslag	Prosessen med å motta forespørsler fra API-konsument om å avgi data.
Valider bevis	Prosessen med kontroll og håndheving av konsumentens rettigheter til å få forespurte data. I tillegg til "validering av sikkerhetsbillett", kan det være behov for kontroll mot virksomhetsinterne policies.
Autoriser brukers tilgang	Prosess for å kontrollere om bruker skal gis tilgang til dataene som etterspørres. Kontrollen må baseres på påstander som følger med sikkerhetsbilletten. Kan for eksempel være tilgangsregler slik som "bruker må være lege".
Håndtere mottatte endringer	Prosess for å utføre mottatte endringer. (NB krever eget avtaleforhold med datakonsument)
Avgi data	Prosessen med å gi svar på forespørselen.
Tjeneste for sikring av API	Tjeneste for å sikre at bruker er autentisert, datakonsument er autentisert og har tilgang til API-et.
Autentiserings-tjeneste for brukere	Tjeneste som gir brukeren mulighet til å velge eID tilbyder og logge seg inn hos denne tilbydere med sin eID.
Datadelingstjeneste	Tjenesten som tilbyr API-et til datakonsumenter.
Loggetjeneste	Tjeneste som håndterer krav til audit logging.
Tilgangskontroll-tjeneste	Tjeneste for å sjekke tilgang til data.
Sikkerhetsbillett	Bevis på at autentisering av bruker og datakonsument er gjennomført. Beviset inneholder også påstander om bruker og datakonsument samt hvilken tilgang datakonsumenten har fått til API-et (scope)

Element	Beskrivelse
HelseID	Fellesløsning for API-sikring for helsesektoren. Den tilbyr selvbetjening av API-er og utstedelse av OAUTH2-tokens som gir forhåndsgodkjente klienter tilgang til å kalle et API.
ID-porten	Portal for å tilby nasjonal godkjente eID-er
Felles API management	Fellesløsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter.
Ressursserver	Dataansvarliges system som lagrer helseopplysningene som deles
Eget loggarkiv	Dataansvarliges eget system for håndtering og lagring av audit logg. Kan være en del av ressursserver eller eget selvstendig system
Egen autorisasjons-komponent	Dataansvarliges eget system for håndtering av tilgang til dataene.

6.4.5 Slå opp eller endre data gjennom et API

Figur 19 Slå opp eller endre data gjennom et API



Element	Beskrivelse
Innhente data	Evnen til å innhente data fra en annen aktør via datadeling
Endre data	Evnen til å gjøre endringer hos en annen aktør via datadeling
Datakonsument	Virksomheten som konsumerer data gjennom bruk av API.
Slå opp eller endre data gjennom API	Prosess for en datakonsument å slå opp eller endre data gjennom bruk av et API hos den dataansvarlige
Avklare tjenstlig behov	Prosess for å avklare grunnlaget for å kunne kalle API-et. Datakonsument er ansvarlig for å avklare brukerens tjenstlige behov for å behandle helseopplysninger fra en annen virksomhet.

Element	Beskrivelse
Be om tilgang til API	Prosess for å be om utstedelse av sikkerhetsbillett som gir tilgang til å kalle API-et.
Autentiserer brukers identitet	Prosess for å autentisere brukers identitet på et tilstrekkelig nivå. Dersom bruker allerede er innlogget på et tilstrekkelig nivå hos en godkjent eID tilbyder, trenger ikke bruker å logge inn på nytt.
Utfør tjenestekall	Prosessen med å benytte (gjøre et oppslag mot) et eksternt API.
Tilgangskontroll-tjeneste	Tjeneste for å sjekke brukerens tilgang og tjenstlig behov til å kalle eksterne API-er.
Tjeneste for sikring av API	Tjeneste som utsteder sikkerhetsbilletter. Sikkerhetsbillett utstedes basert på tildelte rettigheter og eventuelle representasjonsforhold.
Autentiserings-tjeneste for brukere	Tjeneste som gir brukeren mulighet til å velge eID tilbyder og logge seg inn hos denne tilbydere med sin eID.
Klient	Tjeneste for å håndtere kall til den eksterne datadelingstjenesten
Loggetjeneste	Tjeneste for å håndtere audit logg
Sikkerhetsbillett	Bevis på at autentisering av bruker og datakonsument er gjennomført. Beviset inneholder også påstander om bruker og datakonsument samt hvilken tilgang datakonsumenten har fått til API-et (scope)
Delegert rettighet	Tjeneste for sikring av API må kontrollere om det foreligger delegerte rettigheter fra ansvarlig virksomhet til en leverandør.
Tilganger datakonsument	Oversikt over hvilke API og OAUTH-scopes en virksomhet (representert ved organisasjonsnummer) skal ha tilgang til (utstedt token for).
Datakonsuments bevis på identitet	En virksomhets elektroniske ID. Benyttes for å autentisere virksomheten overfor tjeneste for sikring av API.
HelseID	Fellesløsning for API-sikring for helsesektoren. Den tilbyr selvbetjening av API-er og utstedelse av OAUTH2-tokens som gir forhåndsgodkjente klienter tilgang til å kalle et API.
eID tilbyder	Tilbyder av elektroniske identiteter som tilfredsstiller nasjonale sikkerhetsnivåer. BankID, Buypass osv. Virksomheter i helsesektoren kan også være eID tilbyder.
Egen autorisasjons-komponent	Datakonsumentens system for å kontrollere brukers tilgang til å kalle eksterne systemer.
Fagsystem	Datakonsumentens system som utgjør klienten
Eget loggarkiv	Datakonsumentens eget system for håndtering og lagring av audit logg. Kan være en del av klienten eller eget selvstendig system

6.5 Innbyggers behandling av sine helseopplysninger

Innbyggere har rett til innsyn i egne helseopplysninger. Det er ingen krav om at slik innsyn skal være digitalt, men Innbyggere har større og større forventninger om at slike opplysninger er digitalt tilgjengelig. I dag har innbygger mer og mer informasjon tilgjengelig på Helsenorge.no og dette vil utvikles enda mer i årene som kommer.

Det bør ikke bare være Helsenorge.no som er forbeholdt å lage innovative innbyggertjenester. Leverandørmarked bør også få tilgang til å utvikle innovative tjenester for innbygger gjennom å tilby innbyggere innovative apps.

Med "innovative" apps menes i dette dokumentet applikasjoner som kan være webbaserte og/eller mobile applikasjoner som utvikles på bestilling eller som innovative satsninger gjort av markedet selv. Slik innovasjon trenger ofte høy grad av selvbetjening for å senke barrierer for å ta i bruk datadeling.

Leverandørmarked bør få tilgang til å utvikle egne applikasjoner mot innbyggerbaserte API-er. Disse API-ene kan være sektorens egne API-er, fellestjenester/nasjonale løsningers sine API-er eller API-er til innbyggertjenestene på Helsenorge.

Leverandørene sine applikasjoner får tilgang til en pasients helseopplysninger på vegne av innbyggeren og dens innsynsrett. For enkelte tjenester kan også innbygger i tillegg få mulighet til selv å bidra ved at leverandørenes applikasjoner oppdaterer på vegne av innbygger via API-er.

I målarkitekturen er det derfor lagt til grunn at det vil være hensiktsmessig og innovasjonsfremmende å ha felles håndtering av API-er på tvers av alle regioner og kommuner for «innovative utviklere av innbygger-apps». Dette kan utgjøre en type plattform for som muliggjør at 3.parts applikasjonsutviklere kan utvikle, teste og ta i bruk API-er hos aktører i helsesektoren.

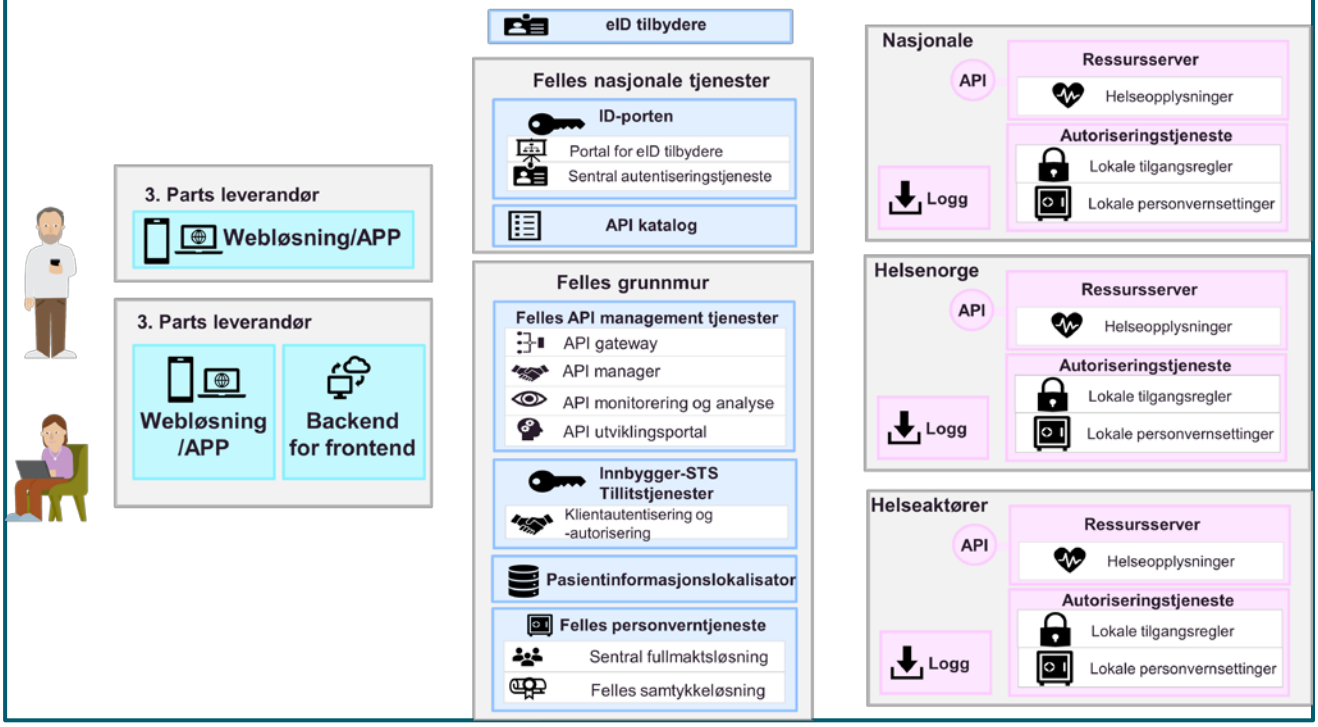
Det er naturlig at Helsenorge kan ha ansvaret for håndtering av en slik plattform på vegne av sektoren, men dette er foreløpig ikke besluttet.

Avtaleverk må gjøre det mulig for plattformeier å videredistribuere helseopplysninger via API-er, med klare vilkår for hvilken behandling og distribusjon av data som er tillatt fra de dataansvarlige.

I arbeidet med målarkitekturen har det fremkommet at håndtering av sikkerhet og personvern for dette bruksområdet vil skille seg såpass fra personell med tjenstlig behov at det er behov for egen håndtering av dette i arkitekturen. Dette kapittelet vil beskrive kapabiliteter, prosesser og bruk av felleskomponenter når innbyggere bruker applikasjoner som får tilgang til å kalle API-er på vegne av innbyggere.

