Direktoratet for e-helse

Målarkitektur for datadeling i helse- og omsorgssektoren

Versjon 1.0

Merknad 25.09.2024
Dette dokumentet ble utarbeidet av Direktoratet for e-helse. Det vil bli oppdatert som en del av arbeidet med digital samhandling.

HITR 1231:2021

Tittel:
Målarkitektur for datadeling i helse- og omsorgstjenesten

Rapportnummer:
HITR 1231:2021

Utgitt:
03/2021

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 omsorgstjenestene og ta i bruk innovative løsninger. Samtidig stiller en slik digitalisering høye krav til sikkerhet og personvern.

Helse- og omsorgssektoren har behov for bedre samhandling og løsninger som effektiviserer tjenestene. 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. Dette økosystemet skal dekke samhandlingsbehovene til helsepersonell og innbyggere, og samtidig sikre at taushetsbelagte opplysninger ikke kommer på avveie.

Målarkitektur for datadeling beskriver behovet for felleskomponenter som vil være en forutsetning for et levedyktig og sikkert økosystem. Det må være en lav terskel og lite byråkrati for dataansvarlige å dele sine helseopplysninger med andre helsepersonell og pasienten selv. Felleskomponentene skal gjøre aktørenes etablering av datadeling enklere. I tillegg skal 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.

Denne rapporten om målarkitektur for datadeling fokuserer i hovedsak på teknisk samhandlingsevne, men belyser også problemstillinger på de organisatoriske og juridiske områdene. For å etablere datadeling som en standardisert samhandlingsform, er det behov for å gjennomføre tiltak i alle de 4 samhandlingsevnene i "EIF-modellen", der de juridiske, semantiske og organisatoriske samhandlingsevnene er vurdert som spesielt viktige. Det vil være andre tiltak for datadeling som vil håndtere disse tre.

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

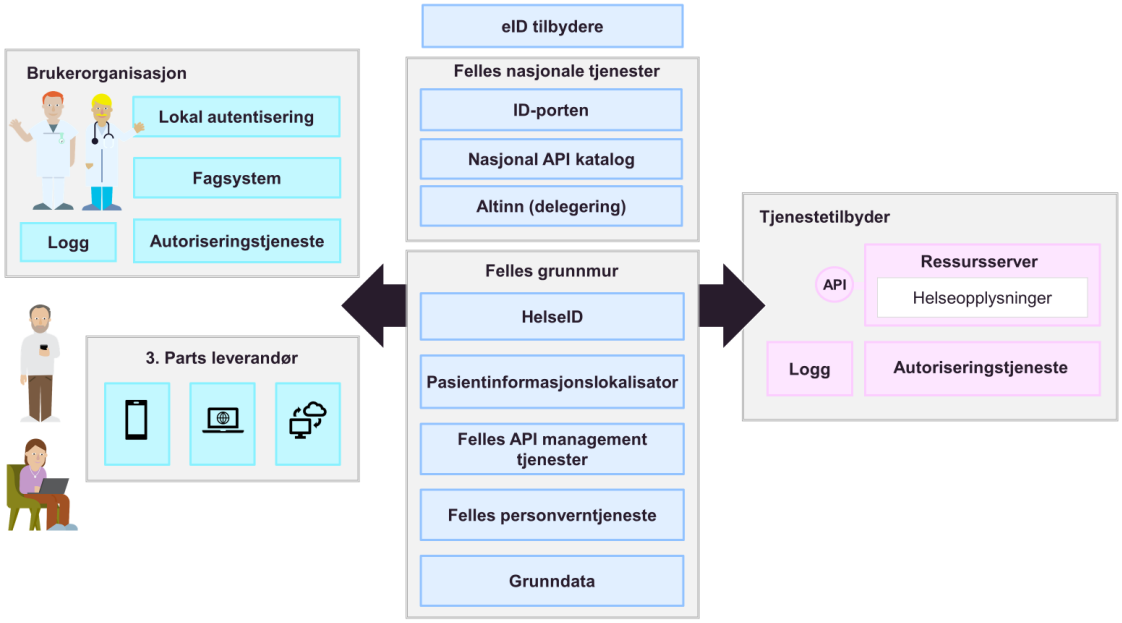
Dokumentet er delt i tre for at leseren enklere skal kunne navigere seg til relevante deler av dokumentet hvor del 1) omhandler innføring i behovet for datadeling og valg av felleskomponenter i målarkitekturen, del 2) de ulike kapabilitetene som må på plass for å realisere målarkitekturen, og til slutt del 3) som beskriver de mer detaljerte vurderingene som ligger bak arkitekturvalgene i del 1).

Målarkitekturen peker ut en fremtidig ønsket arkitektur og tar ikke for seg hvordan denne arkitekturen skal realiseres. Det er ikke gjennomført kvantitativ kost-/nytteanalyse for målarkitekturen og det forutsettes at dette gjøres før en investering og realisering av felleskomponentene. Målarkitekturen kan derfor sees som en reguleringsplan for realisering av datadeling, der hovedformålet er å beskrive nødvendige forretningsmessige evner (kapabiliteter) og felleskomponenter som bør etableres for datadeling. Dokumentet gir derfor heller ikke en tidsplan for realisering.

I arbeidet med målarkitekturen fremkom det at behovene for felleskomponenter for datadeling var ulike, basert på hvilke aktører og brukertyper som er involvert i datadelingen. Det er tatt utgangspunkt i behovene og de lovmessige rettighetene til innbyggere og helsepersonell. Helsedataområdet er holdt utenfor i denne omgang. Målarkitekturen

inkluderer to bruksområder og behovene for felleskomponenter er behandlet atskilt for hvert av områdene:

1. Sektorens samhandling med grunnmur og nasjonale e-helseløsninger
2. Innbyggers behandling av sine helseopplysninger



Figur 1 viser en oppsummering av målarkitekturen for innbygger og nasjonale tjenester.

Gjennom arbeidet med referansearkitekturen for datadeling har vi identifisert flere sentrale byggeklosser. Vurdering av disse byggeklossene er i dokumentet inndelt i disse kategoriene:

1. Felles tillitsøkende tjenester inkludert autentisering, autorisering, sperringer, fullmakter og samtykker.
2. Felles API-katalog
3. Tjenester for felles API håndtering (heretter kalt API management)
4. Felleskomponent for lokalisering av pasientinformasjon
5. Felleskomponent for logging

For de viktigste kapabilitetene i del 2) er det beskrevet løsningsmønstre som beskriver de forretningsmessige stegene som må utføres for å ta i bruk datadeling og hvilke felleskomponenter som er involvert i disse. Løsningsmønstrene er basert på samme metode som Digitaliseringsdirektoratet benytter i sitt arbeid med å beskrive tverrsektoriell datadeling.

Målarkitekturens konsekvens for aktørene er at de må bruke felleskomponenter for datadeling inn mot nasjonale e-helseløsninger og i datadeling mot innbyggerne. Dette vil forenkle bruk av nasjonale e-helseløsninger og gjøre det enklere for leverandører av innbyggertjenester å tilby konsistente løsninger på tvers av helseaktører. Flere bruksområder beskrevet i målarkitekturen er ikke behandlet da disse områdene trenger mer koordinering med andre programmer og prosjekter. Disse er for eksempel datadeling mellom virksomheter, lokal integrasjon og innovasjon, og helsedataområdet.

I innspillsrunden til *målarkitekturen* nevnte flere aktører at det haster å få på plass datadeling. Direktoratet for e-helse deler utålmodigheten i sektoren og ønsket om å dekke

flere bruksområder enn målarkitekturen gjør i denne versjonen. Vi ser også at det er viktig å få delt arbeidet som er gjort i denne runden, og heller legge inn arbeid i nye versjoner i tiden fremover. Målarkitekturen står heller ikke alene, og komplementeres av andre normerende produkter og pågående programmer som bidrar i det totale bildet.

DEL 1:

Datadeling og felleskomponenter i målarkitekturen

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 digital 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 sektoren. Med det ønsker man en raskere utvikling og gevinster for virksomheter, helsepersonell, innbyggere og leverandørmarkedet, samt unngå omfattende opprydding i etterkant på grunn av fragmenterte løsninger med lav samhandlingsevne.

I 2018 ble det publisert en referansearkitektur for datadeling som beskriver en beste praksis for realisering av løsninger som benytter datadeling[8]. Referansearkitekturen inneholder arkitekturprinsipper, begrepsmodell, brukstilfeller, aktører og generiske komponenter og deres sammenheng. Målarkitekturen er basert på dette arbeidet.

1.2 Målsetning

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.
- 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.

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 løsningene i 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.

Ulike bruksområder for datadeling setter ulike krav til målarkitekturen. Målarkitekturen inkluderer to bruksområder i denne versjonen. Dette er beskrevet i kapittel 6.

1.3 Målgruppe

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

Del 1: Vi anbefaler denne delen til alle interessenter av målarkitektur for datadeling. Del 1 gir et raskt overblikk over hva målarkitekturen består av og beskriver nødvendige felleskomponenter for sektoren innenfor bruksområdene. Det er også en introduksjon til målbildet for datadeling og behovet for økt datadeling.

Del 2: Målgruppe for denne delen er arkitekter og tekniske personer som ønsker å forstå hvilke kapabiliteter som må etableres for å realisere målbildet. Det vil også være nyttig for tekniske ledere for å få innsikt i hvilke prosesser som må på plass.

Del 3: Målgruppe er arkitekter og tekniske personer som ønsker å forstå bakgrunnen for arkitekturvalgene i del 1.

Se også mer om normeringsnivå i kapittel 1.8.

1.4 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 og plikter til innbyggere og helsepersonell. Ut ifra dette er det beskrevet ulike bruksområder for datadeling, se kapittel 4. 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. Omfanget for målarkitekturen baserer seg på føringer fra sektoren.

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 2 viser Digitaliseringsdirektoratets 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 juridiske, 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.

1.4.1 Føringer fra sektoren

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 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. Tjenester for felles API management 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 den anbefalte tillitsmodellen hvor tjenstlig behov skal håndheves av anvendende virksomhet heretter kalt brukerorganisasjonene[1]. 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*" [14].

1.5 Forankring av arbeidet

Målarkitekturen for datadeling er utarbeidet av et leveranseteam bestående av representanter fra Direktoratet for e-helse og flere produktmiljø fra Norsk Helsenett, inkludert Kjernejournal, Helsenorge og HelseID. 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.

I arbeidsgruppen har det deltatt representanter fra Helse Vest RHF, Helse Nord RHF, Helse Sør-Øst RHF, Nasjonal IKT (NIKT), Kommunal informasjonssikkerhet (KINS), KS, Bergen kommune, Stavanger kommune, Oslo kommune og Trondheim kommune.

1.6 Forvaltning av målarkitekturen

Målarkitekturen vil følge normerende produkters forvaltningsprosess hos Direktoratet for e-helse, slik at målarkitekturen oppdateres jevnlig. Det er flere arkitekturtemaer som vi har valgt å utsette med bakgrunn i at arbeidet er avhengig av andre prosjekter eller utredninger som ikke var ferdige da arbeidet med dette dokumentet pågikk. Se kapittel 10 - *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.

1.7 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 retningslinje og gjelder hovedsakelig helsevirksomheter i helsesektoren, men systemleverandører vil også indirekte berøres av denne målarkitekturen. 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].

[1] Vi har kalt den konsumerende part innenfor datadeling for *brukerorganisasjon*. Det brukes ulike begreper på denne type rolle i andre normerende produkter fra E-helse. Begrepet tilsvarer eksempelvis *konsumerende virksomhet* og *konsument av helseopplysninger*.

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"*.

Målbildet er at helsesektoren etablerer datadeling på tvers for å gi tilgang til data om en bestemt pasient, for at helsepersonell kan yte best helsehjelp til pasienten. Det kan være nødvendig for behandlingen blant annet å se historikk over tidligere undersøkelser og behandlinger. Datadeling mellom virksomheter vil muliggjøre overføring av informasjon på tvers av virksomhetsgrenser og omsorgsnivåer, samt legge 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 er relevant og nødvendig for å gi helsehjelp.

Innbyggere er helsetjenestens viktigste samarbeidspartnere og er en viktig brukergruppe for datadeling. Innbyggere 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 hele eller deler 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 dette dokumentet 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. Vi ønsker at målarkitekturen på denne måten vil gi grobunn for innovasjon og næringsutvikling.

Overordnet støtter målarkitekturen seg på den nasjonale strategien om å gi alle innbyggere i Norge sammenhengende tjenester på tvers av sektorer, ved at vi tar utgangspunkt i de nasjonale felleskomponentene der hvor det dekker sektorens behov [21].

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 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. Målarkitektur for dokumentdeling[20] støtter punkt 1.

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 [1] 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."

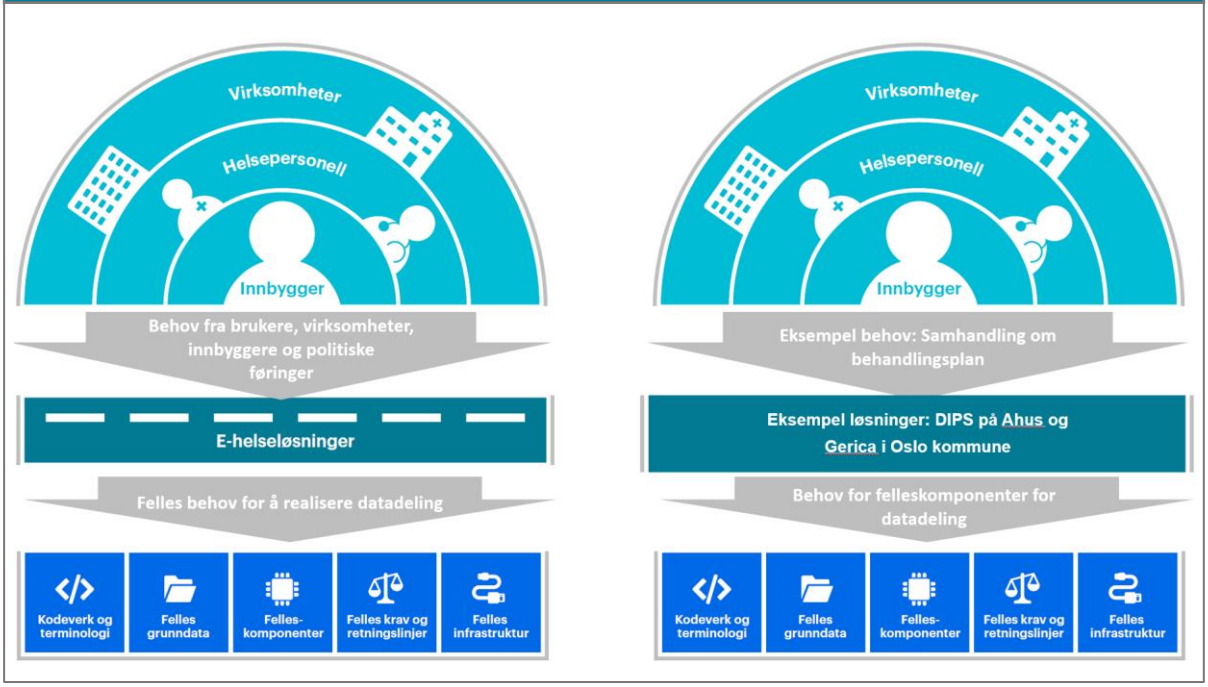
Plan for felles grunnmur definerer følgende resultatmål relatert til datadeling:

> 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. Figur 3 viser hvordan datadeling kan løse felles behov for samhandling.

Figur 3 Eksempel på hvordan målarkitektur for datadeling bidrar til å løse felles samhandlingsbehov



3 Datadeling som samhandlingsmodell

3.1 Hva er datadeling?

På grunn av at behovene for samhandling i helsesektoren er så omfattende, har Direktoratet for e-helse valgt å generalisere samhandlingsbehovene i seks samhandlingsmodeller [16]. En av disse er datadeling som er definert under.

> Datadeling er en samhandlingsmodell i helsesektoren hvor strukturerte data om en pasient deles i sanntid på tvers av virksomheter og med innbygger i helsesektoren

Når vi i målarkitekturen snakker om datadeling, så mener vi alle behovene for samhandling som kan løses ved å dele strukturerte data om en pasient, både muligheten for å lese, behandle og oppdatere data via datadeling.

Samhandlingsmodellen for datadeling i helsesektoren beskriver generaliserte behov som tilhører organisatorisk samhandlingsevne (ref. EIF modell). Datadeling kan teknisk realiseres på flere måter (teknisk samhandlingsevne), men i helsesektoren er det enighet i at førstevalget for realisering av datadeling skal være ved bruk av API.

API betegner et grensesnitt i en programvare slik at spesifikke deler av programvaren kan aktiviseres fra en annen programvare (definisjon hentet fra [8]). 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.