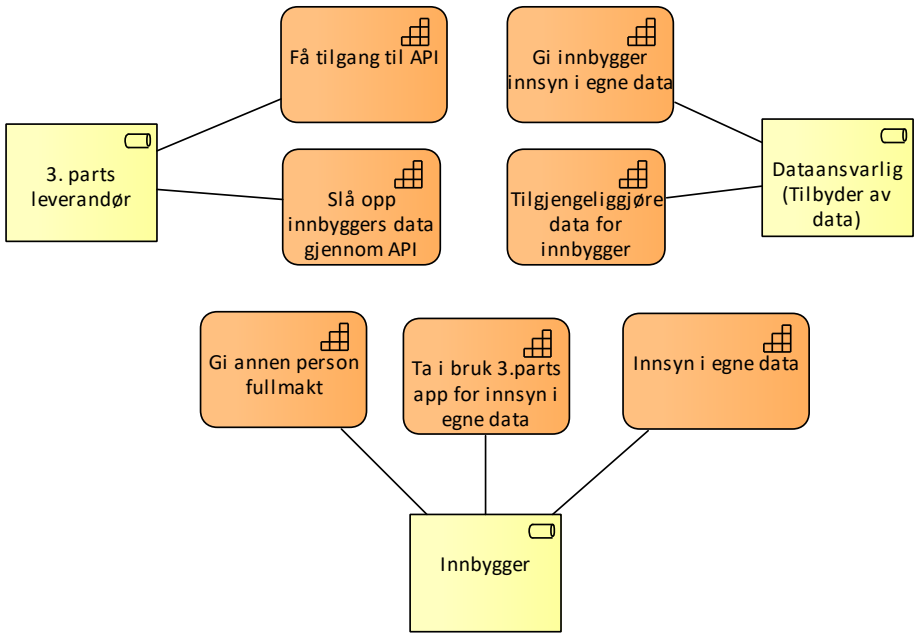
Figur 20 viser målarkitektur for dette bruksområdet og hvilke felleskomponenter som det er behov for. I de neste underkapitlene vil anvendelsene av felleskomponentene knyttes til forretningsprosesser og løsningsmønstre.

Figur 20 Målarkitektur for bruksområdet innbyggers innsyn i sin helsehjelp



Figur 21 viser hovedkapabilitetene som må realiseres for å dekke behovene i dette bruksområdet. Hver kapabilitet er nærmere beskrevet i tabellen under og de mest sentrale er videre detaljert i de neste kapitlene.

Figur 21 Hovedkapabiliter for Innbyggers bruk av datadeling



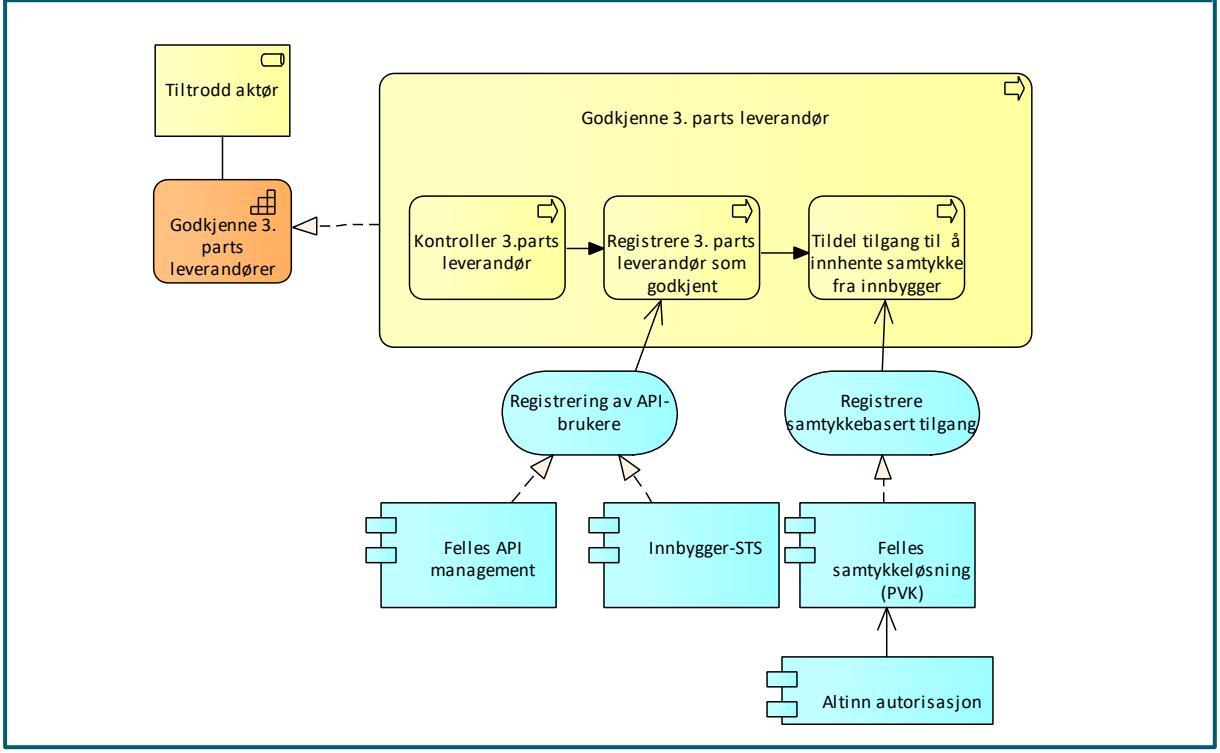
Element	Beskrivelse
3. parts leverandør	Med 3. parts leverandør menes her en leverandør av innbyggertjenester som på vegne av innbygger benytter datadeling for å gi innbygger innsyn i egne data hos en tilbyder av data.
Dataansvarlig (tilbyder av data)	En virksomhet som behandler helseopplysninger og har plikt til å gi innsyn til innbygger. Virksomheten har valgt å tilgjengeliggjøre et API.
Tiltrodd part	En part som de dataansvarlige har tillit til at gjør godkjenning av 3. parts leverandører. Dette kan være et felles bransjeorgan, tillitsanker eller lignende.
Godkjenn 3.parts leverandør	En tiltrodd part gjennomfører en godkjenning av en 3 parts leverandør for å kunne opptre på vegne av innbygger basert på innhentet samtykke fra innbygger.
Tilgjengeliggjøre data til innbygger	Evne til å tilgjengeliggjøre API-er som gir innbyggere mulighet for å få innsyn i sine helseopplysninger via datadeling
Gi annen person fullmakt	Evnen til å registrere at en innbygger gir en annen innbygger fullmakt til å representere seg selv
Få tilgang til API	Evnen til å få tilgang til å bruke et API på vegne av innbygger.

Element	Beskrivelse
Be om innsyn i innbyggers data	Evnen til å hente helseopplysninger på vegne av en innbygger ved hjelp av en 3. parts app via et API
Gi innbygger innsyn i egne data	Evnen til å gi innsyn til en innbygger eller en som kan representere innbygger i sine egne data via datadeling.
Ta i bruk 3. parts app for innsyn i egne data	Evnen til å få innsyn i egne data ved hjelp av en innbyggervalgt App.
Hvor er data lagret om meg?	Evnen til å skaffe en liste over hvilke dataansvarlige som har lagret helseopplysninger om en innbygger
Motsette seg deling	Evne til å støtte krav fra innbygger om å motsette seg deling av hele eller deler av journalen
Hvem har sett på mine data?	Evne til å vise innbygger en logg over hvilke personell som har sett på innbyggers helseopplysninger.

6.5.1 Godkjenne 3. parts leverandør

Realiseringen av denne kapabiliteten detaljerer prosessen med å forhåndsgodkjenne leverandører og eventuelt deres Apper slik at innbyggere kan være trygge på at appene håndterer helseopplysninger på en sikker måte og at leverandørene ikke misbruker deres helseopplysninger.

Figur 22 Tiltrodd aktør godkjenner 3. parts leverandør

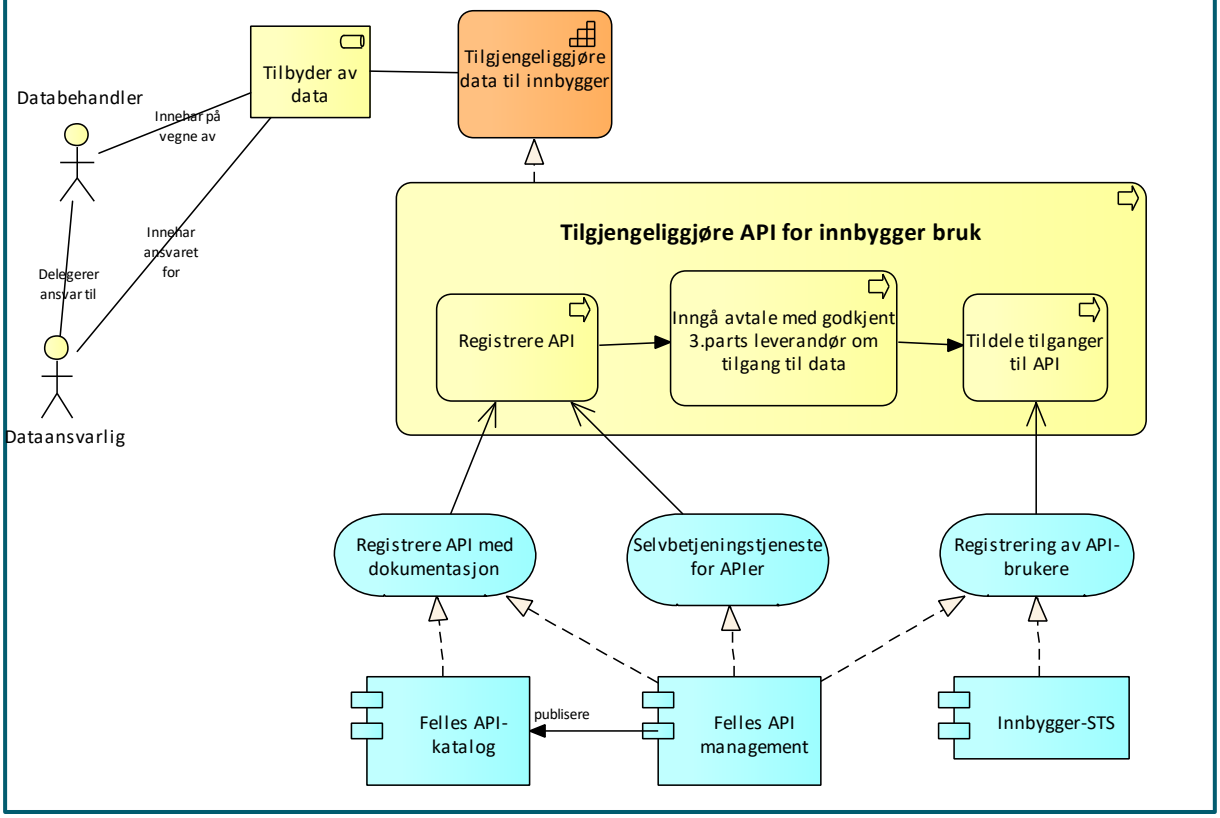


Element	Beskrivelse
Tiltrodd part	En part som de dataansvarlige har tillit til at gjør godkjenning av 3. parts leverandører. Dette kan være et felles bransjeorgan, tillitsanker eller lignende.
Godkjenne 3. parts leverandør	Prosess for å godkjenne og registrere leverandører som kan opptre på vegne av innbygger etter gitte retningslinjer
Kontroller 3. parts leverandør	Prosess for å kontrollere at de gitte retningslinjer er oppfylt.
Registrere 3. parts leverandør som godkjent	Prosess for å registrere godkjente leverandører.
Tildel tilgang til å innhente samtykke fra innbygger	Prosess for å gi godkjente leverandører tilgang til å innhente samtykke fra innbygger
Registrering av API-bruker	Tjeneste for å registrere tilganger til leverandører
Registrere samtykkebasert tilgang	Tjeneste for å håndtere tilgang til å benytte samtykkeløsningen
Felles API management	Fellesløsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter. I denne konteksten vil det være en fellesløsning for håndtering av API-er som dataansvarlige tilbyr leverandører av innbygger apps.
Innbygger STS	Tillitsøkende tjeneste som utsteder bevis på innlogget bruker og eventuelt hvem innbygger representerer samt gir tilgang til å kalle et API hos en tilbyder av data.
Felles samtykkeløsning (PVK)	Felles samtykkeløsning for helsesektoren som innhenter samtykke fra Innbyggere som benytter App-er fra godkjente 3.parts leverandører. PVK = Personvernkompontent
Altinn Autorisasjon	Autorisasjonskomponenten i Altinn som vil gi Innbyggere mulighet til å få oversikt over hvem de har gitt samtykke til.

6.5.2 Tilgjengeliggjøre API

Dette kapittelet beskriver realiseringen av prosess for dataansvarlige med å tilgjengeliggjøre API-er som 3. parts leverandører kan benytte på vegne av innbyggere.

Figur 23 Tilbyder tilgjengeliggjør sitt API



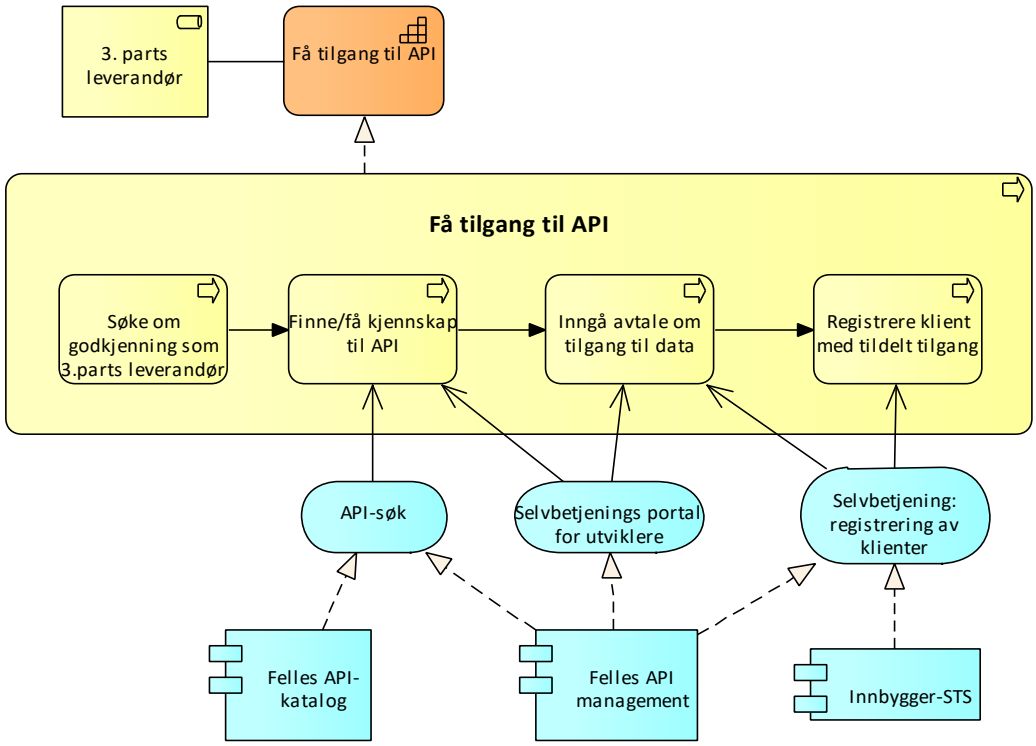
Element	Beskrivelse
Tilgjengeliggjøre data til innbygger	Evne til å tilgjengeliggjøre APIer som gir innbyggere mulighet for å få innsyn i sine helseopplysninger via datadeling
Tilbyder av data	En dataansvarlig som tilbyr innsyn til innbygger til egne data
Tilgjengeliggjøre API til innbygger	Prosessen med å tilby og gi tilgang for en godkjent 3. parts leverandør til et API.
Registrere API	Prosessen med å registrere et API i relevante tjenester, Felles API-katalog, Felles API management og Innbygger-STS.
Inngå avtale om tilgang til data	Prosess for å inngå avtale med en 3. parts leverandør om tilgang til og bruk av data på vegne av en innbygger.
Tildele tilganger til API	Prosessen med å registrere hvilke 3. parts leverandører som skal få tilgang til å kalle et API.

Element	Beskrivelse
Registrere API med dokumentasjon	Tjeneste i Felles API-katalogen og i Felles API managementløsning for å registrere API og dets dokumentasjon. Bruk av tjenesten forutsetter at rettigheter til å gjøre dette på vegne av tilbyders virksomhet.
Selvbetjeningstjeneste for APIer	Tilbyder av API-et må konfigurere sikkerhet og andre operasjonelle forhold. En databehandler kan ha rettigheter til å administrere på vegne av tilbyder.
Registrering av API-brukere	Selvbetjeningstjeneste for å registrere og vedlikeholde tilgangene som datakonsumenter skal ha til API-et
Innbygger-STS	Fellesløsning for sikring av helsesektorens innbygger API-er . Den tilbyr selvbetjening av API-er og utstedelse av OAUTH2-tokens som gir forhåndsgodkjente klienter tilgang til å kalle et API dersom et samtykke fra Innbygger foreligger.
Felles API-katalog	Del av Felles datakatalog som gir mulighet for å registrere API-er og dens dokumentasjon via enten et selvbetjeningsgrensesnitt eller via API-er som en API managementløsning kan benytte. https://fellesdatakatalog.brreg.no/apis
Felles API management	Fellesløsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter. I denne konteksten vil det være en fellesløsning for håndtering av API-er som dataansvarlige tilbyr leverandører av innbygger apps.

6.5.3 Få tilgang til API

Dette kapittelet beskriver realisering av prosessen for 3. parts leverandører med å få tilgang til å bruke et API på vegne av en innbygger.

Figur 24 3. parts leverandør får tilgang til API



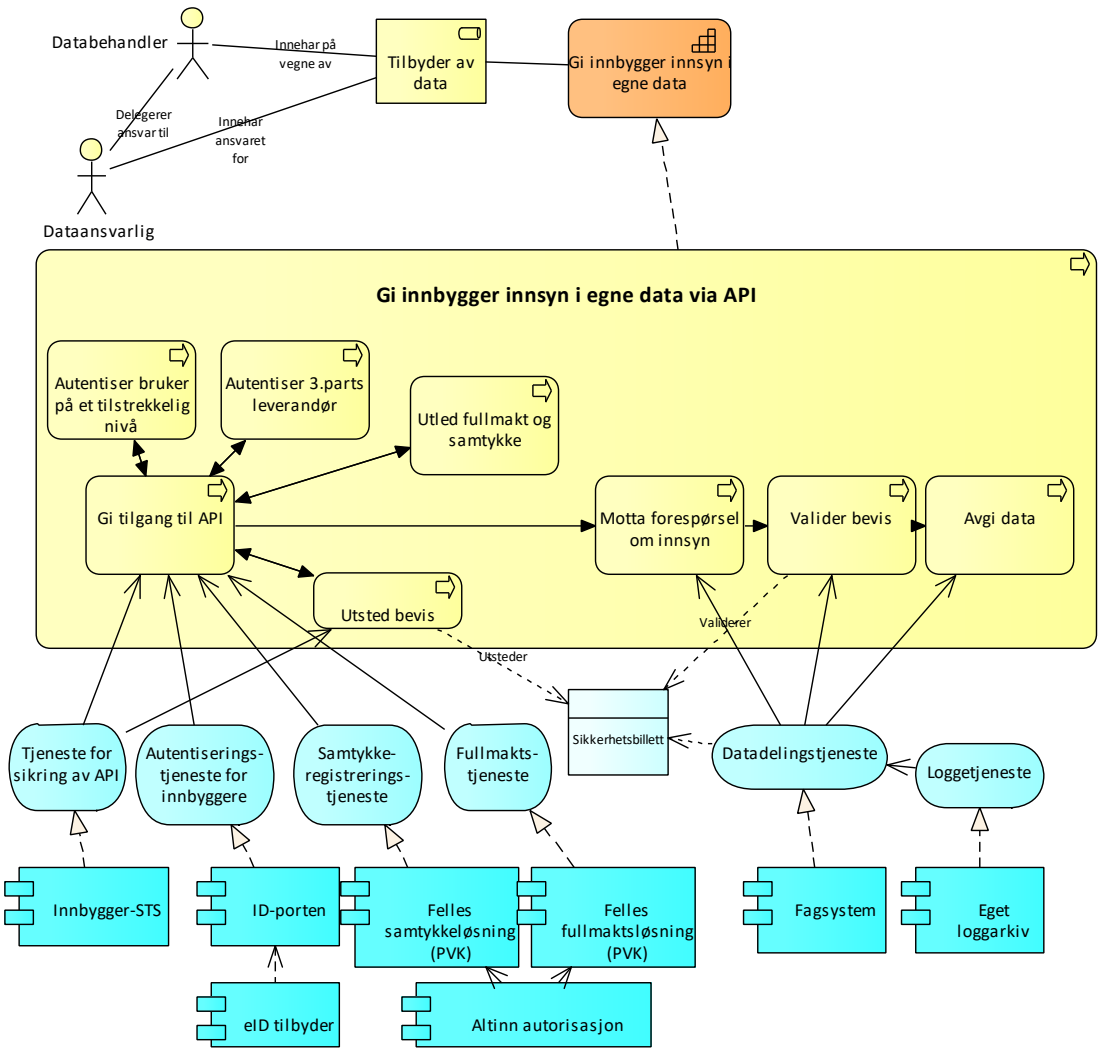
Element	Beskrivelse
Få tilgang til API	Evnen til å få tilgang til å bruke et API på vegne av innbygger.
3. parts leverandør	Med 3. parts leverandør menes her en leverandør av innbyggertjenester som på vegne av innbygger benytter datadeling for å gi innbygger innsyn i egne data hos en tilbyder av data.
Få tilgang til API	Hovedprosessen med å skaffe seg tilgang til tilbudte data fra annen aktør. Omfatte å finne API-er, inngå nødvendige avtaler og få tilganger.
Søke om godkjenning som 3.parts leverandør	Prosessen med å bli en godkjent 3. parts leverandør som er forhåndsgodkjent for å be innbygger om samtykke.
Finne/få kjennskap til API	Prosessen med å finne eller få kjennskap til tilgjengelige API-er gjennom relevante kataloger og søkeløsninger.
Inngå avtale om tilgang til data	Prosess hvor en godkjent 3. parts leverandør inngår eventuell avtale med tilbyder om tilgang til data på vegne av innbygger.

Registrer klient med tildelt tilgang	Prosess for en godkjent 3. parts leverandør med å registrere (provisjonering av) den klienten som skal ha tilgang til API-et ved bruk av sikkerhetsbillett. Dette forutsetter at leverandøren har avtale om bruk av sikkerhetsbillettjenesten og at tilbyder har gitt leverandøren tilgang.
Felles API management	Fellesløsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter. I denne konteksten vil det være en fellesløsning for håndtering av API-er som dataansvarlige tilbyr leverandører av innbygger apps.
Felles API-katalog	Del av Felles datakatalog som gir mulighet for å søke etter API-er og lese API-spesifikasjoner https://fellesdatakatalog.brreg.no/apis
Innbygger-STS	Tillitsøkende tjeneste som utsteder bevis på innlogget bruker og eventuelt hvem innbygger representerer samt gir tilgang til å kalle et API hos en tilbyder av data.
API-søk	Tjeneste for å søke etter og finne tilgjengelige API-er
Selvbetjening: registrering av klienter	Tjeneste for å registrere klienter som skal ha tilgang til et gitt API som kan opptre på vegne av godkjent 3. parts leverandør.
Selvbetjeningsportal for utviklere	Tjeneste for utviklere som skal utvikle klienter som benytter de registrerte API-ene. Portalen må beskrive bruk av API-ene inkludert adresse og operasjoner som tilbys.

6.5.4 Gi innbygger innsyn i egne data med datadeling

Dette kapittelet beskriver realiseringen av prosessen hvor tilbydere av data avgir innbyggers helseopplysninger gjennom kall til deres API. API-et krever at innbygger eller den som har rett til å representere innbygger er innlogget på et tilstrekkelig høyt nivå, at leverandøren av Appen som innbygger bruker er godkjent, og at innbygger har gitt sitt samtykke til at Appen kan motta innbyggers helseopplysninger.