3.2 Når benyttes datadeling?

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

1. Selvbetjent tilgang til helseopplysninger hos andre virksomheter for å yte, administrere eller kvalitetssikre helsehjelp
2. Samarbeid om ytelse av helsehjelp på tvers av flere virksomheter som medfører oppdatering av helseopplysninger gjennom felles ressurser/tjenester.
3. Dele helseopplysninger med innbygger når innbygger benytter egne applikasjoner eller innbyggertjenester på Helsenorge benytter eksterne tjenester.
4. Dele administrative grunndata, både felles offentlige grunndata og helsesektor spesifikke grunndata.
5. Dele helseopplysninger med offentlige etater slik som (men ikke begrenset til) Nav, Helfo, Politiet, Vegvesenet, Skatteetaten
6. Dele helseopplysninger for forsknings- og kvalitetsforbedringsformål

Aktører i helse- og omsorgstjenesten er i dette dokumentet definert som pasienten selv (eller noen som representerer pasienten) og aktører som er dataansvarlige for et behandlingsrettet register. Det skilles i dette dokumentet ikke på private og offentlige dataansvarlige.

Datadeling med bruk av API 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 anvendelser hvor det også er behov for å skrive til andre systemer via API. Teknisk sett har vi erfart at behovet for felleskomponenter er lik uavhengig av om det er snakk om å lese eller skrive.

3.3 Hva er status på informasjonsdeling i helse- og omsorgstjenesten i dag?

Dagens etablerte former for informasjonsdeling mellom helsepersonell i andre virksomheter gir ikke tilstrekkelig oversikt over relevant informasjon om en pasient og det er for arbeidskrevende å skaffe en slik oversikt. Helsepersonell har i dag i liten grad selvbetjent tilgang til helseopplysninger utenfor sin egen virksomhet.

Dette medfører en stor risiko for at helsepersonell ikke får tilstrekkelig informasjon for å yte forsvarlig helsehjelp til pasienter som har blitt behandlet andre steder tidligere. Mangel på relevant og nødvendig informasjon kan gå ut over pasienters liv og helse ved at de ikke gis korrekt og effektiv behandling.

Informasjonsdeling med helsepersonell utenfor egen virksomhet baserer seg i dag oftest på utlevering av informasjon 1-1 mellom helsepersonell hvor ulike metoder som elektronisk

meldingsutveksling, telefon og faks benyttes. For planlagte behandlinger skjer informasjonsdelingen i dag ved hjelp av meldingsutveksling. For uplanlagt behandling og der meldingsutvekslingen ikke gir tilstrekkelig informasjon, må avtaler om utlevering typisk gjøres 1-1 via telefonsamtaler og faks mellom behandlingssteder. Dette fordrer at behandlingstedet blir gjort kjent med at det faktisk foreligger en relevant historikk fra andre behandlingssteder, at de er i stand til å finne ut hvor dette er, for deretter å henvende seg direkte for å avtale utlevering.

3.4 Hvorfor ta i bruk 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.
- Behov for å kunne fordele ansvaret for helsehjelp mellom virksomheter og sikre at den blir fulgt opp.

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. Les mer om relevante lover og forskrifter i Vedlegg A.

3.5 Hva kreves av dataene?

Et område vi ikke dekker i dette dokumentet er semantisk samhandlingsevne (ref EIF modellen). For å realisere datadelingsløsninger må også semantisk samhandlingsevne etableres.

Forutsetninger for å oppnå semantisk samhandlingsevne er

- Felles informasjonsmodeller
- Felles begrepsdefinisjoner, kodeverk og terminologi
- Felles format og syntaks for utveksling

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.

Strukturerte data kan ha forskjellig betydning i forskjellig kontekster og gjennom standardisering av API-er vil strukturerte data kunne enklere gjenbrukes på tvers. 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 og kjønn)
- Sammendrag av kliniske pasientdata (f.eks. allergier, implantater og nylige kirurgiske inngrep)
- Informasjon om pasientens medisinbruk
- Metadata om journalen

Direktoratet har utgitt en veileder om IPS[22].

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 strukturerte 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 [13].

3.6 Hvordan få tilgang til helseopplysninger?

Helsepersonell har taushetsplikt om opplysninger de får vite i egenskap av å være helsepersonell jf. helsepersonelloven § 21.

Deling av opplysninger skal skje innenfor de rettslige rammene for tilgjengeliggjøring av helseopplysninger etter helsepersonelloven §§ 25, 45 og pasientjournalloven § 19. Vilkårene for at dataansvarlig kan tilgjengeliggjøre opplysningene etter disse bestemmelsene er at dette skjer innenfor rammen av helsepersonells taushetsplikt, og at opplysningene er relevante og nødvendige for å yte, administrere og kvalitetssikre helsehjelp på en forsvarlig måte (tjenstlig behov).

En sentral forutsetning for datadeling mellom virksomheter i helsesektoren er at 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.

Tilgangskontroll er den mekanismen som innvilger innsyn i helseopplysninger og for datadeling må slike kontroller automatiseres. 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 personellet er ansatt i. I den anbefalte tillitsmodell [10] er dette en av anbefalingene som ligger til grunn for videre arkitekturarbeid.

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 virksomheten. Tjenstlig behov kan også være avhengig av at den som ønsker tilgang er med i en behandlingsprosess, svarer på telefonforespørsler fra pasient eller lignende.

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.

3.7 Kan en pasient motsette seg deling?

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 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 helsepersonells tilgang til sine helseopplysninger er 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.

3.8 Finnes det ikke allerede mange API-er i dag?

API-er har eksistert i flere titalls år. Mange av dagens e-helseløsninger har API-er. Men når det snakkes om API-er, så kan det ofte misforstås hvor klare API-ene er for bruk av andre utenfor virksomhetene som eier e-helseløsningene. 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 i bruk 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 publisert en Veileder for åpne API [15] 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

3.9 Tilrettelegge for innovasjon og næringsutvikling?

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

Resultatmål 7 i Plan for utvikling av felles grunnmur [1] 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 i bruk 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. Det er utenfor omfanget for målarkitekturen å beskrive økosystemet som helhet.

4 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 hvert enkelt bruksområde. Følgende bruksområder hvor datadeling benyttes er identifisert og behandlet i arbeidet med dette dokumentet:

1. Sektorens samhandling med grunnmur og nasjonale e-helseløsninger
2. Innbyggers samhandling med helse- og omsorgstjenesten
3. Samhandling mellom helsepersonell på tvers av virksomheter
4. Samhandling med helsepersonell og innbyggere lokalt

Det er kun de to første bruksområdene som blir beskrevet i målarkitektur for bruksområder i kapittel 6, men for arkitekturvurderingene i Del 3 er alle 4 bruksområdene inkludert

I tillegg er følgende bruksområder identifisert, men ikke behandlet i arbeidet med dette dokumentet:

a) Samhandling med andre offentlige etater og tjenester utenfor helse- og omsorgstjenesten.
b) Innbyggers deling av egeninnsamlet helseopplysninger fra bruk av privat utstyr
c) Pasienters behov for å samhandle med andre pasienter
d) Samhandling om helsedata for sekundærformål

Alle bruksområdene blir kort beskrevet videre i dette kapittelet.

4.1 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.

4.1.1 Oppslag, oppdatering/registrering i nasjonal e-helsetjeneste

Nasjonal e-helsetjeneste slik som Kjernejournal og Reseptformidleren benyttes som samhandlingsløsninger hvor en av formålene er å unngå mange til mange samhandlingsformer. Kritisk info i Kjernejournal er et eksempel hvor 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.

4.1.2 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 (ikke uttømmende):

- Adresseregisteret (AR)
- Bedriftsregisteret (BedReg)
- 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)

4.2 Innbyggers samhandling med helse- og omsorgstjenesten

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 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 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.	Innbyggertjenestene "Bytte fastlege", "endre timer" og "pasientreiser" benyttes av innbyggerbenyttet applikasjon ved bruk av datadeling

Med Innbygger	Beskrivelse	Eksempler
Skjemaregistrering	Innbygger skal kunne 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 og helseundersøkelser (som HUNT)

4.3 Samhandling mellom helsepersonell på tvers av virksomheter

Dette bruksområdet dekker brukstilfeller som i hovedsak dekker behovet for at helsepersonell i ulike virksomheter må samhandle 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 dokumentdeling via Kjernejournal, Akson journal 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 ulik tidshorisont på når 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].

Dette bruksområdet dekker samhandling gjennom datadeling mellom aktører i ulike helseregioner og mellom aktører i helseregioner 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.

4.4 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 behovet for bruk av datadeling i sluttbrukerapplikasjoner som kan gjenbrukes av flere virksomheter i sektoren. I tillegg skal bruksområdet legge til rette for at nye leverandører skal kunne enklere konkurrere om å lage sluttbrukerapplikasjoner, som benytter datadeling mot interne systemer, 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.

Området er knyttet til samhandlingsbehov helsepersonell har internt i en virksomhet og er normalt utenfor omfanget av nasjonal arkitekturstyring. Det er likevel tatt med på grunn av behovet for å utnytte leverandørmarkedet for utvikling av datadeling i sluttbrukerapplikasjoner og behovet for å standardisere fellesfunksjonalitet for datadeling slik at samme sluttbrukerapplikasjoner kan gjenbrukes mest mulig på tvers av virksomheter.

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. Bruksområdet er derfor relatert til hvordan man kan åpne disse fagsystemene og få andre eksterne leverandører til å utvikle sluttbrukerapplikasjoner som benytter datadeling mot interne systemer.

Temaet ble ikke godt nok dekket i arbeidet med dette dokumentet og dette må det jobbes videre med.

4.5 Samhandling med andre offentlige etater og tjenester utenfor helse- og omsorgstjenesten

Virksomheter i helse- og omsorgstjenesten har behov for å samhandle om helseopplysninger med andre offentlige etater og tjenester ved bruk av datadeling. Dette bruksområdet er ikke behandlet i dette dokumentet.

4.6 Innbyggers deling av egeninnsamlet helseopplysninger fra bruk av privat utstyr

Flere og flere innbyggere går til anskaffelse av kommersielt utstyr som samler inn og lagrer helseopplysninger om personen som bærer utstyret. I behandlingssituasjoner kan det være aktuelt å dele disse opplysningene med helsepersonell ved hjelp av datadeling. Dette bruksområdet er ikke behandlet i dette dokumentet.

4.7 Pasienters behov for å samhandle med andre pasienter

Når innbygger blir syke, har de ofte behov for å dele erfaringer med andre som har samme diagnoser. Internasjonalt er det en utvikling at det etableres fora hvor dette er mulig. Datadeling vil kunne være en viktig kommunikasjonsform for slike løsninger. Dette bruksområdet er ikke behandlet i dette dokumentet.

4.8 Samhandling om helsedata for sekundærformål

Sekundærbruk av helsedata er bruk av helsedata der formålet ikke er å yte helsehjelp til enkeltindividet.

Dette omfatter blant annet helseforskning, styring og beslutningsstøtte for helse- og omsorgstjenestene, oppfølging av befolkningens helsetilstand, kvalitetsforbedring av helsetjenesten og innovasjon og næringsutvikling. Dette bruksområdet dekker samhandling av helsedata for slike formål. Bruksområdet er ikke behandlet i dette dokumentet, men er behandlet i helsedataprogrammet[18].

5 Felleskomponenter

Felleskomponenter defineres som komponenter som kan gjenbrukes i flere IT-løsninger og utvikles iterativt for å dekke felles behov. De kan brukes på tvers av e-helseløsninger, virksomheter og forvaltningsnivå, og kan enten være frivillig eller påkrevd å bruke. Felleskomponenter vil kunne øke utbredelse av datadelingsløsninger og vil legge til rette for at virksomheter raskere kan være i stand til å oppfylle kravene til personvern og informasjonssikkerhet.

I arbeidet med målarkitekturen har det blitt diskutert hvilke felleskomponenter som helsesektoren bør etablere for datadeling. De nasjonale felleskomponentene (fra Digdir) dekker kun deler av helsesektorens behov og helsesektoren har derfor behov for å etablere egne felleskomponenter. Dette kapittelet oppsummerer hvilke felleskomponenter som sektoren har behov for og som legges til grunn i målarkitekturen for datadeling. Arkitekturvurderingene som ligger bak disse felleskomponenter behandles i del 3.

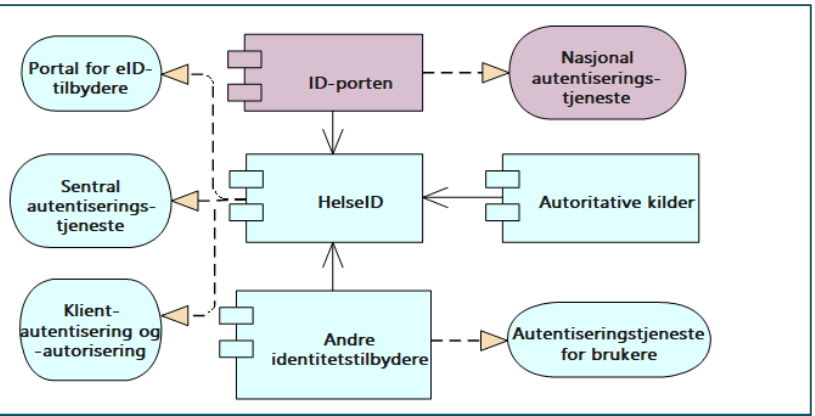
5.1 HelseID

HelseID er i dag en felleskomponent i helsesektoren som understøtter identitets- og tilgangsstyring mellom aktørene i helsesektoren. HelseID er en teknisk komponent som legger til rette for at aktørene skal kunne ha tilstrekkelig tillit for å dele data og dokumenter mellom seg.

HelseID tilbyr tjenester for at helsepersonell kan få engangspålogging (single sign-on). Personell som er autentisert med tilstrekkelig sikkerhetsnivå (eID) lokalt, vil ved bruk av HelseID kunne få tilgang til nasjonale e-helseløsninger, og data og dokumenter ved andre helsevirksomheter, via én sikker pålogging.

HelseID kan også videreformidle informasjon fra brukerens fagsystem og autoritative kilder (slik som Helsepersonellregisteret) for å bekrefte brukerens autorisasjon, herunder om brukeren er helsepersonell. HelseID benyttes i dag i utvalgte nasjonale e-helseløsninger, nasjonale helseregistre og kvalitetsregistre. I Figur 4 er HelseID sine 3 hovedtjenester beskrevet, og disse legges til grunn for behovet for HelseID som en felleskomponent i målarkitekturen.

1. En portal hvor brukerorganisasjoner og andre eID-tilbydere kan tilby sine digitale identiteter
2. Sentral autentiseringsløsning for applikasjoner som bruker portalen i punkt 1
3. Klientautentisering og – autorisering. Sikring av API hvor sluttbrukers identitet transporteres i sikkerhetsbilletter



Figur 4 HelseID sine tillitsøkende tjenester (rød farge = nasjonale felleskomponenter)

5.1.1 **Portal over godkjente** eID-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. Dette vil tilrettelegge for engangspålogging ("single sign-on").

5.1.2 **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.

5.1.3 **Klientautentisering**

For at en API-eier skal kunne tillate en annen virksomhet tilgang til sitt API har API-eier behov for å autentisere klienter fra denne virksomheten. En klient i datadelingssammenheng er et fagsystem eller en integrasjonsløsning hos en brukerorganisasjon. Teknisk sett autentiseres klienten og klienten kobles til brukerorganisasjonen gjennom en klientkonfigurasjon hos HelseID.

5.1.4 **Klientautorisering**

En API-eier må kun akseptere forespørsler til deres API fra brukerorganisasjoner som er forhåndsgodkjente til å motta eller endre deres helseopplysninger. Dette kan gjøres ved klientene fra en gitt brukerorganisasjon autoriseres for få tilgang til å kalle API-et til API-eier. Denne oppgaven tilbyr HelseID som en tjeneste til API-eiere. En API-eier kan også velge å benytte egen løsning for detaljert Klientautorisering, selv om HelseID benyttes for Klientautentisering.

Arkitekturvalg 1

Målarkitekturen legger til grunn at HelseID skal være en felleskomponent for datadeling som tilbyr:

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

1b) Tjeneste for å autentisere og autorisere klienter (fagsystemer eller integrasjonsløsninger) som en API-eier **kan** velge å benytte.

5.2 Innbygger-STS

Målarkitekturen legger til grunn en egen felleskomponent som tilbyr tillitsøkende tjeneste for innbyggers bruk av API-er fra helsesektoren gjennom innbyggerbenyttede applikasjoner. Felleskomponenten skal bygge på Helsenorge sin sikkerhetstjeneste som også inneholder funksjonalitet som kun dekker Helsenorge sine behov. Vi har valgt å kalle den delen av Helsenorge sin sikkerhetstjeneste som leverer fellestjenester til sektoren for Innbygger-STS

I dag understøtter Helsenorge sikkerhetstjenesten datadeling ved å tilby tjenester for autentisering og autorisasjon av innbyggere for Helsenorge sine to hovedkomponenter:

1. En integrasjonsplattform mellom innbygger (pasienten) og øvrige systemer i sektoren.
2. En web-portal der innbygger får tilgang til en rekke tjenester samt datautveksling og datadeling med sektoren via integrasjonsplattformen i 1).