Figur 25 Gi innbygger innsyn i egne data via API



Element	Beskrivelse
Gi innbygger innsyn i egne data	Evne til å avgi data som en dataansvarlig har lagret om en innbygger via datadeling
Tilbyder av data	En aktør som tilbyr data til innbygger, enten på vegne av andre, som forvalter av data eller som dataansvarlig.
Gi tilgang til API	Prosess for å sikre at bruker er autentisert, 3. parts leverandør er autentisert og har tilgang til API-et og at innbygger har gitt samtykke til at klienten kan utføre API-kallet.
Autentiser bruker på et tilstrekkelig nivå	Prosess for å sikre at bruker er autentisert på et tilstrekkelig nivå

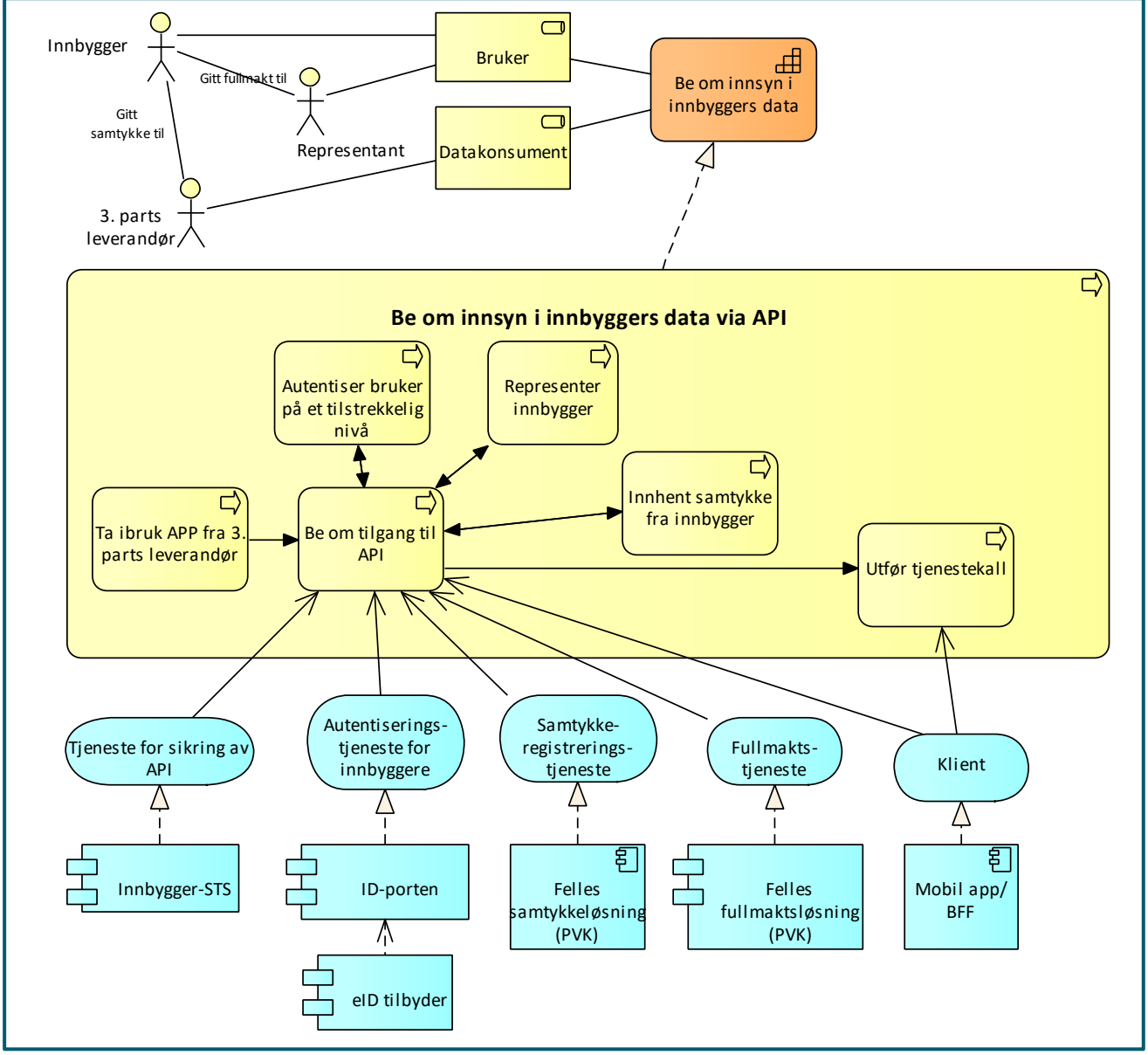
Element	Beskrivelse
Autentiser 3. parts leverandør	Prosess for å sikre at 3. parts leverandør er autentisert og har tilgang til API-et.
Utled fullmakt og samtykke	Prosess for å kontrollere fullmakt dersom innlogget bruker representerer en annen innbygger. Prosess for å kontrollere at innbygger har gitt samtykke for at App-en kan hente innbyggers data gjennom APIet.
Utsted bevis	Prosess for å opprette og gi ut et bevis for at bruker er innlogget, 3.parts leverandør er autentisert og autorisert, at samtykke og eventuelt fullmakt er kontrollert.
Motta forespørsel om innsyn	Prosess for å ta imot kall til et API.
Valider bevis	Prosess for å kontrollere at kallende klient er gitt tillatelse til å få tilgang til innbyggers data.
Avgi data	Prosess for å behandle API-kallet og returnere dataene som etterspørres.
Tjeneste for sikring av API	Tjeneste for å sikre at bruker er autentisert, 3. parts leverandør er autentisert og har tilgang til API-et og at innbygger har gitt samtykke til at klienten kan utføre API-kallet.
Autentiserings-tjeneste for innbyggere	Tjeneste for å autentisere brukers identitet
Samtykke-registrerings-tjeneste	Tjeneste som kan benyttes for å verifisere at en innbygger har gitt samtykke til at klienten kan be om innbyggers data.
Fullmaktstjeneste	Tjeneste for å slå opp hvilke andre personer en person kan representere.
Datadelingstjeneste	Tjeneste som tilbyr API
Loggetjeneste	Tjeneste som håndterer audit logging
Sikkerhetsbillett	Sikkerhetsbillett er et samlebegrep for alle typer identitets- og tilgangsbilletter uavhengig av protokoll og format.
Innbygger-STS	Tillitsøkende tjeneste som utsteder bevis på innlogget bruker og eventuelt hvem innbygger representerer samt gir tilgang til å kalle et API hos en tilbyder av data.
ID-porten	Nasjonal felleskomponent med ansvar for å autentisere innbygger med nasjonale eID-er.

Element	Beskrivelse
eID tilbyder	Tilbyder av elektroniske identiteter som tilfredsstiller nasjonale sikkerhetsnivåer. BankID, Buypass osv
ID-porten	Portal som tilbyr nasjonal godkjente eID-er
Felles API management	Fellesløsning for eksponering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter. I denne konteksten vil det være en fellesløsning for håndtering av API-er som dataansvarlige tilbyr leverandører av innbygger apps.
Ressursserver	Dataansvarliges system som lagrer helseopplysningene som deles
Eget loggarkiv	Dataansvarliges eget system for håndtering og lagring av audit logg. Kan være en del av ressursserver eller eget selvstendig system
Egen autorisasjons-komponent	Dataansvarliges eget system for håndtering av tilgang til dataene.
Felles samtykkeløsning	Felleskomponent for helsesektoren for å håndtere samtykke fra innbygger. En del av personvernkomponenten(PVK)
Felles fullmaktsløsning	Felleskomponent for helsesektoren for å håndtere fullmakter og representasjoner basert på fullmakter. En del av personvernkomponenten(PVK)

6.5.5 Innsyn i innbyggers data

Dette kapittelet beskriver realiseringen av prosessen hvor innbygger har tatt i bruk en 3. parts App som innbygger har gitt samtykke til å be om å hente innbyggers helseopplysninger via datadeling.

Figur 26 Innbygger ber om innsyn i egne data via API



Element	Beskrivelse
Be om innsyn i innbyggers data	Evne til å be om innbyggers data som en dataansvarlig har lagret om en innbygger via datadeling
Bruker	Den påloggede innbygger eller en person som representerer innbyggeren
Datakonsument	3. partsleverandøren som representerer innbygger.

Element	Beskrivelse
Ta ibruk App fra 3. parts leverandør	Innbygger finner og velger å benytte en App fra en godkjent 3. parts leverandør.
Be om tilgang til API	Prosess for å sikre at bruker blir autentisert, 3. parts leverandør er autentiseres og at innbygger gir samtykke til at klienten kan utføre API-kallet.
Autentiser bruker på et tilstrekkelig nivå	Prosess for å sikre at bruker blir autentisert på et tilstrekkelig nivå
Representer innbygger	Prosess som lar pålogget bruker representere en annen person.
Innhent samtykke	Prosess for å innhente samtykke fra Innbygger.
Utfør tjenestekall	Prosess for å gjennomføre API-kallet.
Tjeneste for sikring av API	Tjeneste for å utstede bevis på at bruker er autentisert, 3. parts leverandør er autentisert og har tilgang til API-et og at innbygger har gitt samtykke til at klienten kan utføre API-kallet.
Autentiserings-tjeneste for innbyggere	Tjeneste for å autentisere brukers identitet
Samtykke-registrerings-tjeneste	Tjeneste for å innhente samtykke fra innbygger
Fullmaktstjeneste	Tjeneste for å slå opp hvilke andre personer en person kan representere.
Klient	Tjeneste som utfører API-kallet
Loggetjeneste	Tjeneste som håndterer audit logging
Innbygger-STS	Tillitsøkende tjeneste som utsteder bevis på innlogget bruker og eventuelt hvem innbygger representerer samt gir tilgang til å kalle et API hos en tilbyder av data.
ID-porten	Nasjonal felleskomponent med ansvar for å autentisere innbygger med nasjonale eID-er.
eID tilbyder	Tilbyder av elektroniske identiteter som tilfredsstiller nasjonale sikkerhetsnivåer. BankID, Buypass osv
Felles samtykkeløsning	Felleskomponent for helsesektoren for å håndtere samtykke fra innbygger. En del av personvernkomponenten(PVK)

Element	Beskrivelse
Felles fullmaktsløsning	Felleskomponent for helsesektoren for å håndtere fullmakter og representasjoner basert på fullmakter. En del av personvernkomponenten(PVK)
Mobil APP/BFF	Systemet som teknisk sett kaller API-et. BFF (backend for frontend) er serverdelen av en mobil app løsning.

6.6 Samhandling mellom helsepersonell i andre virksomheter

Dette bruksområdet dekker samhandling gjennom datadeling mellom aktører i ulike helseregioner og mellom aktører i helseregion og den kommunale helse- og omsorgstjenesten inkludert fastleger.
Målarkitekturen for dette bruksområdet trenger mer arbeid og vi har valgt å ikke beskrive arkitekturen nærmere i denne versjonen av dokumentet.

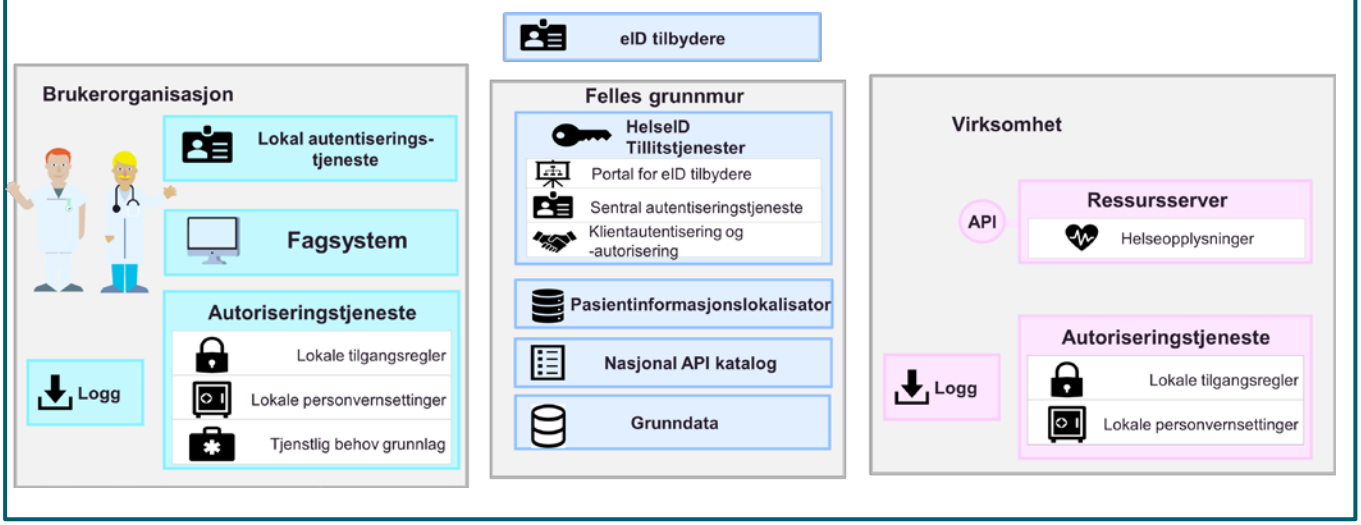
Skal datadeling for dette bruksområdet foregå peer-to-peer eller gjennom en sentral samhandlingskomponent?

Dersom sektoren velger peer-to-peer:

- Hvor mye API-management kapabiliteter skal så være lokalt?
  - Kun validering av tokens?
  - Autorisering av klienter?
  - Statistikk/analyse?
  - Utviklerportal?
  - Eller bør dette sentraliseres?
- Hvor mye trengs av støtte i felleskomponenter?

Figur 27 viser et forslag på en peer-to-peer arkitektur hvor hver virksomhet selv har ansvaret for å etablere API management løsning.

Figur 27 Peer-to-peer arkitektur



I Akson-tiltaket er det planlagt en sentral samhandlingsløsning for dette bruksområdet. For samhandling med datadeling mellom Akson og helseregionene kan en tenke seg at en samhandlingsløsning med API management kapabiliteter dekker behovet. Da vil trolig en slik samhandlingsløsning dekke aktørenes behov for API management. Det er ennå ikke avklart hvilken støtte en slik løsning krever av felleskomponenter.

6.7 Samhandling med helsepersonell og innbyggere lokalt

Dette bruksområdet dekker, som nevnt i kapittel 5.1.4, brukstilfeller hvor helsepersonell og innbyggere benytter lette og/eller mobile applikasjoner samt velferdsteknologi for å samhandle om helseopplysninger.

Området er nært knyttet til samhandlingsbehov helsepersonell har internt i en virksomhet og er normalt utenfor omfang av nasjonal arkitekturstyring, men er tatt med på grunn av behovet for å utnytte leverandørmarkedet for utvikling av innovative applikasjoner og tilpasse fellesfunksjonalitet slik den også kan gjenbrukes på tvers av virksomheter.

Brukere kan være egne eller eksterne ansatte med tjenstlige behov samt innbyggere som på en eller annen måte bidrar i helsehjelpen som de mottar.

Det er i dag i liten grad tilrettelagt for innovasjon innen dette bruksområdet da mange av de eksisterende løsningene er lukkede systemer uten åpne API-er. Virksomheter blir avhengig av sine leverandører og deres kapasitet til å utvikle og vilje til å åpne opp for andre leverandører. Hvordan åpne disse og få andre eksterne leverandører til å utvikle innovative apps?

Temaet ble ikke godt nok dekket i arbeidet med dette dokumentet og dette må det jobbes videre med. Noen betraktninger vi har gjort oss for dette bruksområdet:

- Trenger helseregioner og kommuner/Akson egen kontroll på API management for apps mot egne helsearbeidere og velferdsteknologi?
- Hvor mye bør sentraliseres? Klientregister, API katalog, autentisering, autorisering, utviklerportal, analyse/drift?
- Hvor standardiserte bør de lokale API-ene være? Er målet full standardisering eller mer fleksibilitet?

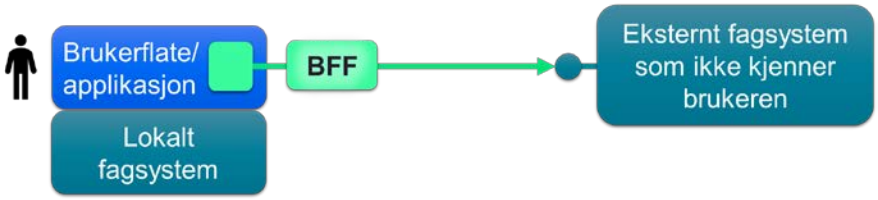
En veileder for åpne API i helse og omsorgstjenesten [18] er lagt ut på ehelse.no for innspill (frem til 2 mars 2020). En slik veileder kan være et virkemiddel som virksomheter kan benytte ved anskaffelser for å sikre at nye e-helseløsninger har åpne API-er.

7 Integrasjonsmønstre for datadeling

Datadeling anvendes normalt ved at en klient kaller et API hos en ekstern tjener til en annen virksomhet. Klientene utvikles, eies og brukes av andre aktører enn de som tilbyr API-er. API-ene tilbyr tilgang til helse- og personopplysninger og det kreves god kontroll på at kun pasienten selv (eller en med fullmakt) og personell med tjenstlig behov får tilgang.

Figur 28: Klient-tjener mot eksternt system

A Klient-tjener mot eksternt system
Eksempel: En EPJ eller en applikasjon i EPJ henter informasjon fra en annen EPJ (det gis tilgang til annen virksomhets EPJ). Kall kan gjøres fra en nedlastbar applikasjon eller innebygget EPJ-funksjonalitet. BFF: Backend for Frontend: se kapittel 7.1 for forklaring.



Denne standardanvendelsen kan vi si er en generisk oppskrift for hvordan datadeling realiseres og anvendes mellom virksomheter. Dette er vist i Figur 28. Vi har valgt å kalle oppskriften for et integrasjonsmønster for datadeling. Mønsteret er videre detaljert i kapittel 10. Gjennom arbeidet med målarkitekturen har vi avdekket andre integrasjonsmønstre for realisering og anvendelser av datadeling. Et mønster har ulike egenskaper og karakteristikker og et mønster vil egne seg bedre enn andre mønstre under ulike kontekster.

Eksempler på viktige egenskaper og karakteristikker er:

- Om en autentisert bruker er involvert i dataflyten, eller om dataflyten kun involverer systemer.
- Om tjenesten som tilbyr et API er lokal for brukeren og har detaljert informasjon om den aktuelle brukeren, eller om tjenesten er i en ekstern virksomhet eller nasjonal tjeneste med en løsere knytning til brukeren.
- Hvordan og hvor presentasjonslogikk og forretningslogikk er implementert og hvor den henter data fra.
- Hvordan ekstern presentasjonslogikk og/eller forretningslogikk aktiveres og eventuelt lastes ned.

7.1 Backend for Frontend (BFF)

Backend-for-Frontend (BFF) er et utbredt designkonsept som benyttes for mange klienter og API-er. Konseptet går ut på å la ulike brukergrensesnittyper (Nettleserbaserte, App-er på mobil osv) ha hver sin backend slik at spesialtilpasninger på API-er som kreves for de ulike brukergrensesnitttypene kan realiseres uten at det går utover vedlikeholdbarheten til API-ene.

Konseptet er mest knyttet til bruk av en virksomhet sine API-er hvor de selv har kontroll på alle typer klienter. Men konseptet kan også benyttes i andre anvendelser. I de integrasjonsmønstre som beskrives her, kan alle mønstrene utvides med bruk av dette konseptet.

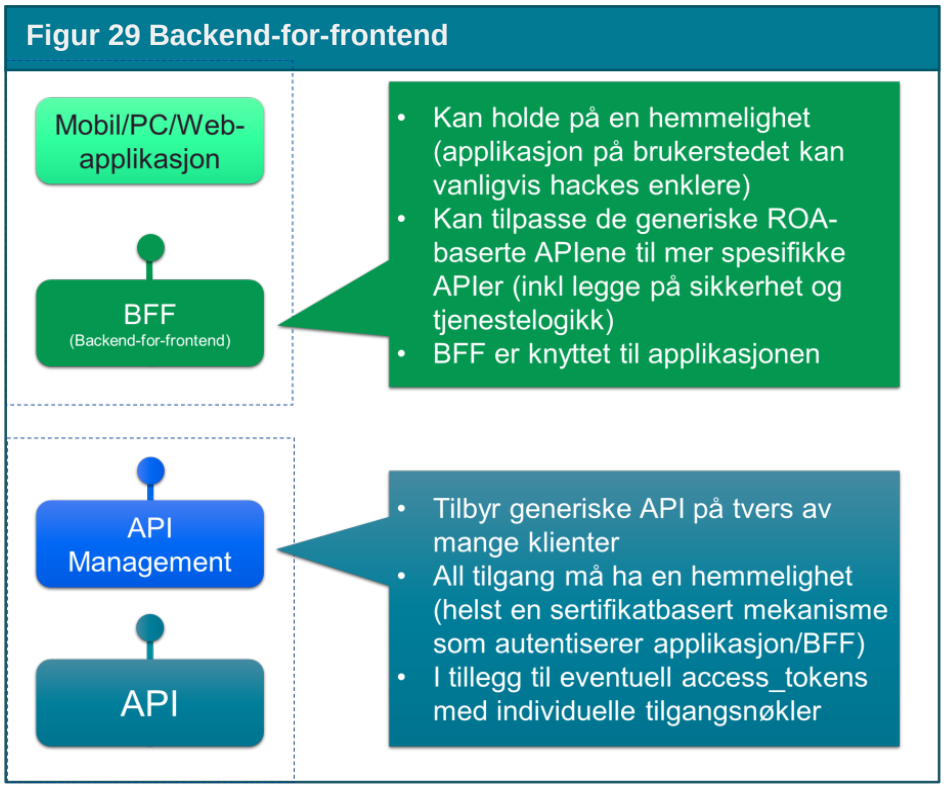
Ved bruk av API-er som eies av andre virksomheter settes det krav til at klientene MÅ støtte sikker lagring og behandling av hemmeligheter for å sikre konfidensialitet og integritet ved overføring av sensitive personopplysninger mellom klientene og API-et.

Eksempel på behov for bruk av dette konseptet:

1. En mobil-frontend ønsker å bruke minst mulig båndbredde ved å redusere datamengden per kall, mens en web-frontend vil kunne sende mer data over linjen.
2. Det er ikke anbefalt at javascriptbasert web-frontend mottar sikkerhetsbilletter for å aksessere eksterne API-er (se IETF draft: OAuth 2.0 for Browser-Based Apps kap 4 og 6.1). En backend for web-frontenden kan være en løsning på dette.

Når dette konseptet benyttes i mønsteret "klient-tjener mot eksternt system" medfører det at selve backenden vil være klienten til API-ene. I velferdsteknologisammenheng brukes ordet "forsystem" av og til om "Backend-for-frontend".

Figur 29 Backend-for-frontend



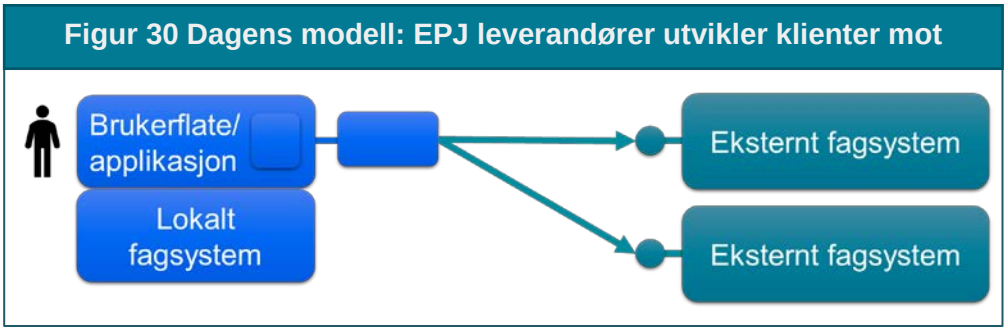
7.2 Alternative integrasjonsmønstre

Dagens arkitektur i helse- og omsorgstjenesten er meget kompleks og utvikling av felles funksjonalitet for samhandling krever konsolidering av systemer slik som "En innbygger en journal"-målbilde legger opp til. For å realisere dette målbilde, må det tilrettelegges for samhandling gjennom bruk av datadeling. Dagens realiseringsmodell er basert på at EPJ-leverandører implementerer selv integrasjonen mot forskjellige eksterne fagsystemer. Se Figur 29. Men dette har flere utfordringer:

1. Hvert enkelt system må realisere samme funksjonalitet samt påkrevd støtte for sikkerhet og personvern for bruk av andres API-er. Hvert av API-ene kan i tillegg ha ulike autentiseringsmekanismer osv.
2. Systemleverandører har begrenset kapasitet og det kan ta lang tid før alle samhandlende systemer har nødvendig støtte for bruk av felles API-er.
3. Manglende finansieringsevne hos mindre aktører medfører lange ledetider for utvikling av ny funksjonalitet i deres systemer.