Sikkerhetstjenesten støtter i dag også innbyggerbenyttede applikasjoner som benytter datadelingsgrensesnitt på integrasjonsplattform. Denne støtten inkluderer håndtering av samtykkebasert tilgang, som er beskrevet under.

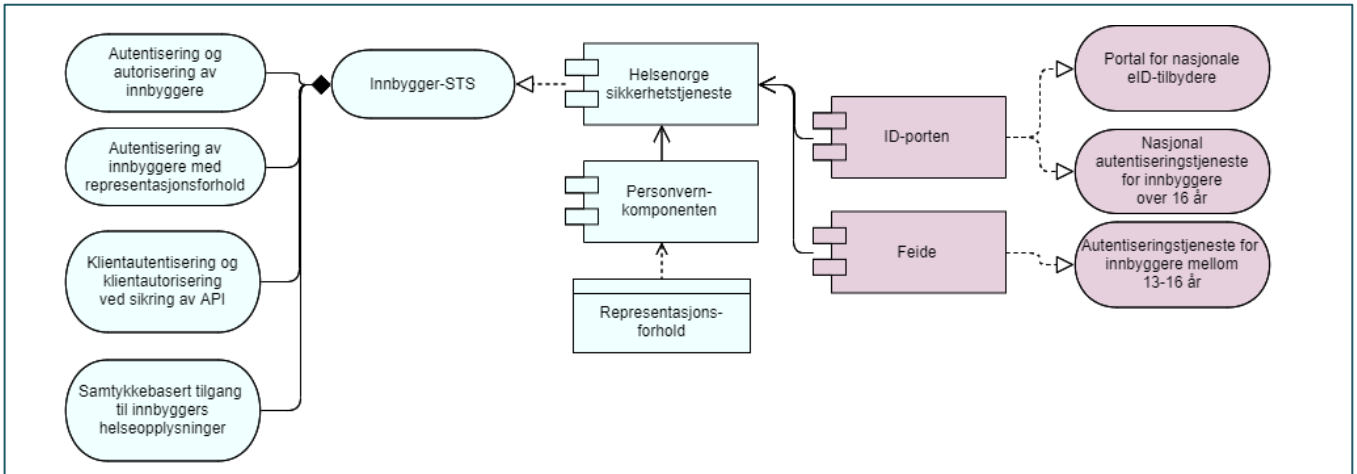
Figur 5 viser de tillitsøkende tjenestene for sikkerhetstjenesten og samspillet med de nasjonale felleskomponentene ID-porten og Feide for autentisering av innbyggere ved datadeling. I tillegg benyttes personvernkomponenten (se kapittel 5.3 for mer detaljer) for representasjonsforhold

For autentisering av innbyggere benyttes eksisterende identitetstilbydere:

- Innbyggere over 16 år: ID-porten
- Innbyggere mellom 13 og 16 år: Feide

Helsenorge sikkerhetstjeneste tilbyr i dag også en autentiseringstjeneste av innbyggere til andre systemer. Tjenesten kan berike sikkerhetsbilletten med informasjon om eventuelle representasjonsforhold. Dette kan være foreldreansvar, fullmakt eller vergemål.

Tjenesten utsteder en sikkerhetsbillett til autentiserte system/applikasjon som innbyggeren benytter. Sikkerhetsbilletten autoriserer hvilke API-er som kan benyttes mot Helsenorge. Tjenesten støtter i dag kun autorisasjon av de API-ene som er tilgjengelig på integrasjonsplattformen.



Figur 5 Helsenorge sikkerhetstjeneste sine felles tillitsøkende tjenester (rød farge = nasjonale felleskomponenter)

I "Plan for utvikling av felles grunnmur" [1] er denne komponenten identifisert som en mulig fellestjeneste for helse- og omsorgstjenesten.

5.2.1 **Tjeneste for** samtykkebasert tilgang til helsesektorens API-er

Helsenorge sikkerhetstjenesten har i dag funksjonalitet for å håndtere samtykke for de tjenester som finnes på Helsenorge. Sikkerhetstjenesten bør utvides til å støtte samtykkebasert tilgang som en tjeneste for hele helsesektoren.
Samtykkebasert tilgang menes her hvor en dataansvarlig for en innbyggerbenyttede applikasjon må innhente samtykke fra innbygger får å få tilgang til innbyggers helseopplysninger via API-er som Helsenorge eller andre e-helseløsninger i sektoren tilbyr. Dette vil si at tjenesten må støtte følgende tillitsøkende tjenester:

1. En felles autentiseringsløsning av innbyggere når innbyggerbenyttede applikasjoner ønsker å få tilgang til API-er i helsesektoren på vegne av innbygger.
2. Felles tjeneste for klientautentisering av innbyggerbenyttede applikasjoner – en sikker autentisering av forhåndsgodkjente innbyggerbenyttede applikasjoner.
3. Felles tjeneste for klientautorisering når innbyggerbenyttede applikasjoner ber om tilgang til et API i sektoren– håndtering av autorisasjoner som en innbyggerbenyttede applikasjoner må ha for å benytte API-er i sektoren, inkludert håndtering av samtykke fra innbygger. For håndtering av samtykke må tjenesten samspille med personvernkomponentens samtykketjeneste.

En slik samtykketjeneste er det også behov for i andre sektorer og gjennom Altinn Autorisasjon er det etablert en slik løsning for offentlige etater som datakilde og API-eiere. Det bør alltid tilstrebes at helsesektoren ikke etablerer egen sektoriell løsning, men benytter en nasjonal løsning. I arbeidet med målarkitekturen ble det vurdert at Altinn Autorisasjon ikke løser alle helsesektorens behov per dags dato, blant annet dekkes ikke private aktører som datakilde. Men dette kan endre seg over tid og det bør derfor vurderes på nytt på et senere tidspunkt.

Det bør også vurderes om det er behov for å etablere en samtykketjeneste for helsepersonell, det vil si at helsepersonell kan be om samtykke fra innbygger om å få tilgang til innbyggers helseopplysninger.

Arkitekturvalg 2

Målarkitekturen legger til grunn at Helsenorge sin sikkerhetstjeneste også skal være en felles tillitstjeneste for innbyggers bruk av datadeling gjennom innbyggerbenyttede applikasjoner og tilby:

2a) autentisere innbyggere, eller en som representerer han/hun, via ID-porten når innbyggerbenyttede applikasjoner ber om tilgang til API-er i helsesektoren.

2b) autentisere og autorisere innbyggerbenyttede applikasjoner som ber om tilgang til å API-er i helsesektoren på vegne av innbygger.

2c) håndtere samtykkebasert tilgang til innbyggers helseopplysninger gjennom å tilby følgende tjenester:

Arkitekturvalg 2

1. Registrere tjenester som krever samtykke samt legge inn beskrivelse av hva innbygger gir samtykke til
2. Innhente samtykke fra innbygger om en innbygger-benyttet applikasjon kan få tilgang til et begrenset sett av helseopplysninger fra et gitt API.
3. Funksjonalitet hvor innbygger kan administrere sine gitte samtykker.

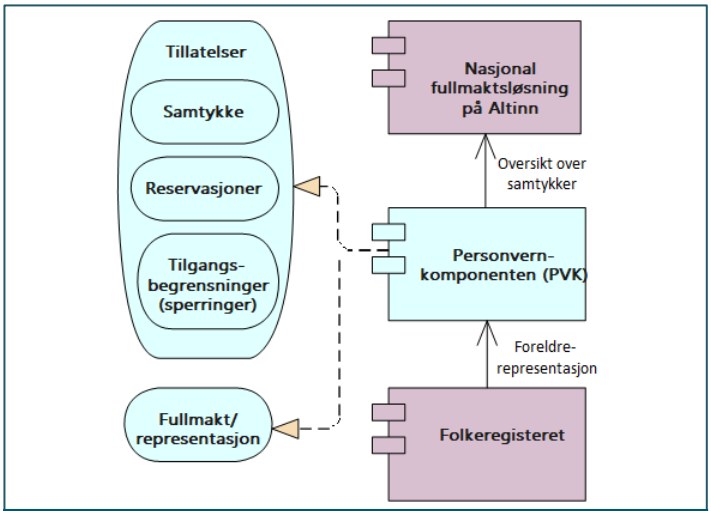
Fellestjenestene benevnes som Innbygger-STS

5.3 Personvernkomponenten

Personvernkomponenten (PVK) er en fellesløsning der en innbyggers innstillinger knyttet til personvern er lagret. Dette er en felleskomponent for sektoren. Med dette menes at det lagres (og kan vedlikeholdes) innbyggers personverninnstillinger som både gjelder på Helsenorge og for andre aktører i sektoren slik som helseregistre, forskningsprosjekter og screeningprogrammer.

Personvernkomponenten inneholder to hovedgrupper av innstillinger:

- Fullmakter: Der en innbygger har gitt en annen person fullmakt til å representere seg innen visse områder eller har fullmakt i henhold til andre forhold (forelder, verge eller ikke samtykkekompetent)
- Personverninnstillinger:
    - Samtykker: Der innbygger har samtykket til at en aktør kan behandle deres helseopplysninger for at aktøren skal ha et gyldig behandlingsgrunnlag. Eksempler på behandling kan være registrering av helsedata, deltager i et forskningsprosjekt, helseundersøkelser m.m. Slike samtykker kan lagres i PVK. Vi har i arbeidet med målarkitekturen ikke funnet behov for å benytte slike samtykker i datadeling og videre vurdering er derfor ikke inkludert i dette kapittelet.
    - Reservasjoner: Der innbygger har reservert seg mot registrering, deltagelse eller spesiell behandling av personopplysninger.
    - Tilgangsbegrensninger(sperringer): Der innbygger har begrenset tilgang eller sperret opplysninger fra innsyn for helsepersonell



Figur 6 Personvernkomponenten (rød farge = nasjonale felleskomponenter)

5.3.1 **Fullmaktstjeneste**

I dag kan en innbygger benytte Helsenorge sine tjenester på andres vegne. Hvem en innbygger kan representere hentes fra fullmaktsløsningen i personvernkomponenten til Helsenorge. Løsningen 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 samt fullmakt på vegne av personer med manglende samtykkekompetanse. 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.

Arkitekturvalg 3

Målarkitekturen legger til grunn at for datadeling skal personvernkomponenten benyttes som kilde for representasjon av innbyggere, og API-eiere i sektoren må stole på informasjon om representasjon i sikkerhetsbilletten fra Helsenorge sikkerhetstjeneste.

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.

5.3.2 **Reservasjonstjene**ste

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

I dag har personvernkomponenten 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. Den er derfor oppført i figur 5.

Arkitekturvalg 4

Målarkitekturen legger til grunn at behov for reservasjoner er knyttet til nasjonale e-helsetjenester som har egne lovhjemler for behandling av helseopplysninger og er allerede støttet i Personvernkomponenten i dag. Det er derfor ikke behov innen datadeling for en felles tjeneste for håndheving av reservasjoner for andre enn de nasjonale e-helsetjenester.

5.3.3 **Sperretjeneste (tjeneste for tilgangsbegrensninger)**

En pasient har rett til å 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. I dag kan man gjennom personvernkomponenten legge inn sperringer på opplysninger i Kjernejournal og resepter på Reseptformidleren.

Ved bruk av datadeling utenfor Kjernejournal og Reseptformidleren 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 i tillegg kunne administrere sperringer samt tilby tjeneste for at de kan håndheves.

I arbeidet med Akson [17] ble det jobbet mer med denne problemstillingen og her anbefales det å etablere funksjonalitet for sperringer i personvernkomponenten. Kort oppsummert anbefales det at:

1. Personvernkomponenten etablerer et toppnivå for sperringer som kun kan sperre tilgang til hele fagsystemer for navngitte personell, grupper av personell og virksomheter for alle fagsystemer underlagt pasientjournalloven.
2. Personvernkomponenten håndterer sperringer av enkeltelementer for nasjonale e-helseløsninger
3. Lokale fagsystemer håndterer selv sperringer av enkeltelementer.

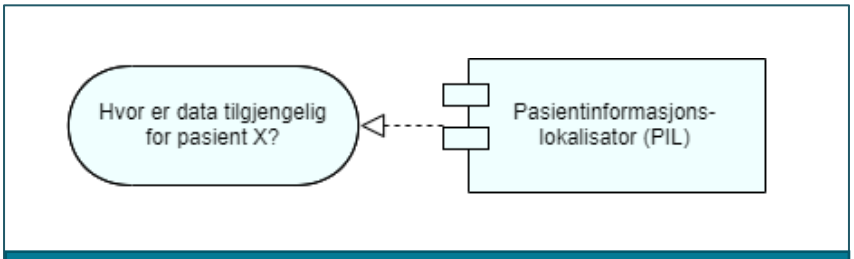
Arkitekturvalg 5

Målarkitekturen legger til grunn arbeidet fra Akson og anbefaler at Personvernkomponenten må tilby tjenester for håndtering av administrasjon av topp-nivå sperringer i tillegg til dagens støtte for sperringer for nasjonale e-helseløsninger.

5.4 Pasientinformasjonslokalisator (PIL)

Det er i en rekke situasjoner tilknyttet datadeling behov for å kunne fremskaffe en oversikt over hvem som har en pasientjournal for en gitt pasient (begrenset til behandlingsrettede helseregistre, ref pasientjournalloven). Det legges til grunn i målarkitekturen at en slik oversikt etableres som en felleskomponent hvor det fremgår hvem som har helseopplysninger om en gitt pasient. Vi har valgt å kalle denne felleskomponenten for pasientinformasjonslokalisator, forkortet til PIL.

Denne komponenten er i liten grad utredet og derfor umoden. Ved en realisering av PIL må behov, konsept og kost/nytte vurderes. Det må også tas stilling til om lagring av slik informasjon krever eget behandlingsgrunnlag i form av en forskrift.



Figur 7 Pasientinformasjonslokalisator (PIL)

Arkitekturvalg 6

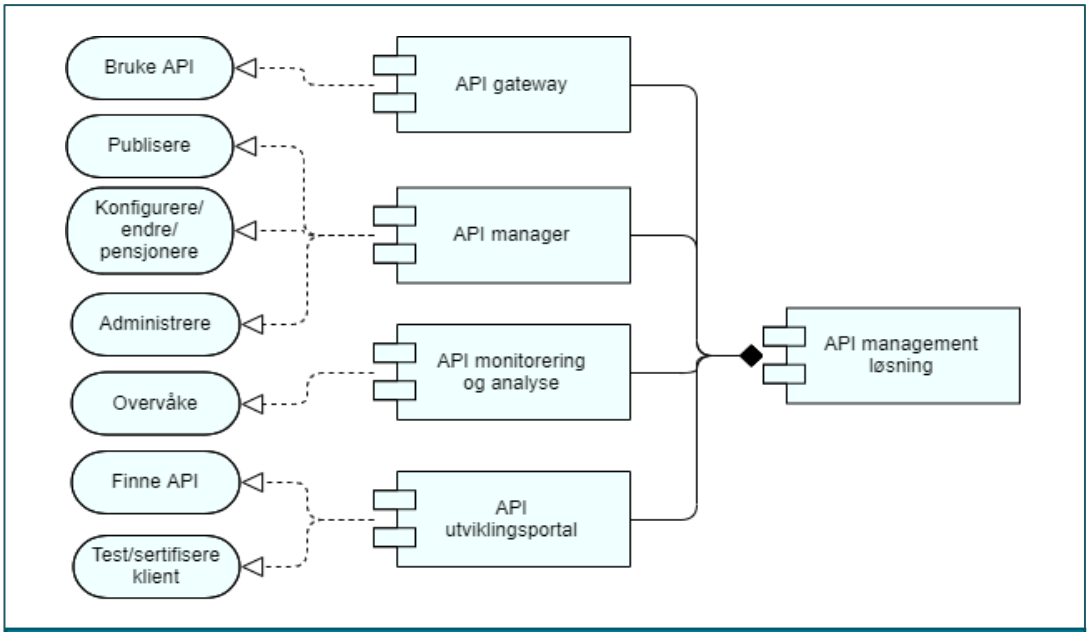
Målarkitekturen legger til grunn at det etableres en pasientinformasjonslokalisator (PIL) som en felleskomponent i grunnmuren hvor alle virksomheter som eksponerer API-er registrerer hvilke pasienter de har data om. Dette gjelder også aktuelle grunnmurskomponenter og nasjonale e-helseløsninger.

5.5 Tjenester for felles API management

Effektiv styring, forvaltning og administrasjon av API-er som benyttes på tvers i helsesektoren krever IKT-støtte, og slik støtte leverer produktleverandører med sine API managementløsninger. Tjenester for API management er en sentral del av målarkitekturen for datadeling i helse- og omsorgstjenesten. Det er i dag ikke etablert noen fellestjenester for API management i sektoren.