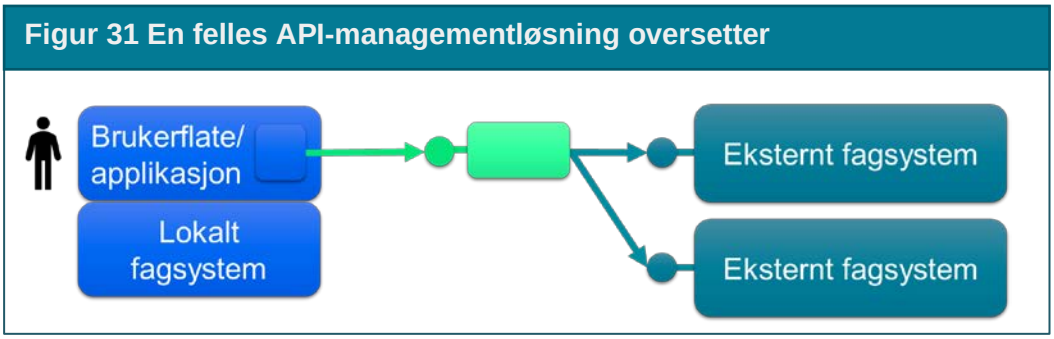
4. I tillegg er det en stor risiko for at funksjonalitet som skal være lik i alle systemer blir forskjellig, noe som medfører dårligere kvalitet på informasjon som benyttes til yting av helsehjelp. Det kan da være behov for å innføre klientsertifiseringsordninger.

Figur 30 Dagens modell: EPJ leverandører utvikler klienter mot



Hvordan redusere disse utfordringen? Et alternativ er å bruke en felles API-management løsning som kan oversette, transformere og samordne API-er fra flere eksterne systemer.

Figur 31 En felles API-managementløsning oversetter



Se Figur 30. Her vil EPJ-leverandører kunne implementere klienten selv, men jobben vil være enklere fordi API-ene er likere og følger samme arkitektur, autentisering etc.

Et annet alternativ er at EPJ-leverandører tillater andre aktører å utvikle funksjonalitet tett integrert med deres systemer. Vi skal se på to alternative integrasjonsmønstre for datadeling som åpner opp for en raskere og kostnadseffektiv bredding og ibruktagelse av funksjonalitet for samhandling mellom helsepersonell og mellom innbyggere og helsepersonell. Mønstrene er vist i Figur 32.

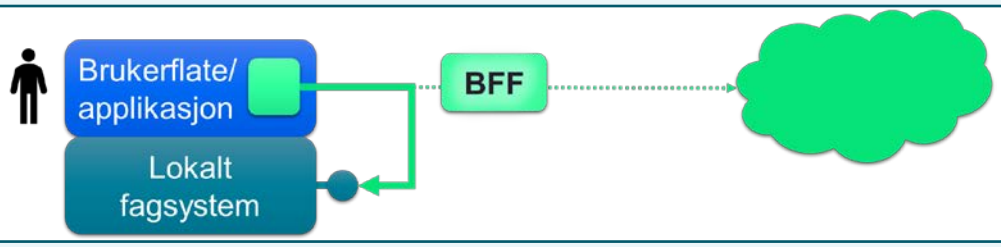
Den første har vi valgt å kalle "*A1 - nedlastbar webapp*" og er basert på standarden "SMART on FHIR" [14]. Dette mønstre muliggjør at 3.parts systemleverandører kan utvikle webbaserte applikasjoner med felles funksjonalitet som kan benyttes av alle som har fagsystemer som støtter mønsteret. Et fagsystem laster ned en webapplikasjon fra en ekstern kilde og kjører denne lokalt i fagsystemet. Applikasjonen kan få tilgang til lokale data og tjenester gjennom lokale, standardiserte API-er. Mønsteret kan også utvides ved at den nedlastbare webapplikasjonen benytter eksterne API-er slik at funksjonaliteten i webapplikasjonen kan kombinere lokale data og eksterne tjenester. Dette medfører at virksomheter kan få tilgang til nye tjenester raskere og uten å måtte vente på at systemleverandøren må implementere støtte for disse tjenestene. Mønsteret er detaljert i kapittel 10.2.

Det andre mønsteret har vi kalt "*A2 - ekstern applikasjon med forretningslogikk gis tilgang til lokalt system*" og er basert på standarden "CDS Hooks". Dette mønstret gjør det mulig for

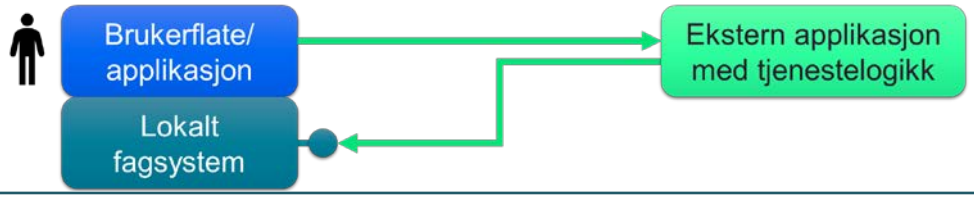
virksomheter å benytte felles ekstern funksjonalitet, men med å benytte lokale data. Den eksterne applikasjonen kjøres hos en tiltrodd virksomhet og kan tilby avgrenset helserelatert funksjonalitet som er lite egnet for å inkluderes i fagsystemene. Det lokale fagsystemet kaller en eller flere eksterne mikrotjenester som i retur kan vise små informasjonselementer og linker på definerte steder i brukerflaten på fagsystemet. Dette medfører at virksomheter kan enkelt få tilgang til nye mikrotjenester raskt og slippe å vedlikeholde funksjonaliteten i eget system. Mønsteret er detaljert i kapittel 10.3.

Figur 32 To alternative integrasjonsmønstre

A1 Nedlastbar webapp (SMART on FHIR)
Eksempel: Ekstern applikasjon som lastes ned og kjøres lokalt. Webapp gis API-tilgang til det lokale fagsystemet som brukeren er pålogget. Kan aksessere eksterne API, men arbeid gjenstår her. (*HL7 har endret navnet til Smart App Lanch*)



A2 Eksternt applikasjon gis tilgang (CDS Hooks)
Eksempel: Primært en ekstern applikasjon som støtter brukeren med informasjon og beslutningsstøtte. Den eksterne applikasjonen får API-tilgang til fagsystem og brukerflate, trigget av bruker.



7.3 Datadeling hvor ingen bruker er involvert

I dette integrasjonsmønsteret kaller et fagsystem i en virksomhet et annet fagsystem i en annen virksomhet, uten at en spesifikk bruker er involvert i flyten. Kallene gjøres altså ikke på vegne av spesifikke brukere, men det gis tilgang basert på virksomhetsautentisering og avtaler mellom virksomhetene. Slike integrasjonsmønstre kan for eksempel brukes hvis en virksomhet vil informere en annen virksomhet om en hendelse som bør følges opp av virksomheten, eller for å overføre batchvis informasjon og oppdateringer om pasienter. Mønsteret er detaljert i kapittel 10.4.

Figur 33 Integrasjonsmønster hvor ingen bruker er involvert

B Automatiserte prosesser (Maskin-2- maskin) uten bruker
Kall gjøres av en automatisert prosess i en applikasjon uten at dette representerer en eksplisitt bruker. Data presenteres eventuelt i etterkant til sluttbrukere, men da fra det lokale fagsystemet.

8 Veien videre

8.1 Om realisering

Målarkitekturen sier ikke noe om realisering. Det er i dokumentet identifisert behov for både videreutvikling av eksisterende felleskomponenter samt etablering av nye komponenter. Det må jobbes videre med hvordan dette skal gjennomføres.

8.2 Områder som ikke ble dekt i arbeidet med dette dokumentet

I arbeidet med dette dokumentet har vi identifisert temaer som det bør arbeides videre med. Noen viktige tema for videre arbeid er:

1. To av bruksområdene (samhandling mellom helsepersonell på tvers samt samhandling med helsepersonell lokalt) trenger videre diskusjon for å komme frem til en ønsket målarkitektur.
2. For bruksområdet "innbyggers behandling av sine helseopplysninger" har vi identifisert noen temaer det må arbeides videre med:
    a. Hva skal til for at Helsenorge kan videreformidle API-er fra den enkelte dataansvarlige?
    b. Må 3.parts leverandører med Apps ha en databehandleravtale med API-eier som er dataansvarlig?
    c. Godkjenning av 3.parts leverandører. Det er i kapittel 6.5.1 beskrevet en prosess for å godkjenne 3.parts leverandører med Apps som skal kalle API-er som behandler helseopplysninger. Hva består en slik godkjenning av?
    d. Skal Apps kunne benytte innsynsAPI-er direkte eller må de ha en egen BFF?
3. Bruk av CDS hooks. Internasjonalt er dette en forholdsvis ny standard som akkurat er sluppet i en 1.0 versjon. Skal vi tilrettelegge for denne standarden nasjonalt?
4. I innspillsrunden kom det frem at det er behov for å se på behovet for å etablere en kodeverksserver som en felleskomponent hvor sektoren kan kontrollere at verdier som benyttes i et API er gyldige verdier i det refererte kodeverket.

5. Behov for grunndata i datadeling er i liten grad diskutert i dette dokumentet. Det ble i arbeidet med dette dokumentet blant annet avdekket behov for data rundt virskomhetsstrukturer. Om slike behov ikke er dekket av enhetsregisteret er uavklart og må sees på nærmere.
6. Målarkitekturen har tatt utgangspunkt i "Anbefaling av tillitsmodell for data- og dokumentdeling"[10]. Det vil være behov for å detaljere kravene til identitet- og tilgangsstyring i denne tillitsmodellen. Dette tiltaket er planlagt gjennomført i 2020.
7. Testmiljøer for felleskomponenter er ikke omhandlet i dette dokumentet da dette er svært knyttet til realisering av målarkitekturen. Testmiljøer for bruk av API-er er også et viktig tema som ikke er omhandlet i dette dokumentet. I arbeidet med "Veileder for åpne API-er" [18] er det beskrevet anbefalinger om at testing av bruk av API-er bør være mulig uten at leverandøren er involvert.

9 Referanser

[1] Plan for utvikling av felles grunnmur for digitale tjenester i helse-og omsorgstjenesten, Direktoratet for e-helse, 2019 (ehelse.no)

[2] Veikart for realiseringen av målbildet Én innbygger–én journal, Direktoratet for e-helse, 2018 (ehelse.no)

[3] "Nytt nasjonalt rammeverk for samhandling", Digitaliseringsdirektoratet 2018, (https://www.difi.no/arkitektur/nytt-nasjonalt-rammeverk-samhandling)

[4] Normeringsnivå og dokumenttyper, Direktoratet for e-helse (ehelse.no)

[5] Forskrift om IKT-standarder i helse- og omsorgstjenesten (lovdata.no)

[6] Nasjonal e-helsestrategi og handlingsplan 2017-2022, Direktoratet for e-helse, 2019, https://ehelse.no/strategi/nasjonal-e-helsestrategi-og-handlingsplan-2017-2022

[7] Én innbygger – én journal Behovsanalyse Nasjonal løsning for kommunal helse- og omsorgstjeneste Vedlegg (Direktoratet for e-helse, 2018)

[8] Referansearkitektur for datadeling (HITR 1215:2018 12/2018), https://ehelse.no/standarder/ikke-standarder/referansearkitektur-for-datadeling

[9] Retningslinjer for logging ved data- og dokumentdeling (HITS 1219:2019 03/2019) https://ehelse.no/standarder/ikke-standarder/retningslinjer-for-logging-ved-data-og-dokumentdeling

[10] Anbefaling av tillitsmodell for data- og dokumentdeling (HITR 1223:2019) https://ehelse.no/standarder/ikke-standarder/anbefaling-av-tillitsmodell-for-data-og-dokumentdeling .