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.*".

I "Referansearkitektur for datadeling" [8] er det beskrevet hvilke generiske komponenter som API management består av. Dette er gjengitt i Figur 8 og videre detaljert i Figur 9



Figur 8 Fellestjenester og komponenter for håndtering av API

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

I arbeidet med målarkitekturen ble det diskutert hvordan behov for tjenester for felles API management skal løses. Konklusjonen var at helsesektorens virksomheter vil ha forskjellige behov som gjør det vanskelig å etablere kun én felles løsning for hele sektoren. Derimot bør de nasjonale e-helseløsninger og grunnmurskomponenter etablere tjenester for felles API management som dekker behovene de og deres brukere har, slik at det legges til rette for innovasjon og næringsutvikling av e-helseløsninger som benytter API-er fra nasjonale e-helseløsninger og grunnmurstjenester. Det kan også vurderes behov for at andre virksomheter også kan benytte de samme tjenestene. En mer detaljert vurdering er beskrevet i kapittel 8.3.

Arkitekturvalg 7

Målarkitekturen legger til grunn at:

4a) det må etableres tjenester for felles API-management som tilbyr sektoren tilgang til API-ene til grunnmurskomponenter og nasjonale e-helseløsninger (i produksjon).

4b) det må etableres tjenester for felles API-management som tilbyr leverandørmarkedet tilgang til innbyggerbaserte API-er i sektoren, hos fellestjenester/nasjonale løsninger og til innbyggertjenestene på Helsenorge slik at leverandørmarkedet kan utvikle innbyggerbenyttede applikasjoner som kan hente ut innbyggers helseopplysninger fra disse API-ene.

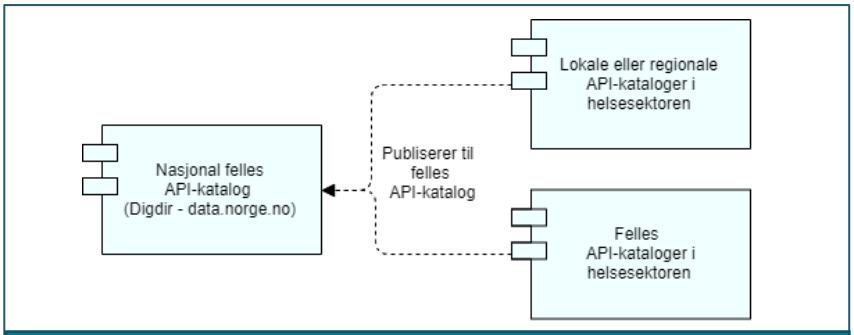
4c) andre virksomheter etablerer sine egne tjenester for API management.

Vi presiserer at API management ikke kun handler om tekniske løsninger, og håndtering av API-er må etableres på organisatorisk nivå før tekniske løsninger realiseres.

5.6 Felles 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 felles 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[19] på felles datakatalogportalen (data.norge.no).



Figur 10 Felles API-katalog

Arkitekturvalg 8

Målarkitekturen legger til grunn en hierarkisk modell for API-kataloger hvor Digdir sin felles katalog for API-er er toppnoden. Alle API-eiere i helse- og omsorgstjenesten publiserer informasjon om sine relevante og åpne API-er i API katalogen til felles datakatalog som forvaltes av DigDir.

5.7 Andre vurderte felleskomponenter

Et nasjonalt loggarkiv for bruk i helse- og omsorgssektoren er blitt vurdert, men vil ikke være hensiktsmessig pga mengden loggmeldinger. Detaljert vurdering kan leses i kapittel 8.5.

Arkitekturvalg 9

Målarkitekturen legger til grunn at det ikke etableres et nasjonalt loggarkiv for datadeling, men det anbefales at alle parter følger felles retningslinjer for logging slik at det er mulig å sammenstille/sammenligne logger på tvers.

5.8 Ikke-vurderte felleskomponenter

Gjennom innspillsrunden har det kommet innspill på andre felleskomponenter som bør være en del av målarkitekturen. Disse er ikke vurdert, men vi har allikevel valgt å gjengi disse her. Dette er:

- **Design– og sanntidsterminologiserver**

  Komponent som kan tilgjengeliggjøre og validere kodeverk (ValueSet) i FHIR. Et ValueSet i FHIR definerer tillate kodeverdier for et kodet informasjonselement i en gitt FHIR-profil, for eksempel at "mann", "kvinne", "ukjent" er tillate verdier i informasjonselementet kjønn. Slike ValueSet må publiseres både for nedlasting i designtime for løsninger som skal implementere ValueSet-ene, men på sikt også i run-time slik at det kan gjøres en direkte validering av om et informasjonssett som utveksles inneholder ulovlige koder (for eksempel "banan" for kjønn). Det er ønskelig at ValueSet kan gjøres tilgjengelig på URL-en som også fungerer som identifikatoren for et ValueSet på nasjonalt nivå. For eksempel at "www.ehelse.no/valueset/kjonn" inneholder både menneskelesbare og maskinlesbare beskrivelser/ definisjoner av ValueSet-et.

- **Repository for FHIR StructureDefinitions**

  Komponent for nasjonale basisprofiler og nasjonale områdeprofiler. Det kan være ønskelig at nasjonale profiler gjøres tilgjengelig for nedlasting, men også sanntidsfunksjonalitet som validering. StructureDefinitions for de lokale grensesnittene vil være tilgjengelig fra lokal FHIR-server, men høyere ordens profiler (basisprofiler/ områdeprofiler) de har arvet bør være tilgjengelig på en URL som resolver slik at konsumerende applikasjoner kan hente disse ned ved behov.

6 Målarkitekturer for bruksområder

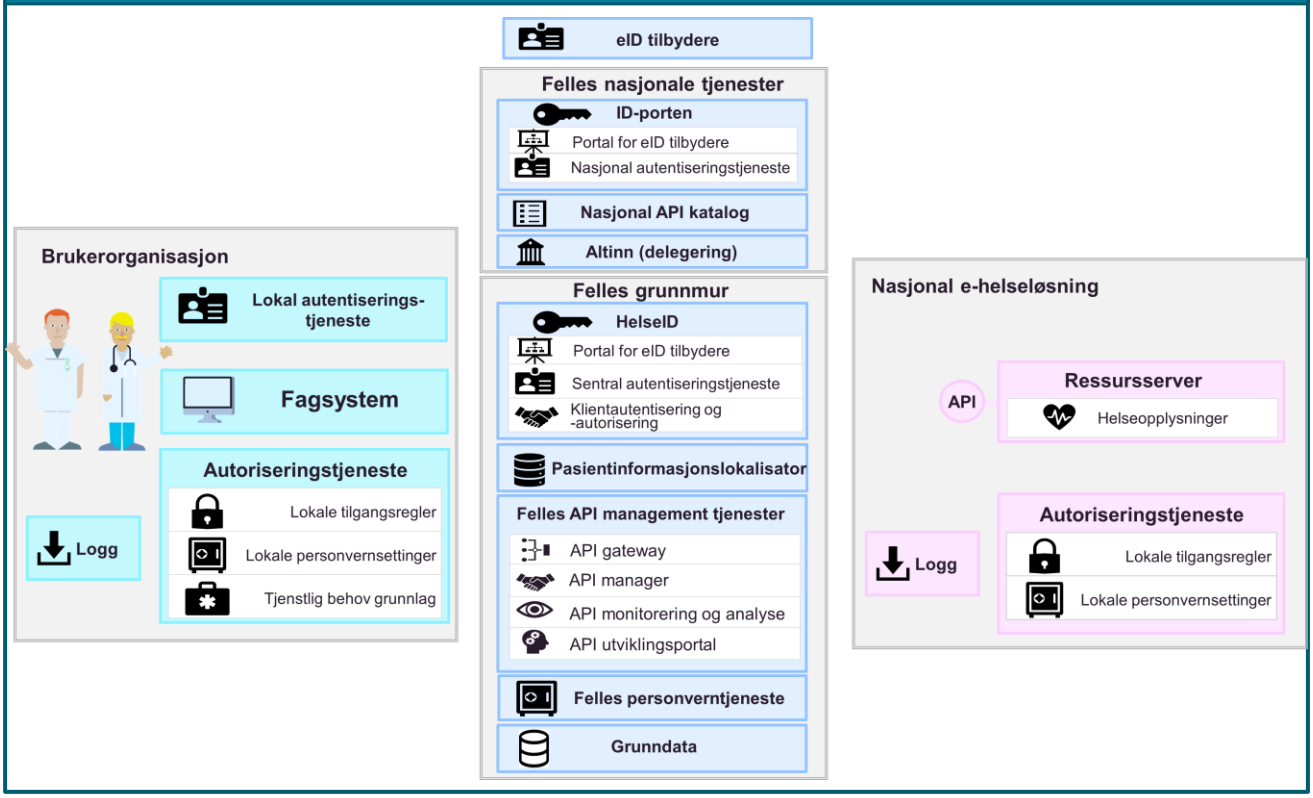
Dette dokumentet dekker målarkitekturer for to bruksområder for samhandling som benytter datadeling som samhandlingsmodell:

1. Sektorens samhandling med grunnmur og nasjonale e-helseløsninger
2. Innbyggers samhandling med helse- og omsorgstjenesten.

6.1 Sektorens samhandling med grunnmur og nasjonale e-helseløsninger

Dette bruksområdet er avgrenset til at brukere er personell med tjenstlig behov for tilgang til helseopplysninger og har behov for å samhandle om opplysninger som er lagret i grunnmurskomponenter og/eller i nasjonale e-helseløsninger.

Figur 11 Målarkitektur for sektorens samhandling med grunnmur og nasjonale e-helseløsninger



viser målarkitektur for datadeling for dette bruksområdet med oversikt over involverte løsninger og felleskomponentene. Vi har beskrevet hvilke roller og ansvar som felleskomponentene har i kapittel 7.2.

6.2 Innbyggers samhandling med helse- og omsorgstjenesten

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

I dag benytter Helsenorge.no datadelingstjenester levert av virksomheter i sektoren samt at Helsenorge.no har egne tjenester som kan tilbys via datadeling. Det bør ikke bare være Helsenorge.no som er forbeholdt å benytte disse tjenestene. Leverandørmarkedet bør også få tilgang til disse datadelingstjenestene slik at det muliggjør utvikling av innbyggerbenyttede applikasjoner som benytter disse tjenestene.

Med innbyggerbenyttede applikasjoner 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. For å muliggjøre slik innovasjon, har leverandørmarkedet behov for en høy grad av selvbetjening for å senke barrierer for å ta i bruk datadeling.

Det legges derfor til grunn i målarkitekturen at leverandørmarkedet 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 via datadeling på vegne av innbyggeren selv. 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 helseregioner og kommuner for å muliggjøre utvikling av innbyggerbenyttede applikasjoner. Dette kan utgjøre en type plattform som muliggjør at 3.parts applikasjonsutviklere kan utvikle, teste og ta i bruk API-er hos aktører i helsesektoren i sine applikasjoner.

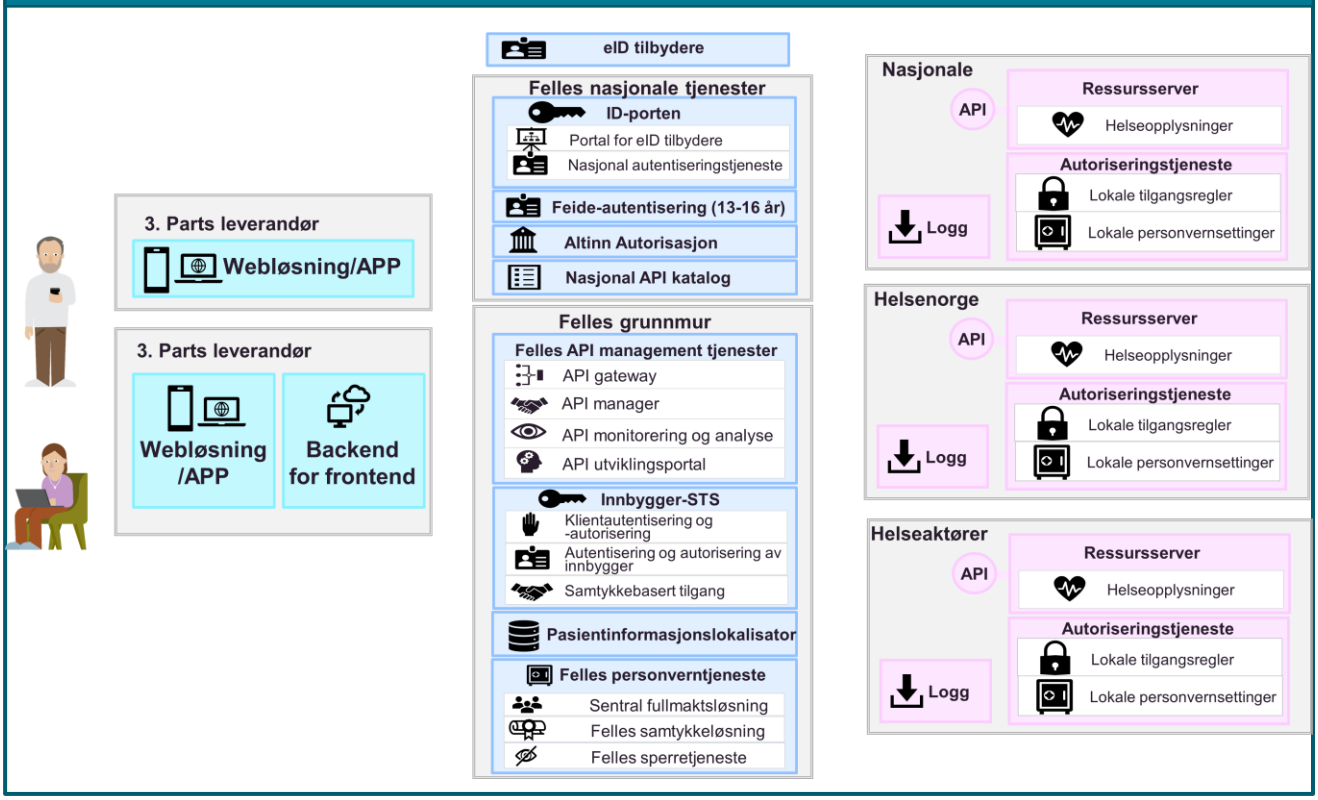
Det er naturlig at Helsenorge kan ha ansvaret for håndtering av en slik plattform på vegne av sektoren, men dette er foreløpig ikke besluttet.

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. Målarkitekturen 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 12 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 12 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 kapittel 7.3.

DEL 2: Kapabiliteter for datadeling

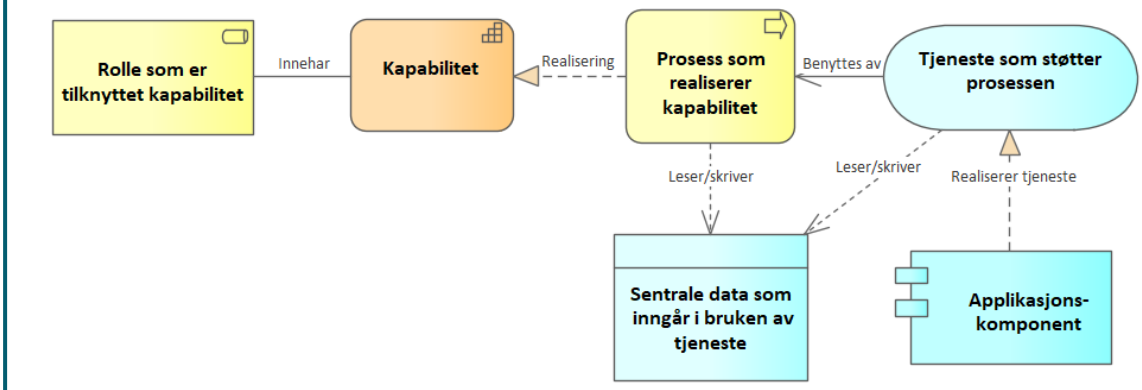
7 Felleskomponenters roller og ansvar

Hva er rollen og ansvaret til en felleskomponent i målarkitekturen? Vi har benyttet en metode fra Digdir til å beskrive dette, vist i Figur 13. Metoden tar utgangspunkt i kapabilitetene som det er behov for ved bruk av datadeling. For hver kapabilitet vises så hvilke prosesser som gjennomføres for å realisere en kapabilitet. For hver prosess vises hvilke applikasjonstjenester, felleskomponenter og sentrale data som blir benyttet.

I kapittel 7.1 er de kapabilitetene som er nødvendig for å realisere samhandling ved bruk av datadeling beskrevet.

I kapittel 7.2 er så kapabilitetene detaljert med hvilke prosesser som det er behov for ved bruk av datadeling for bruksområdet "sektorens samhandling med helse- og omsorgstjenesten". Her er det videre detaljert hvilke applikasjonstjenester som det er behov for og hvilke felleskomponenter som har ansvaret for å tilby disse tjenestene. Kapittel 7.3 beskriver det samme men for bruksområdet "innbyggers samhandling med helse- og omsorgstjenesten".