[11] Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten. (utgitt 23.01.2019) https://ehelse.no/publikasjoner/plan-for-utvikling-av-felles-grunnmur-for-digitale-tjenester-i-helse-og-omsorgstjenesten

[12] Generisk referansearkitektur for Datautveksling (per høst 2019 under arbeid), DigDir med flere, https://doc.DigDir.no/nasjonal-arkitektur/nab_referanse_arkitekturer

[13] EPJ standarden – Tilgangsstyring, retting og sletting https://ehelse.no/standarder/EPJ%20standard%20-%20Tilgangsstyring,%20retting%20og%20sletting

[14] Anbefaling om bruk av SMART on FHIR – (HITR 1225:2019) https://ehelse.no/standarder/ikke-standarder/anbefaling-om-bruk-av-smart-on-fhir

[15] Målbilde for Felles språk i helse- og omsorgssektoren – (IE-1052 okt 2019) https://ehelse.no/publikasjoner/felles-sprak-i-helse-og-omsorgssektoren-malbilde-versjon-1.0

[16] Veileder for utvikling av datadelingsgrensesnitt – (HITR 1221:2019) https://ehelse.no/standarder/ikke-standarder/veileder-for-utvikling-av-datadelingsgrensesnitt

[17] Krav til sikkerhetsbillett ved deling av helseopplysninger – (HITS 1220:2019) https://ehelse.no/standarder/ikke-standarder/krav-til-sikkerhetsbillett-ved-deling-av-helseopplysninger

[18] Innspillsrunde: Veileder for åpne API i helse- og omsorgsektoren (HITR 1229 utkast 2019) https://ehelse.no/standarder/ikke-standarder/innspillsrunde-veiledning-for-%C3%A5pne-api-i-helse-og-omsorgssektoren

Vedlegg 1 Detaljert beskrivelse av integrasjonsmønstrene

Dette vedlegget beskriver integrasjonsmønstrene i mer detalj. I tillegg henvises det til *Veileder for utvikling for datadelingsgrensesnitt* [16] hvor enda flere detaljer rundt utvikling av datadelingsgrensesnitt er beskrevet.

9.1 A: Klient-tjener mot eksternt system

I dette integrasjonsmønsteret kaller en lokal applikasjon (klient) eksterne fagsystemer som tilbyr forretnings- og datalagringslogikk. Den lokale brukeren forholder seg til presentasjons- og forretningslogikk som ligger i den lokale brukerflaten. Det eksterne fagsystemet tilbyr et datadelingsgrensesnitt som gjør det mulig å hente ut og lagre data, basert på tilgangsstyringsregler som er basert på avtalen mellom virksomhetene og brukerens tjenstlige behov.

I dette integrasjonsmønsteret kan også klienten være delt i to, med en "Backend for frontend" (BFF) mellom det lokale og det eksterne fagsystemet. BFF er typisk en klientnær komponent som hjelper til å sikre og tilpasse grensesnitt som brukes av klienten, og kan også være del av det lokale fagsystemet.

Spesielle karakteristikker ved dette integrasjonsmønsteret er:

- Presentasjons- og forretningslogikk ligger primært i det lokale fagsystemet, mens datalagring er ekstern. Den interne forretningslogikken gis mulighet til å hente og skrive mot de eksterne dataene gjennom standardiserte grensesnitt.
- Åpne og standardiserte grensesnitt gjør det mulig for flere fagsystem å gjenbruke det samme eksterne fagsystemet.
- Tilgangsstyringen av brukeren vil være primært klientens ansvar. Dette vil styres av avtalen mellom virksomhetene og den lokale brukerens tjenstlige behov i hver aktuell kontekst hvor det er behov for å benytte den eksterne tjenesten.
- Brukeren og brukerens virksomhet må ha gjensidig tillit til den eksterne tjenesteleverandøren og ha avtaler som sikrer hvordan partene behandler og lagrer data.

9.1.1 Hva må spesifiseres i dette integrasjonsmønsteret?

Følgende kan beskrives som del av målarkitekturen (eventuelt med referanse til eksterne spesifikasjoner og standarder):

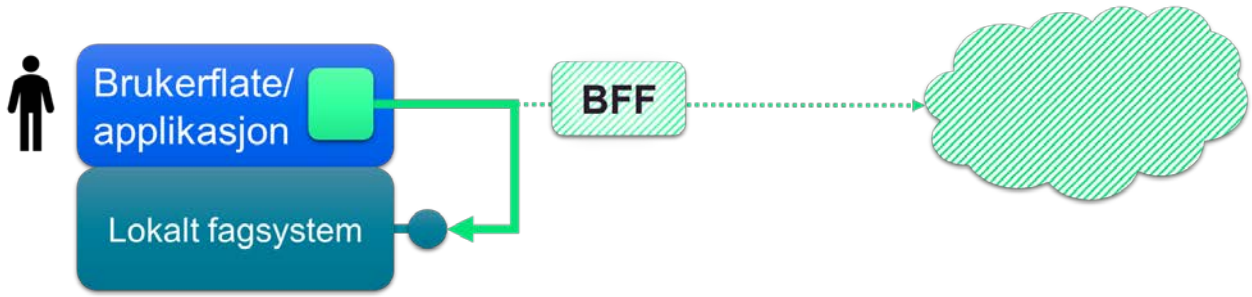
- Hvordan håndteres autentisering og tilgangsstyring for ekstern data- og tjenestegrensesnitt, der informasjon om brukeren primært ligger i det lokale systemet?
- Avtaler, testing, sertifisering etc.
- Hvordan sikres det eksterne fagsystemet for angrep?
- Hvilke standardiserte grensesnitt bør støttes (best å ta dette i et annet dokument)
- Felleskomponenter som brukes – HelseID, MPI, API-katalog, ekstern tjeneste m/tilgangstyringslogikk

9.1.2 Eksempler på anvendelse

A) Kjernejournal tilbyr API for Kritisk Info til helseaktører. API-et kan benyttes av virksomheter med EPJ hvor Kritisk Info kan vises direkte i EPJ-ens brukerflate. Brukere av EPJ-en må autentiseres via HelseID for å få tilgang til kritisk info om en gitt pasient gjennom API-et. Virksomheten må også autentiseres og autoriseres at de har avtale om bruk av API-et.
https://ehelse.no/standarder-kodeverk-og-referansekatalog/standarder-og-referansekatalog/standard-for-kritisk-informasjon-i-kjernejournal-his-1202-2018

B) Sentral forskrivningsmodul (SFM) tilbyr et REST API mot sentral legemiddelmodul hvor det legges til rette for at EPJ-leverandøren selv utvikler GUI. API som tilbys er en utvidelse av FHIR (JSON) som vil understøtte all nødvendig GUI funksjonalitet knyttet til legemiddelmodulen og nødvendige tjenester for å ivareta annen funksjonalitet som EPJ tilbyr.
(https://ehelse.no/Documents/Nasjonale%20prosjekter/Hva%20er%20Sentral%20forskrivningsmodul%20(SFM).pdf)

9.2 A1: Nedlastbar webapplikasjon (basert på SMART on FHIR)



I dette integrasjonsmønsteret laster fagsystemet ned en webapplikasjon fra en ekstern kilde og kjører denne lokalt på fagsystemet. Applikasjonen kan få tilgang til lokale data og tjenester gjennom lokale, standardiserte datadelingsgrensesnitt.

Applikasjonen inneholder forretningslogikk og presentasjonslogikk, men bruker primært datalagring som tilbys av det lokale fagsystemet. Applikasjonen kan også bruke ekstern logikk og ekstern lagring av data. Slik ekstern tilgang kan benytte integrasjonsmønster A.

I utgangspunktet kan mønsteret også inkludere mobile applikasjoner og mer permanent installerte applikasjoner på brukerens datamaskin, men hovedhensikten med mønsteret er knyttet til bruk av rammeverket «SMART on FHIR», der pasientjournalsystemer og andre fagsystemer kan laste ned webapplikasjoner og gi disse tilgang til lokale datadelingsgrensesnitt slik at webapplikasjonene kan hente ut og vise data som ligger lagret lokalt, eller skrive data tilbake til fagsystemet.

Spesielle karakteristikker ved dette integrasjonsmønsteret er:

- Applikasjonen med forretningslogikk og presentasjonslogikk lastes ned fra en ekstern kilde, men gis tilgang til lokale data og tjenester gjennom standardiserte grensesnitt.
- Standardiserte, lokale grensesnitt gjør det mulig for eksterne leverandører å lage applikasjoner som kan brukes mot forskjellige fagsystemer som støtter samme standard.
- De lokale grensesnittene brukes av en lokal bruker, som gjør tilgangsstyring mye enklere.
- Applikasjonen kan også bruke eksterne grensesnitt hos en annen virksomhet, enten spesifikke for applikasjonen eller andre standardiserte grensesnitt tilbudt av andre tjenester eller leverandører. Dersom disse grensesnittene krever tilgangsstyring så må integrasjonen støtte autentisering og tilgangsstyring på tvers av virksomhetsgrenser. Dette behovet dekkes i integrasjonsmønster A.
- Den nedlastbare applikasjonen får potensielt tilgang til lokale, sensitive personopplysninger, på vegne av brukeren. Brukeren og brukerens virksomhet må ha tillit til applikasjonsleverandøren og avtaler som sikrer hvordan applikasjonen behandler og lagrer data, inkludert eventuelt flytting av data ut av det lokale systemet.

9.2.1 Hva må spesifiseres i dette integrasjonsmønsteret?

Følgende kan beskrives som del av målarkitekturen (eventuelt med referanse til eksterne spesifikasjoner og standarder):

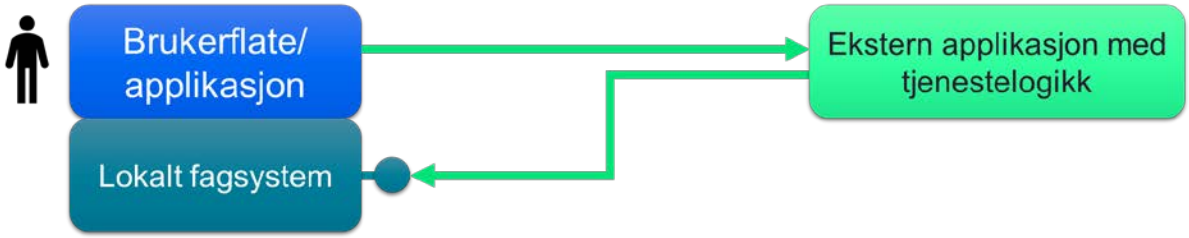
- Hvordan håndteres autentisering og tilgangsstyring for lokale data- og tjenestegrensesnitt?
- Hvordan håndteres autentisering og tilgangsstyring for eksterne data- og tjenestegrensesnitt? (integrasjonsmønster C)
- Hvordan håndteres nedlasting av applikasjoner? Avtaler, sertifisering etc.
- Hvordan sikres applikasjoner fra å angripe systemet eller flytte data ut uten lov?
- Hvilke standardiserte grensesnitt bør støttes (best å ta dette i et annet dokument)
- Felleskomponenter som brukes – applikasjonskatalog (hos EPJ-leverandør eller nasjonalt?), HelseID, ekstern tjeneste m/tilgangsstyringslogikk.