Figur 13 Metode for å beskrive roller og ansvar felleskomponenter har ved bruk av datadeling

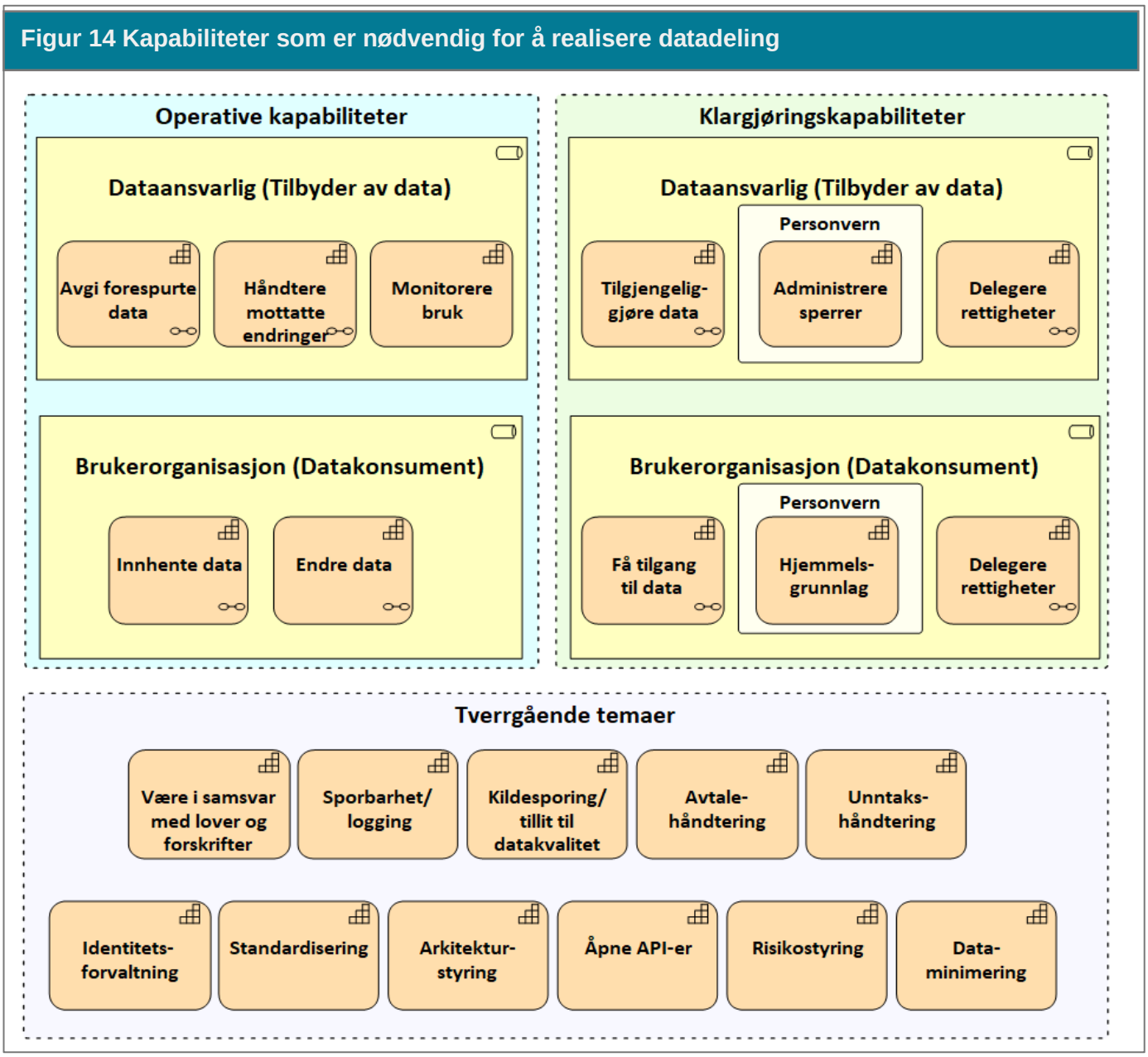


7.1 Nødvendige kapabiliteter for å realisere datadeling

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 [11]. Vi har tatt utgangspunkt i denne modellen og tilpasset temaene behov og begreper som helse- og omsorgstjenesten har. Dette er vist i Figur 14 og hver kapabilitet er beskrevet i Tabell 1. Kapabilitetene benyttes videre i kapittel 7.2 og 7.3 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 14 Kapabiliteter som er nødvendig for å realisere datadeling



Tabell 1 Beskrivelse av kapabilitetene

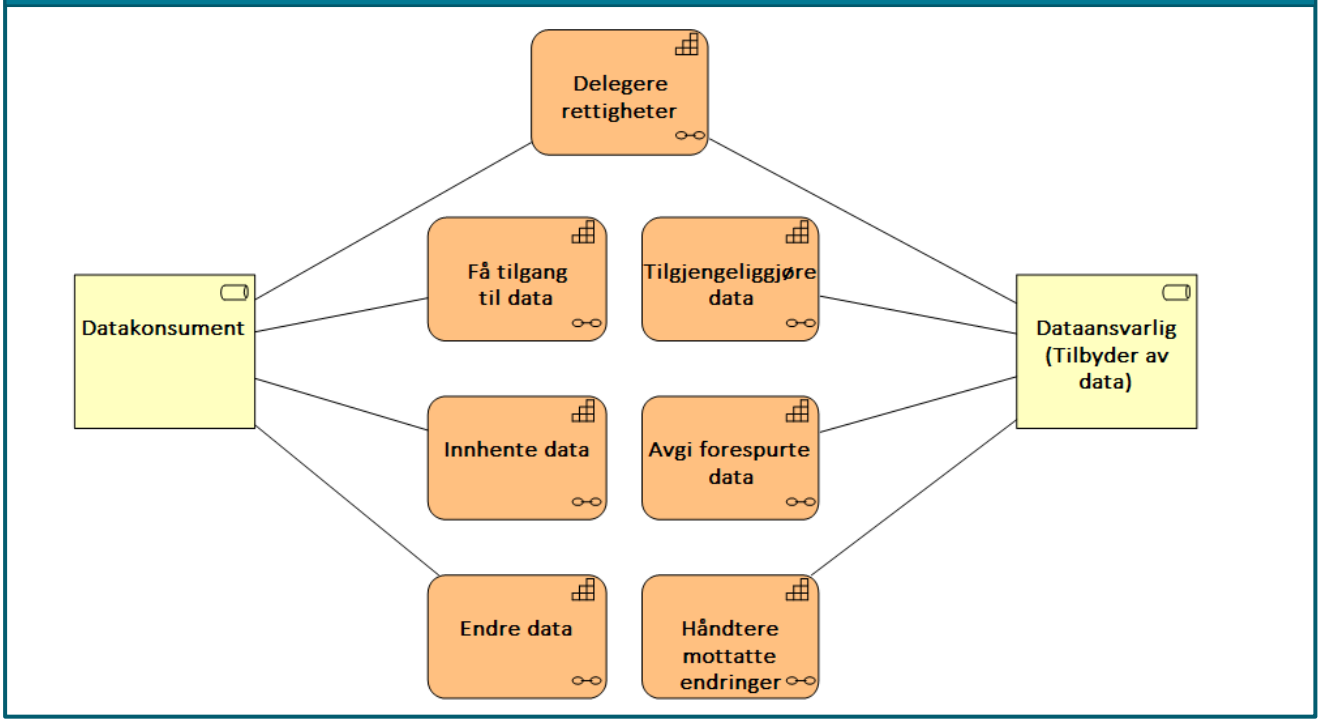
Kapabilitet	Ansvarlig aktør	Beskrivelse
Avgi forespurte data	Dataansvarlig	Evne til å avgi data på forespørsel via datadeling. Kan omfatte tilgangsstyring på brukernivå.

Kapabilitet	Ansvarlig aktør	Beskrivelse
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
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. Tilgangsstyring inngår her.
Administrere sperrer	Dataansvarlig	Evnen til å håndtere mottak og registrering av ønsker fra pasienter som vil motsette seg deling.
Delegere rettigheter	Både dataansvarlig og Brukerorganisasjon	Evnen til å delegere rettigheter til databehandler som utfører oppgaver på vegne av dataansvarlig.
Få tilgang til data	Brukerorganisasjon	Evnen til å skaffe seg tilgang til tilbudte data fra annen aktør ved hjelp av datadeling.
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.
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/ tillit til datakvalitet	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

Kapabilitet	Ansvarlig aktør	Beskrivelse
		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.
Identitetsforvaltning	Tverrgående	Evne til håndtering av opplysninger om hvem en person er.
Standardisering	Tverrgående	Evne til å utarbeide, enes om og ta i bruk 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	Evnen dataansvarlige har som risikoeier til å forstå sitt ansvar og innarbeide håndtering av risiko i sin organisasjon ved deling av helseopplysninger mellom aktører.
Dataminimering	Tverrgående	Evne til å minimere informasjonen som deles ved at kun relevant og nødvendig helseopplysninger deles til andre aktører.

7.2 Sektorens samhandling med grunnmur og nasjonale e-helseløsninger

Figur 15 Hovedkapabiliteter for bruk av datadeling i dette bruksområdet (røde bokser)



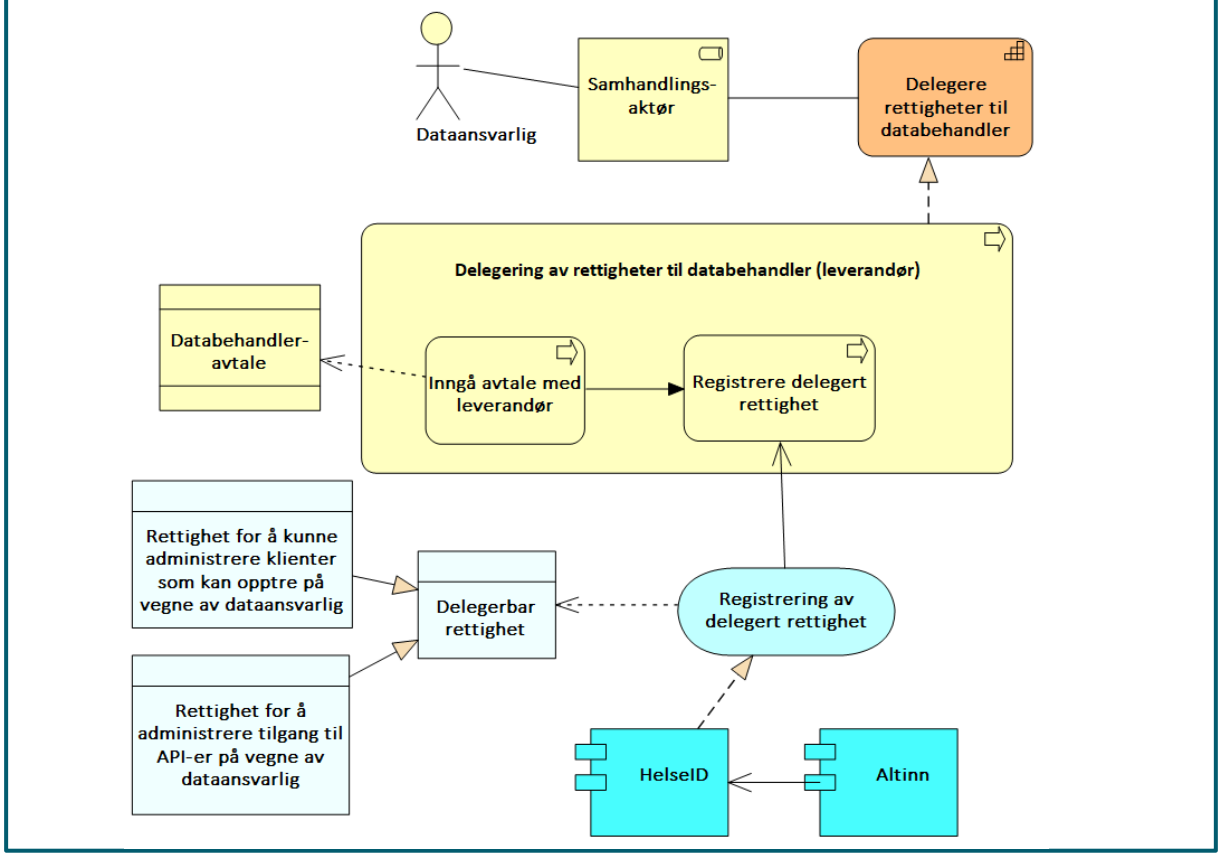
Kapabiliteter for både datakonsument og dataansvarlig som må på plass for målarkitektur for datadeling mellom sektoren og grunnmur og nasjonale e-helseløsninger beskrives under.

7.2.1 Delegere rettigheter

I mange tilfeller vil det ikke være dataansvarlige som er involvert i den operative delen av datadeling. Det delegeres ofte rettigheter til ulike typer leverandører som inngår databehandleravtale med den dataansvarlige. Eksempler på leverandører er IKT-tjenesteleverandør som er databehandler for en dataansvarlig. Dersom databehandleren er involvert i samhandlingen og opptrer på vegne av en dataansvarlig, bør delegeringene være kjent av alle parter i samhandlingen slik at det er klart hvem databehandleren opptrer på vegne av samt har de nødvendige rettighetene til dette i samhandlingen.

Figur 16 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 å kontrollere 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 16 Delegering av rettighet til databehandler (leverandør)



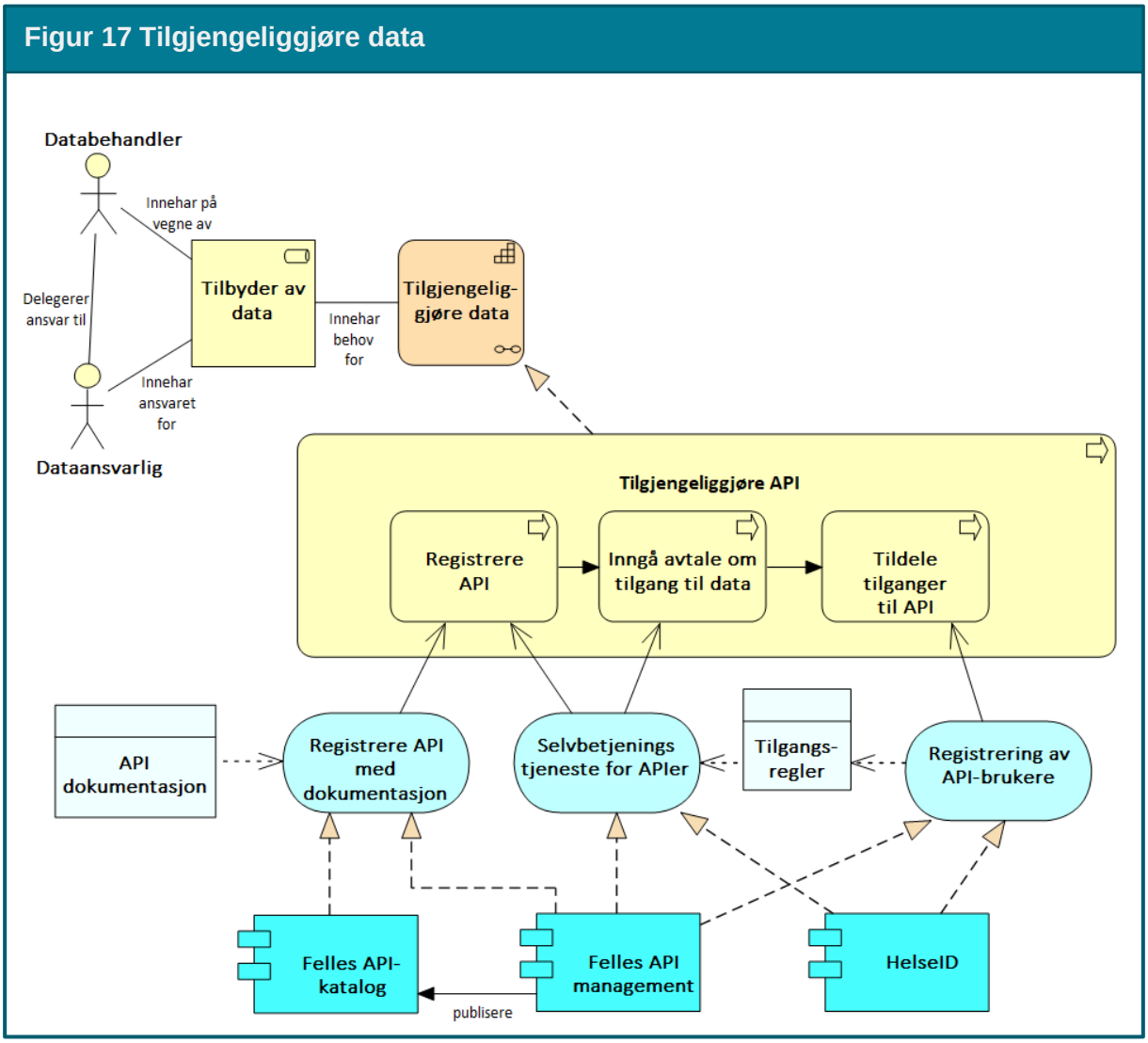
Element	Beskrivelse
Register for rettigheter	Komponent som gir muligheter til å delegere rettigheter til andre organisasjoner eller personer. Rettigheter til bruk av autorisasjonskomponenten må baseres på registrerte roller i Enhetsregisteret. Ikke endelig avklart hvilken løsning som velges. Altinn Autorisasjon 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.

7.2.2 Tilgjengeliggjøre data

Figur 17 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.

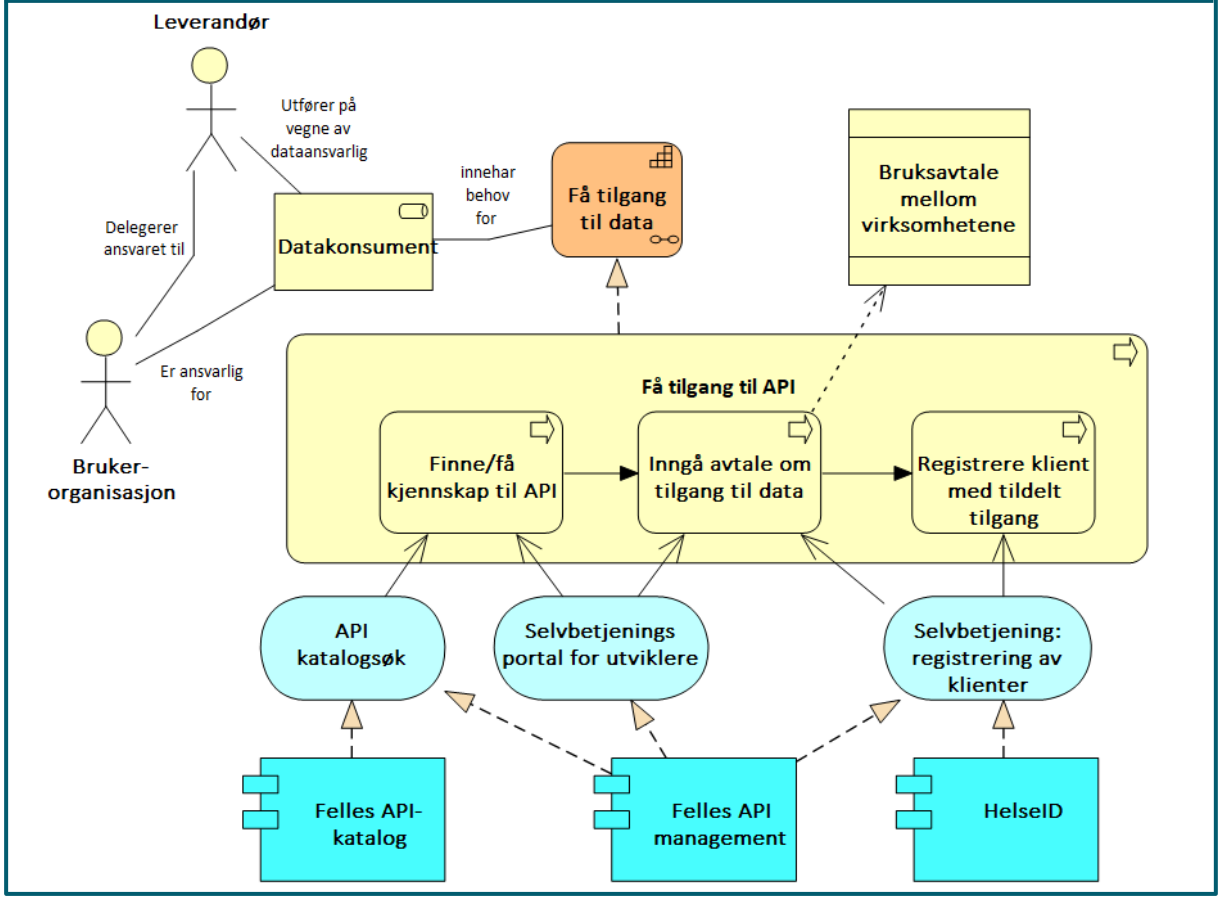
Figur 17 Tilgjengeliggjøre data



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 management 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.
Felles API management	Tjenester for felles håndtering av API-er fra nasjonale e-helseløsninger og grunnmurskomponenter.
API dokumentasjon	Dataobjekt som dokumenterer et API inkludert adresse og operasjoner som tilbys.

7.2.3 Få tilgang til data

Figur 18 Få tilgang til data

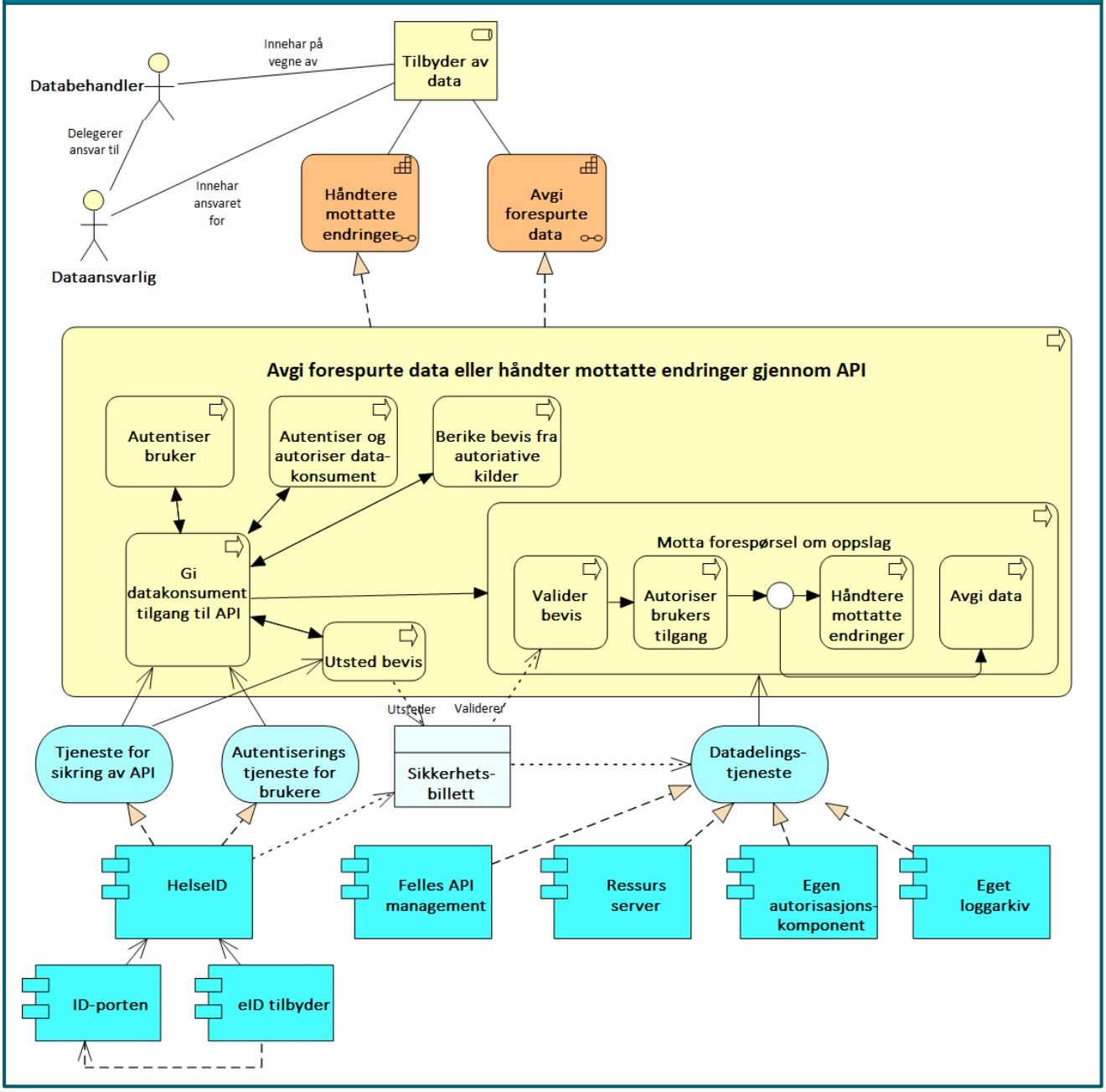


Element	Beskrivelse
Få tilgang til data	Evnen til å skaffe seg tilgang til tilbudte data fra annen aktør.
Datakonsument	Virksomheten som konsumerer data gjennom bruk av API.
Få tilgang til API	Hovedprosessen med å skaffe seg tilgang til tilbudte data fra annen aktør. Omfatter å finne API-er, inngå nødvendige 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	Tjenester for felles håndtering 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.
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.

7.2.4 Avgi forespurte data eller håndter mottatte endringer

Figur 19 Avgi forespurte data eller håndter mottatte endringer



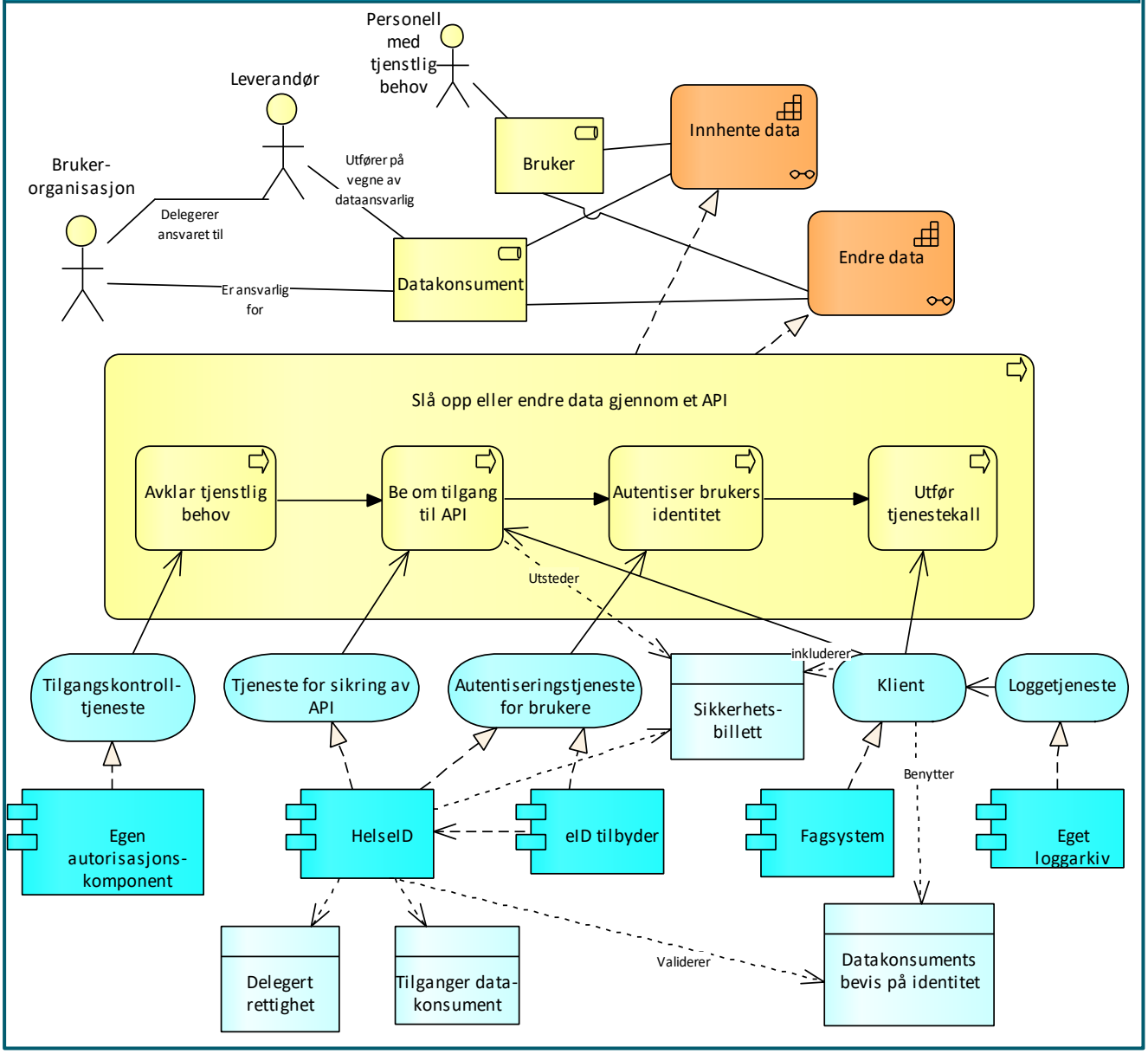
Element	Beskrivelse
Avgi forespurte data	Evne til å avgi data på forespørsel ved hjelp av datadeling.
Håndtere mottatte endringer	Evne til å motta endringer for å opprette, oppdatere eller slette data som er lagret hos den dataansvarlig (NB krever bestemte avtaleforhold)
Tilbyder av data	En aktør som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

Element	Beskrivelse
Felles API management	Tjenester for felles håndtering 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.

7.2.5 Innhente eller endre data gjennom et API

Figur 20 Slå opp eller endre data gjennom et API

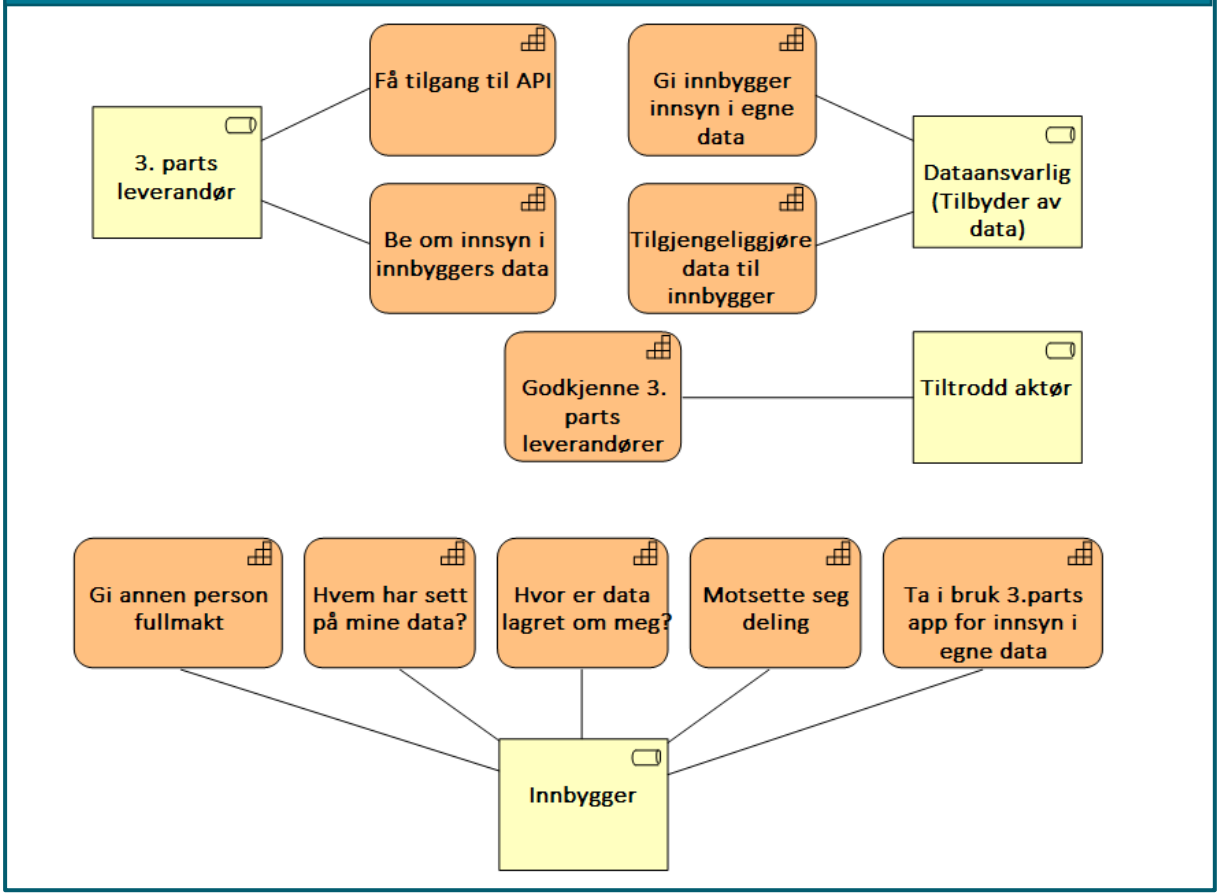


Element	Beskrivelse
Innhente data	Evnen til å innhente data fra en annen aktør via datadeling
Endre data	Evnen til å gjøre endringer hos en annen aktør via datadeling
Datakonsument	Virksomheten som konsumerer data gjennom bruk av API.
Slå opp eller endre data gjennom API	Prosess for en datakonsument 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.
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.