9.2.2 Eksempler på anvendelse

A) **Godkjenning av helse ved fornyelse av førerett**
Helsedirektoratet ønsker at alle leger skal følge samme sjekkliste/metoder ved godkjenning av helse ved fornyelse av førerett. Statens vegvesen ønsker at godkjenningen av helsen skal skje via API.
Direktoratet for e-helse utvikler en nedlastbar webapplikasjon som inneholder presentasjonslogikk for de ulike godkjenningspunktene som legen må gjøre. Webapplikasjonen har behov for pasientinformasjon som må hentes via lokale API-er samt at den må journalføre arbeidet med godkjenningen via kall til API-er. Tilslutt kaller webapplikasjonen et eksternt API hos Veivesenet med selve godkjenningen.

B) https://apps.smarthealthit.org/ er en "appstore" med eksisterende SMART applikasjoner. De fleste av de kan testes. Eksempler:
   a. The chest pain application is an innovative new way to display patient data in the electronic medical records. Based on a given chief complaint of the patient, the app can be programmed to display different data elements from the patient's in-house medical records or from an outside source.

9.3 A2: Ekstern applikasjon med tjenestelogikk gis tilgang til lokalt system



I dette integrasjonsmønsteret kaller det lokale fagsystemet eksterne mikrotjenester som i retur kan vise små informasjonselementer og linker på definerte steder i brukerflaten på fagsystemet. Konfigurasjonsparametre om en mikrotjeneste må være lastet ned og lagt inn i fagsystemet før bruk. Den eksterne mikrotjenesten kan få tilgang til lokale tjeneste- og datagrensesnitt, behandle data eksternt og så returnere informasjon som enkelt kan vises i brukerflaten. Integrasjonsmønsteret består altså primært av lokal presentasjon- og datalagringslogikk, men benytter seg av ekstern forretningslogikk innen visse predefinerte helserelaterte områder.

Integrasjonsmønsteret er basert på standarden «CDS Hooks», et HL7 basert rammeverk som lar eksterne tjenester få tilgang til lokale pasientjournaldata via FHIR baserte ressurser og presentere informasjon i definerte deler av pasientjournalens brukerflate.

Spesielle karakteristikker ved dette integrasjonsmønsteret er:

- Presentasjonslogikk ligger primært i det lokale fagsystemet, mens forretningslogikken er ekstern. Den eksterne forretningslogikken gis mulighet til hente (og skrive?) lokale data gjennom standardiserte grensesnitt, og kan returnere små informasjonselementer som enkelt kan vises i brukerflaten.

- Bruk av standardiserte FHIR baserte grensesnitt i fagsystemene gjør det mulig for eksterne leverandører å lage eksterne applikasjoner som kan brukes av alle fagsystemer med slike standardiserte grensesnitt.
- De lokale datadelingsgrensesnittene brukes av en ekstern tjeneste, på vegne av en lokal bruker. Tilgangsstyringen vil være primært basert på den lokale brukerens rettigheter, men også være styrt av databehandleravtaler med den eksterne tjenesten.
- Den eksterne tjenesten kan også bruke eksterne grensesnitt hos en annen virksomhet, enten spesifikke for applikasjonen eller andre standardiserte grensesnitt tilbudt av andre tjenester eller leverandører. Dersom disse grensesnittene krever tilgangsstyring så må integrasjonen støtte autentisering og tilgangsstyring på tvers av virksomhetsgrenser.
- Brukeren og brukerens virksomhet må ha tillit til den eksterne tjenesteleverandøren og ha avtaler som sikrer hvordan tjenesteleverandøren behandler og lagrer data, inkludert videre distribuering av data som er hentet fra det lokale systemet.

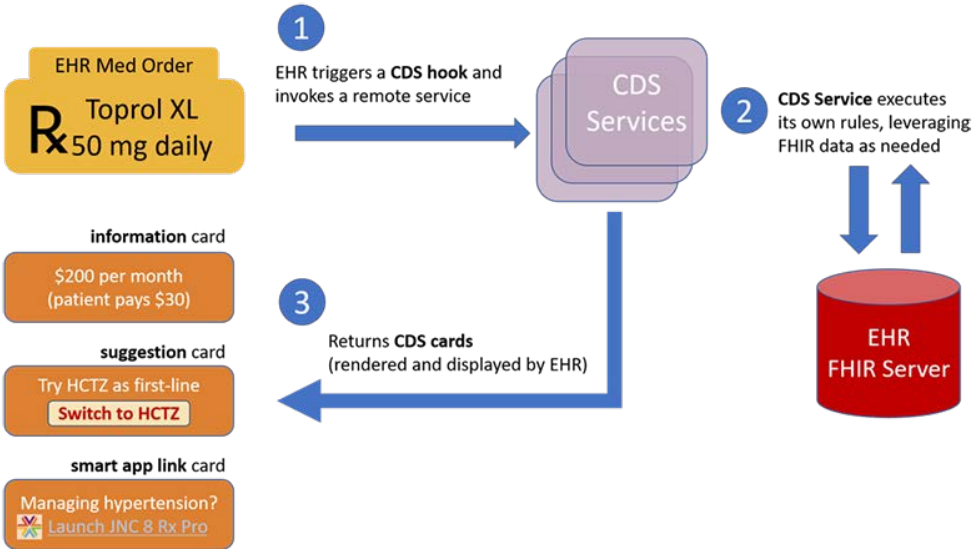
9.3.1 Hva må spesifiseres i dette integrasjonsmønsteret?

Følgende kan beskrives som del av målarkitekturen (eventuelt med referanse til eksterne spesifikasjoner og standarder):

- Hvordan håndteres autentisering og tilgangsstyring for den eksterne tjenesten tilgang til det lokale data- og tjenestegrensesnitt?
- Hvordan finner og stoler fagsystemet på eksterne applikasjoner? Avtaler, sertifisering etc.
- Eventuelt hvordan sikres eksterne applikasjoner fra å angripe systemet eller flytte data ut uten lov?
- Felleskomponenter som brukes – katalog over eksterne tjenester (hos EPJ-leverandør eller nasjonal?), HelseID, ekstern tjeneste m/tilgangsstyringslogikk

9.3.2 Eksempler på anvendelser

1. http://sandbox.cds-hooks.org/ viser en demo på en ekstern CDS hooks tjeneste som regner ut prisen for legemidler som en lege forskriver. EPJen vil kalle en eller flere eksterne tjenester når en lege foreskriver en resept. For eksempel, når en prisingstjeneste er konfigurert til å svare på denne hendelsen, mottar den koden for medisinen, sjekker den vanlige prisen pasienten betaler og kan da foreslå et mer kostnadseffektivt alternativ.



2. Kliniske anbefalinger som inneholder link til nedlastbare applikasjoner (integrasjonsmønster B): https://www.youtube.com/watch?v=cI_33sTIXKY.
3. Integrasjonsmønsteret kan brukes der man har behov for at sentrale tjenester eller andre systemer skal kunne vise små informasjonsmengder i en EPJ brukerflate, der man kun ønsker å vise litt informasjon fra den eksterne kilden. Dette kan være priser på legemidler, status på frikort, grunndatainformasjon, informasjon fra kontaktregisteret, indikasjon om informasjon er tilgjengelig i en annet system osv.

9.4 C: Automatiserte prosesser som klient mot eksternt system (Maskin-til-maskin)

I dette integrasjonsmønsteret kaller to forskjellige fagsystemer hverandre, uten at en spesifikk bruker er involvert i flyten. Kallene gjøres altså ikke på vegne av spesifikke brukere, men det gis tilgang basert på virksomhetsautentisering og avtaler mellom virksomhetene. Slike integrasjonsmønstre kan for eksempel brukes hvis en virksomhet vil informere en annen virksomhet om en hendelse som bør følges opp av virksomheten, eller for å overføre batchvis informasjon og oppdateringer om pasienter.

Spesielle karakteristikker ved dette integrasjonsmønsteret er:

- Ingen brukere er direkte involvert i dataflyten, og det utleverende systemet kan derfor ikke logge hvilken bruker som får tilgang til eventuelle sensitive helseopplysninger.
- Informasjon som utveksles kan trigge en senere flyt av informasjon basert på de andre integrasjonsmønstrene.

9.4.1 Hva må spesifiseres i dette integrasjonsmønsteret?

Følgende kan beskrives som del av målarkitekturen (eventuelt med referanse til eksterne spesifikasjoner og standarder):

- Avtaler om hvordan data fra det eksterne fagsystemet eventuelt kan lagres og gjøres tilgjengelig for lokale brukere på et senere tidspunkt, basert på tjenstlig behov.
- Hvordan håndteres autentisering og tilgangsstyring av fagsystemene som tilhører forskjellige virksomheter.
- Tillit, Avtaler, testing, sertifisering etc.
- Felleskomponenter som brukes – HelseID, Maskinporten, MPI, API-katalog, ekstern tjeneste m/tilgangsstyringslogikk

9.4.2 Eksempler på anvendelser

A) Et responssenter tilbyr tjenester for å følge opp pasienter som bor hjemme med velferdsteknologi. Responssenterløsningen har behov for å ha en oversikt over alle pasienter som har velferdsteknologi hjemme for en gitt kommune slik at når varsler fra en velferdsteknologienhet mottas, så kan varslet kobles til riktig pasient. Responssenterløsningen kaller (via velferdsteknologiknutepunktet) et API hos kommunens EPJ som gir ut informasjon om alle pasienter med velferdsteknologi utplassert av kommunen.

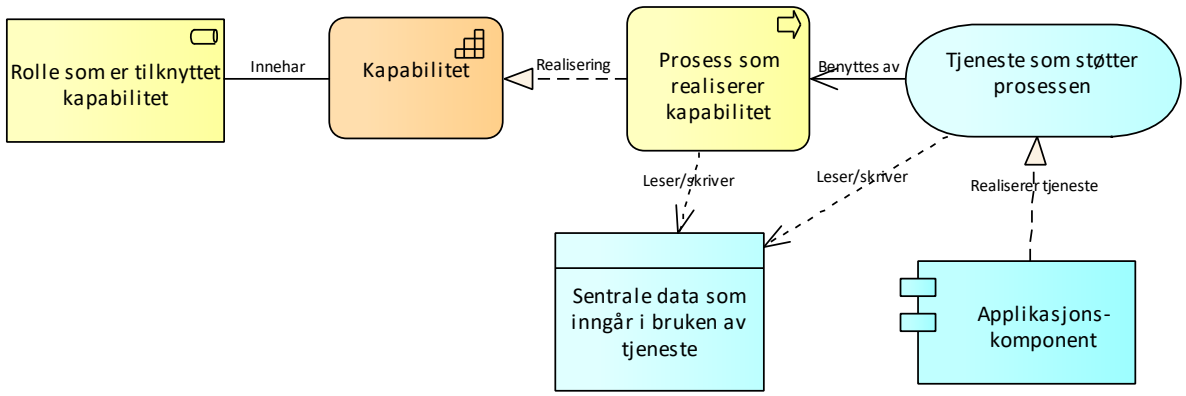
B) En virksomhet har behov for å bli varslet om en spesiell hendelse for en spesiell pasient har oppstått hos en annen virksomhet. Når hendelsen oppstår, kaller virksomheten automatisk den andre virksomheten med informasjon om hendelsen.

C) En kommune har behov for å motta lister over pasienter som skal skrives ut til kommunen, for å kunne forberede hjemmehjelp og sykehjem på utskrivelsen. I dette integrasjonsmønsteret kan da kommunens system sette opp et abonnement på utskrivningshendelser eller laste ned slik informasjon periodisk.

Vedlegg 2 Hvordan lese modellene for arkitektur

For å beskrive hvilke behov som ulike felleskomponenter løser, så er det beskrevet løsningsmønstre som gir en beskrivelse – på overordnet nivå – når og i hvilke kontekster felleskomponenter benyttes. Figur 34 forklarer hvordan modellene må leses.

Figur 34 Grunnleggende elementer i modellen og deres sammenheng



Vedlegg 3 Deltagere i arbeidsgruppen

Tabell 3 Virksomheter med i arbeidsgruppen med sektoren

Liste over virksomheter som har stilt med representanter i prosjektets arbeidsgruppe
Helse Vest
Helse Nord
Helse Sør-Øst
Nasjonal IKT (NIKT)
Kommunal informasjonssikkerhet (KINS)
KS
Bergen kommune
Stavanger kommune
Oslo kommune
Trondheim kommune

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no