Element	Beskrivelse
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. Kan også være en integrasjonsløsning.
Eget loggarkiv	Datakonsumentens eget system for håndtering og lagring av audit logg. Kan være en del av klienten eller eget selvstendig system.

7.3 Innbyggers samhandling med helse- og omsorgstjenesten

Figur 21 Hovedkapabiliter for Innbyggers bruk av datadeling



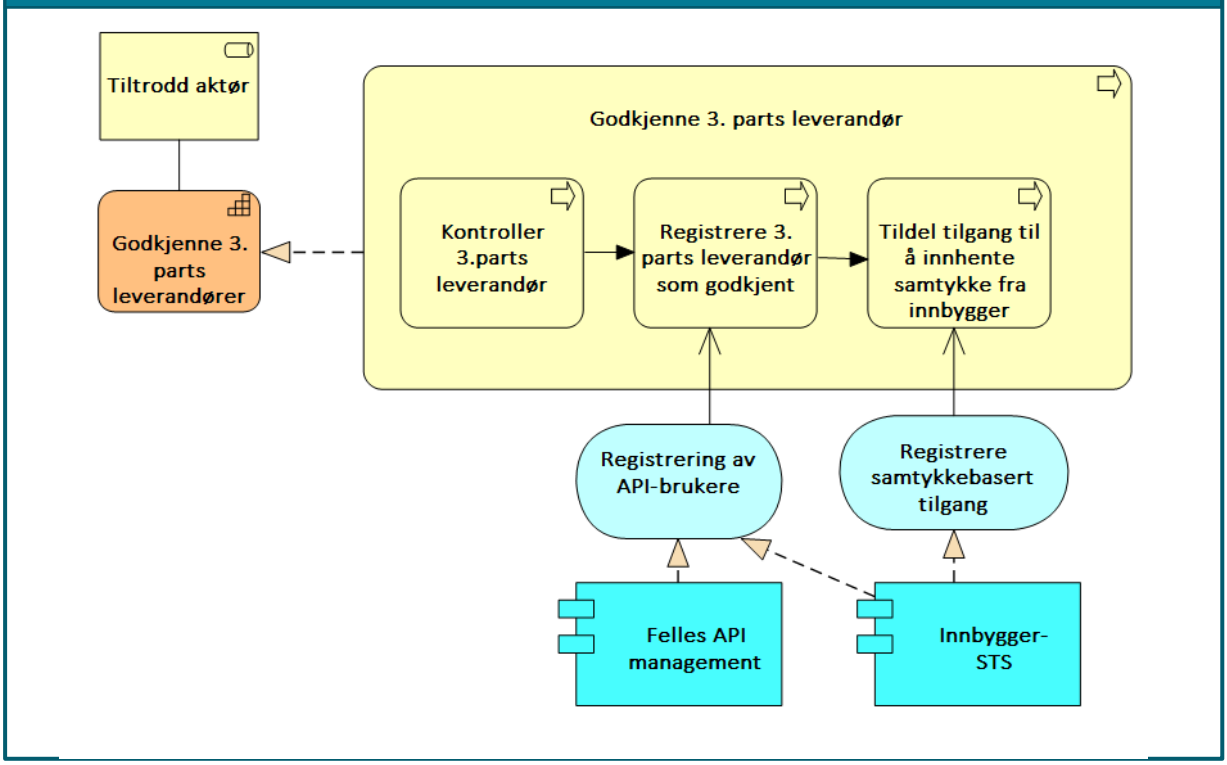
Element	Beskrivelse
3. parts leverandør	Med 3. parts leverandør menes her en leverandør av innbyggertjenester som på vegne av innbygger benytter datadeling for å gi innbygger innsyn i egne data hos en tilbyder av data.
Dataansvarlig (Tilbyder av data)	En virksomhet som behandler helseopplysninger og 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.
Innbygger	Hovedbrukeren av bruksområdet
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.
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. Inkluderer også behandling av innbyggers data (evne til å oppdatere dataene).
Ta i bruk 3. parts app for innsyn i egne data	Evnen til å få innsyn i egne data ved hjelp av en innbyggerbenyttet applikasjon. Inkluderer også behandling av egne data (evne til å oppdatere dataene).
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.

7.3.1 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



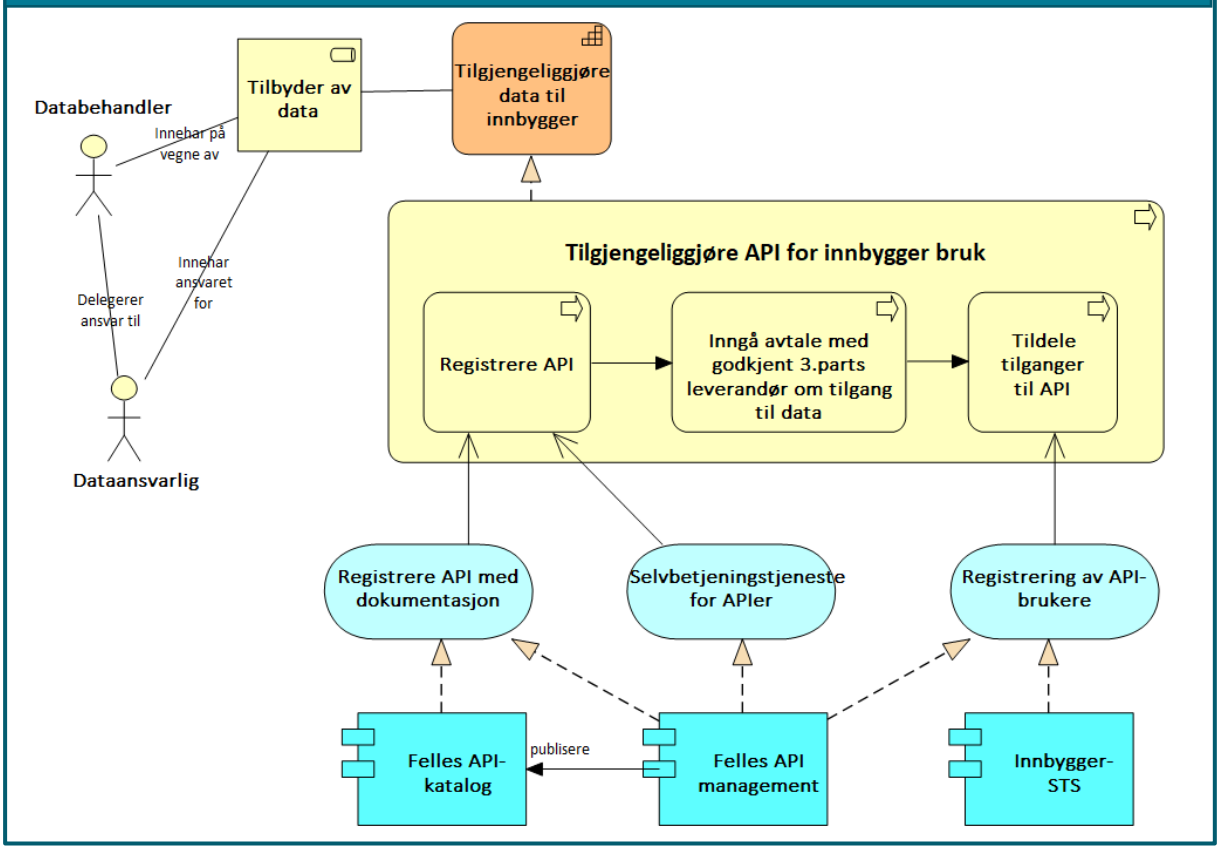
Element	Beskrivelse
Tiltrodd part	En part som de dataansvarlige har tillit til at gjør godkjenning av 3. parts leverandører. Dette kan være et felles bransjeorgan, tillitsanker eller lignende.
Godkjenne 3. parts leverandør	Prosess for å godkjenne og registrere leverandører som kan opptre på vegne av 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.

Element	Beskrivelse
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	Tjenester for felles håndtering 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 innbyggerbenyttede applikasjoner.
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. Komponenten har også ansvar for å innhente samtykke fra innbyggere som benytter applikasjoner fra godkjente 3.parts leverandører.

7.3.2 Tilgjengeliggjøre data

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



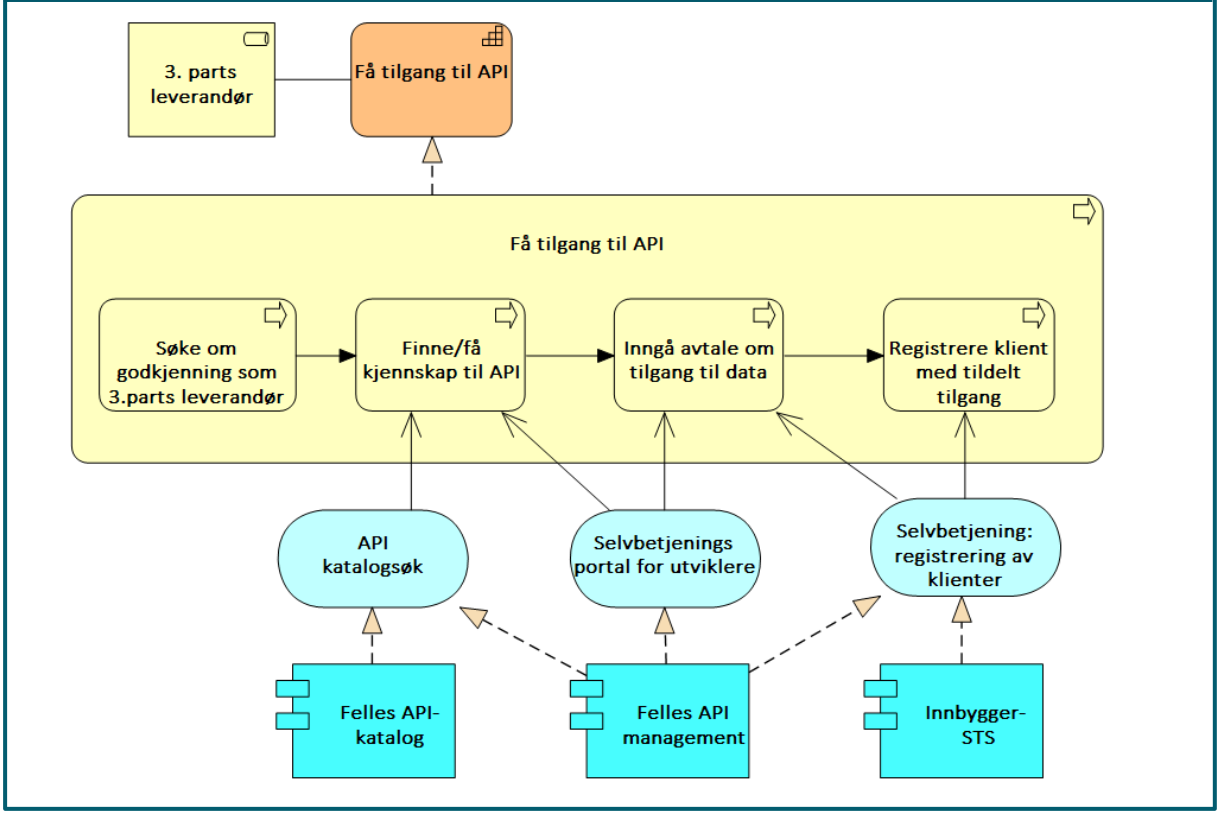
Element	Beskrivelse
Tilgjengeliggjøre data til innbygger	Evne til å tilgjengeliggjøre APIer som gir innbyggere mulighet for å få innsyn i sine helseopplysninger via datadeling.
Tilbyder av data	En dataansvarlig som tilbyr innsyn til innbygger til egne data.
Tilgjengeliggjøre API til innbygger	Prosessen 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.
Registrere API med dokumentasjon	Tjeneste i Felles API-katalogen og i Felles API management for å registrere API og dets dokumentasjon. Bruk av tjenesten forutsetter at rettigheter til å gjøre dette på vegne av tilbyders virksomhet.

Element	Beskrivelse
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.
Felles API management	Tjenester for felles håndtering 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.

7.3.3 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



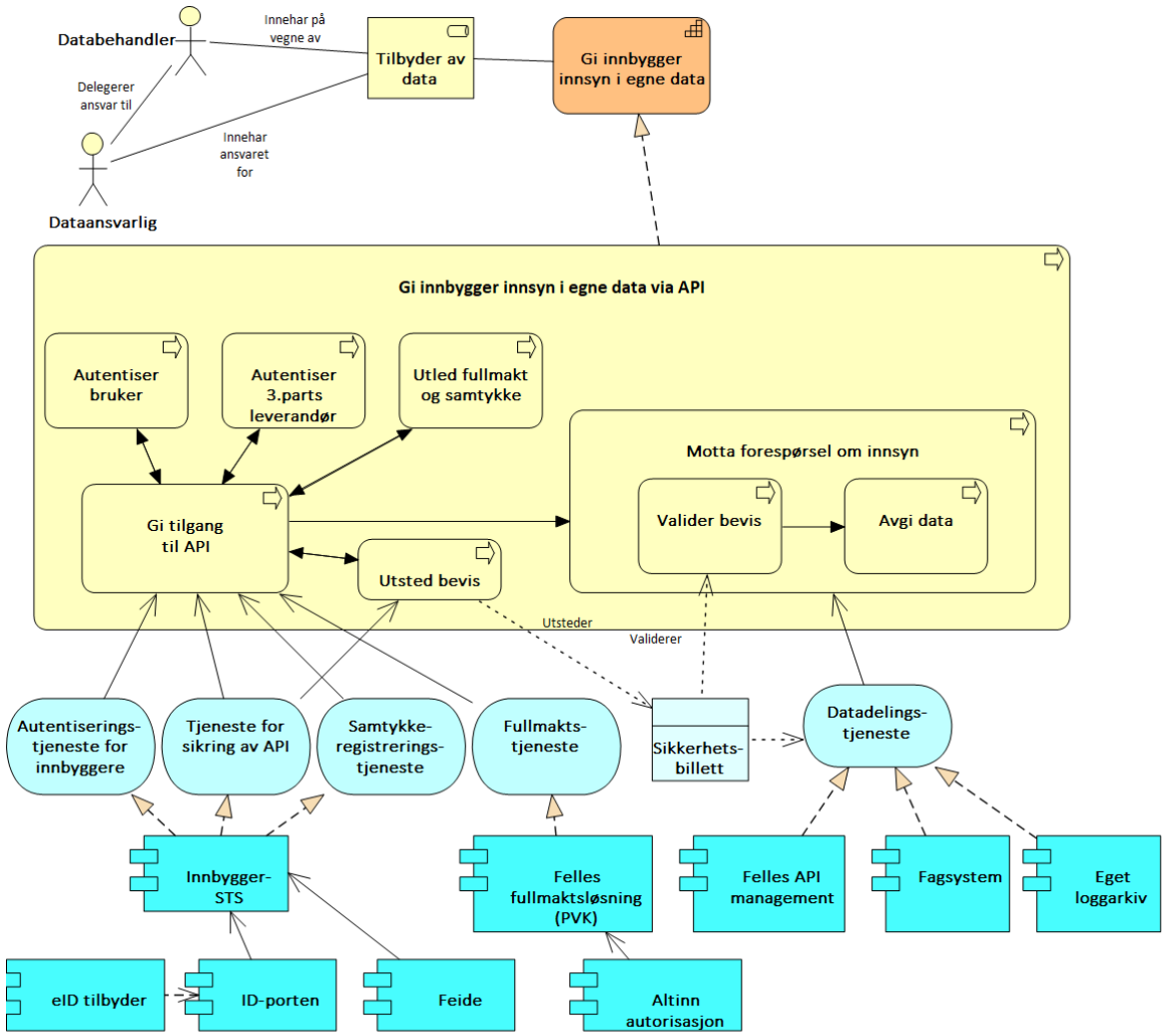
Element	Beskrivelse
Få tilgang til API	Evnen til å få tilgang til å bruke et API på vegne av innbygger.
3. parts leverandør	Med 3. parts leverandør menes her en leverandør av innbyggertjenester som på vegne av innbygger benytter datadeling for å gi innbygger innsyn i egne data hos en tilbyder av data.
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	Tjenester for felles håndtering 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.
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.

7.3.4 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.

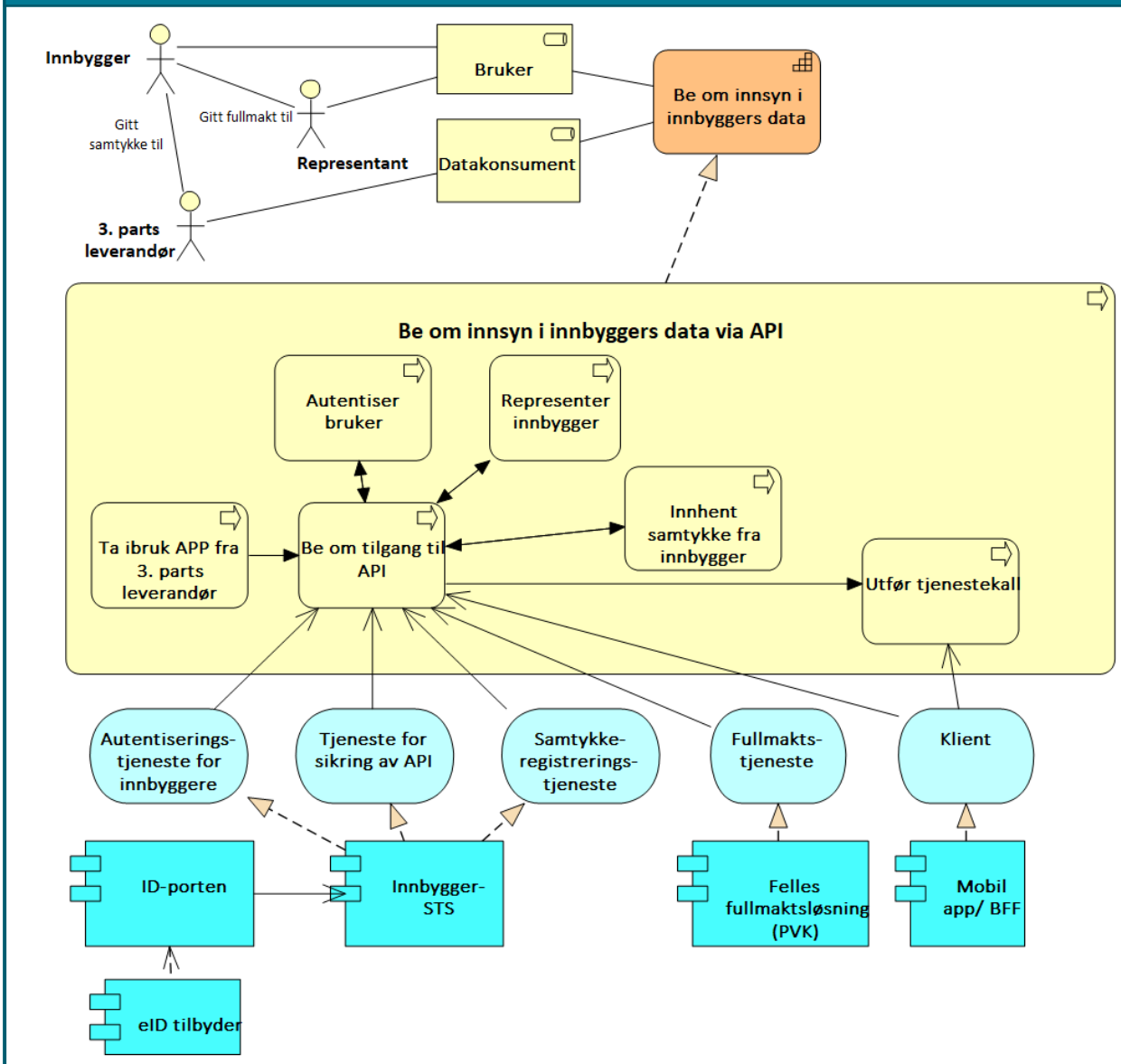
Element	Beskrivelse
Autentiser 3. parts leverandør	Prosess for å sikre at 3. parts leverandør er autentisert og har tilgang til API-et.
Utled fullmakt og samtykke	Prosess for å kontrollere fullmakt dersom innlogget bruker representerer en annen innbygger. Prosess for å kontrollere at innbygger har gitt 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-registreringstjeneste	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.
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.
Feide	Innloggingstjeneste for ungdom (13-16 år)

Element	Beskrivelse
eID tilbyder	Tilbyder av elektroniske identiteter som tilfredsstiller nasjonale sikkerhetsnivåer. BankID, Buypass osv.
Felles API management	Tjenester for felles håndtering av API-er. I denne konteksten vil det være en fellesløsning for håndtering av API-er som dataansvarlige tilbyr leverandører av innbyggerbenyttede applikasjoner.
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 fullmaktsløsning	Felleskomponent for helsesektoren for å håndtere fullmakter og representasjoner basert på fullmakter. En del av personvern-komponenten (PVK).

7.3.5 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 i bruk 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-registreringstjeneste	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 fullmaktsløsning	Felleskomponent for helsesektoren for å håndtere fullmakter og representasjoner basert på fullmakter. En del av personvernkomponenten (PVK).

Element	Beskrivelse
Mobil APP/BFF	Systemet som teknisk sett kaller API-et. BFF (backend for frontend) er serverdelen av en mobil app løsning.

DEL 3: Arkitekturvurderinger

8 Arkitekturvurdering for felleskomponenter

I del 1 ble felleskomponentene i målarkitekturen beskrevet. Dette kapittelet gir en dypere beskrivelse av hvilke vurderinger som er gjort for de enkelte felleskomponentene som har ført frem til valgene som er tatt. I tillegg beskriver dette kapittelet vurderinger av komponenter som det er enighet om at ikke skal etableres som felleskomponenter.

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 tilgjengeliggjøres for brukerorganisasjoner når det finnes et rettslig grunnlag for dette. De rettslige grunnlagene vi dekker i målarkitekturen er:

1. Innbyggers rett til innsyn i egne helseopplysninger, jf. personvernforordningen pasientjournalloven § 18, helsepersonelloven § 41, pasient- og brukerrettighetsloven § 5-1, jf. også personvernforordningen artikkel 15.
2. Tilgjengeliggjøring av opplysninger for personell med tjenstlig behov, jf. pasientjournallovens regler.
3. Samtykkebasert tilgang hvor personell gis tilgang basert på eksplisitt samtykke fra innbygger.

Hvilke felleskomponenter er det behov for ved bruk av datadeling? Dette er et sentralt spørsmål som målarkitekturen svarer ut. Gjennom arbeidet med plan for utvikling av felles grunnmur [1] 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:

1. Felles tillitsøkende tjenester
    a. HelseID
    b. Innbygger STS
    c. Personvernkomponenten
2. Felles API-katalog
3. Tjeneste for felles API management
4. Felleskomponent for lokalisering av pasientinformasjon
5. Felleskomponent for logging

8.1 Vurdering av HelseID og Innbygger-STS

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 de felles tillitsøkende tjenestene HelseID og Innbygger-STS som er beskrevet i kapittel 0).

Følgende behov for felles tjenester hos HelseID og Innbygger-STS er vurdert:

1. En portal hvor godkjente tilbydere av digitale identiteter kan tilby sine digitale identiteter
2. En felles autentiseringsløsning av sluttbrukere 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.

8.1.1 Felles forutsetninger til bruk av felleskomponentene HelseID og Innbygger-STS

Referansearkitektur for datadeling [8][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 HelseID og Innbygger-STS for å bruke dem.
2. I henhold til helsepersonelloven § 45 skal det fremgå av journal at annet helsepersonell er gitt 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 HelseID og Innbygger-STS sikrer at en sluttbruker er innlogget med en elektronisk identitet på et tilstrekkelig avtalt tillitsnivå.
3. Sluttbrukere må kunne velge hvilken eID tilbyder de 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 HelseID eller Innbygger-STSsom et bevis på at sluttbruker er innlogget med riktig sikkerhetsnivå.
5. Alle API-er (eller den de har delegerte ansvaret til) må ha tillit til de sikkerhetsbilletter som er utstedt av HelseID eller Innbygger-STS.
6. Alle klienter av et API må kunne entydig kobles til en registrert klientkonfigurasjon gjennom autentisering av klienten. Klientkonfigurasjonen må kunne kobles til en organisasjon dersom sluttbruker representerer en organisasjon eller en leverandør dersom sluttbruker er en innbygger og klienten er en innbyggerbenyttet applikasjon.
7. Når en sluttbruker representerer en organisasjon, må hjemmelsgrunnlaget som organisasjonen har for å behandle helseopplysninger fra eksterne API-er, være avklart på forhånd. Systemet som organisasjonen benytter, må i forkant være godkjent for slik behandling og være gitt en forhåndstillatelse for å kalle et gitt API. Hjemmelsgrunnlaget 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.

8.1.2 Detaljert beskrivelse av de tillitsøkende tjenestene

8.1.2.1 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").

8.1.2.2 Sentral autentiseringsløsning

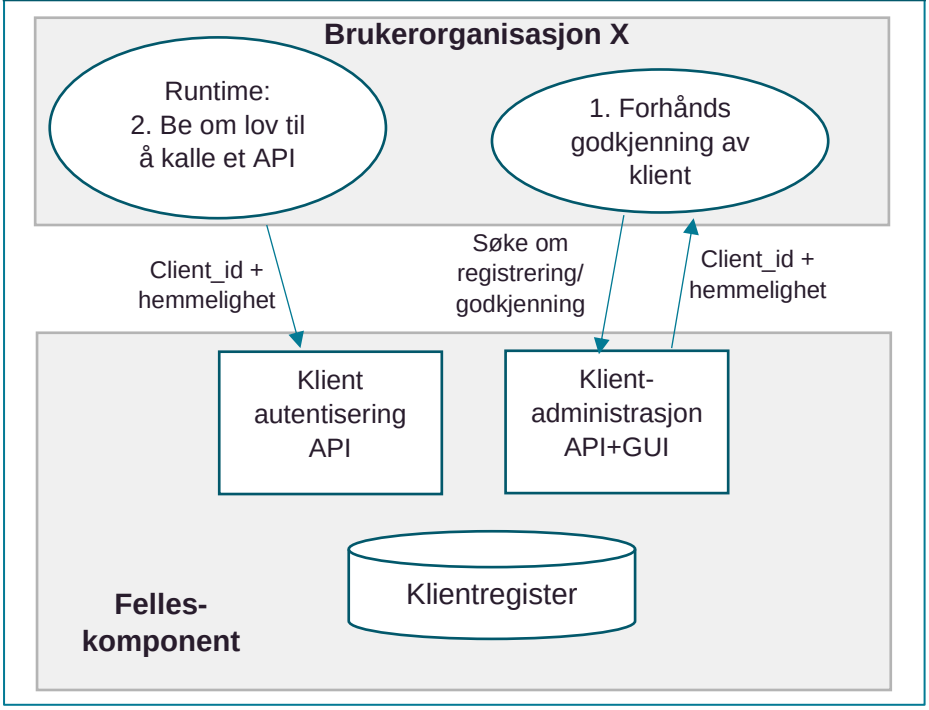
Det er behov for å ha en sentral autentiseringsløsning som fungerer som en tillitstjeneste for hele helse- og omsorgstjenesten og tilrettelegger for single sign-on. Sentral autentiseringsløsning må fungere slik at alle API-eiere må stole på påloginger gjennomført via denne løsningen. Siden det legges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

8.1.2.3 Klientautentisering

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 brukerorganisasjonens system og systemet kobles til brukerorganisasjonen gjennom en klientkonfigurasjon som vedlikeholdes i HelseID. Brukerorganisasjonens system omtales ofte som klienten og kan være et fagsystem eller en integrasjonsløsning. Følgende behov må dekkes av klientautentisering:

- Konsumerende system (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 27 Konseptuell arkitektur for Klientautentisering



Figur 27 viser konseptet bak klientautentisering. En brukerorganisasjon må kunne registrere og få godkjent sine systemer som skal få tilgang til et eksternt API. 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 brukerorganisasjon starte med å søke API-eiere om å ta i bruk deres API-er. Når API-eieren har gitt tillatelse til brukerorganisasjon, kan brukerorganisasjon starte å benytte API-et. Ved kall til API-ene må tillitstjenesten autentisere klienten før klientautoriseringen kan gjøres.

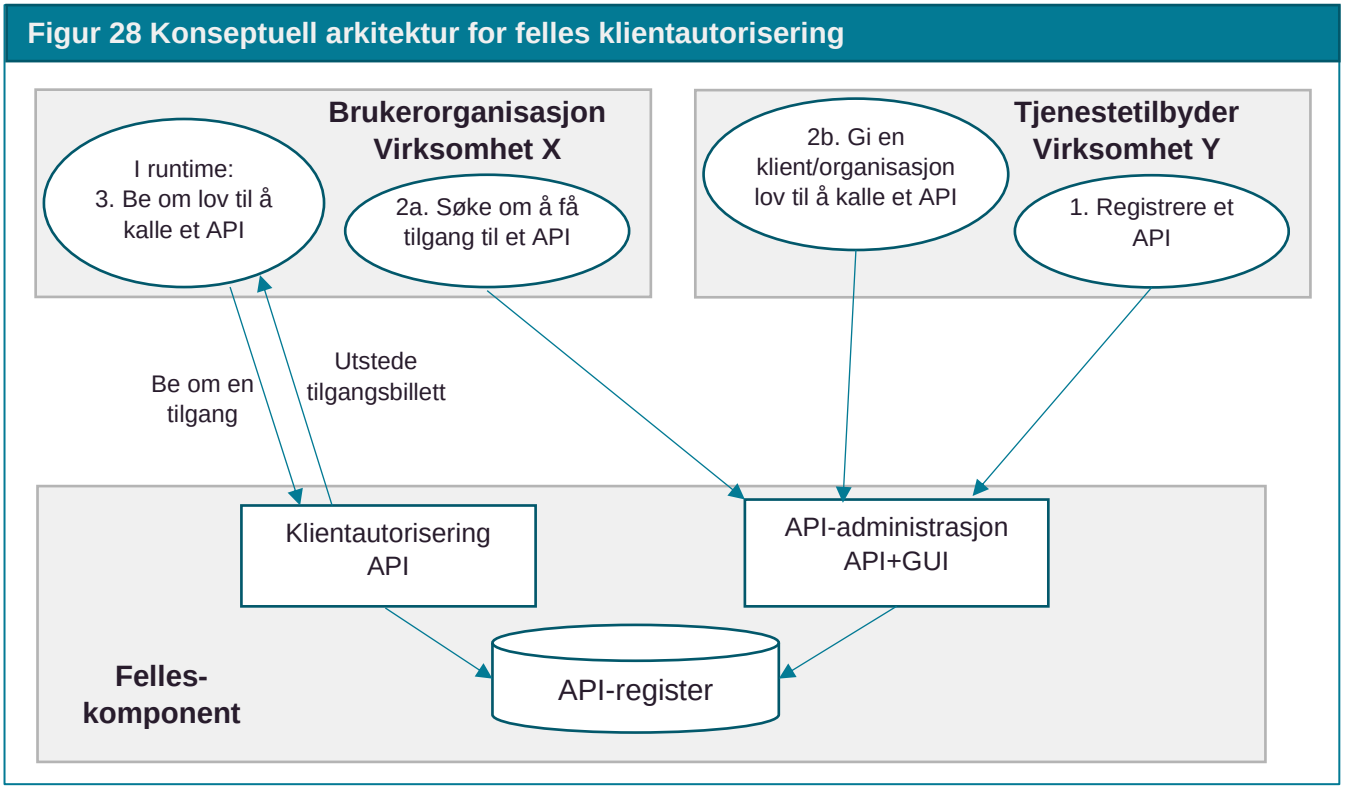
8.1.2.4 Klientautorisering

En API-eier må kun akseptere forespørsler fra brukerorganisasjoner som er forhånds-godkjente 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 HelseID eller Innbygger-STS. 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 eller flere autorisasjoner (scopes) 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 28 Konseptuell arkitektur for felles klientautorisering



Figur 28 viser konseptet bak felles klientautorisering hvor API-eier må først registrere API-et sitt. Deretter må virksomheten som eier klienten søke om å få tilgang til å kalle API-et. API-eier må godkjenne søknaden før klienten kan få tilgang til å kalle API-et.

8.1.3 Oppsummering av vurdering

I Figur 29 er det gjort en overordnet vurdering av hvilke bruksområder som har behov for de ulike tillitstjenestene som HelseID og Innbygger-STS kan levere. 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

Fargekode	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 29 Behovsvurdering av tillitstjenestene for HelseID og Innbygger-STS				
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 autentiserings-løsning for personell/innbygger				
Behov for felles klientautentisering og -autorisering				

8.1.4 Bør HelseID og Innbygger-STS være samme løsning?

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 tilganger som gis til personell basert på 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.

> Målarkitekturen anbefaler å videreføre Innbygger-STS og HelseID som separate løsninger for de respektive brukergruppene.

8.2 Vurdering av personvernkomponenten

Helsenorgeplattformen har etablert en personvernkomponent som dekker tillitstjenestene fullmakt, samtykke, sperringer og reservasjon. I "Plan for utvikling av felles grunnmur" [1] 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.

1. Sentral fullmaktsløsning – for håndtering av fullmakter til de personer en innbygger har gitt adgang til å representere seg.
2. Felles samtykkeløsning – for håndtering av tilfeller der innbygger har samtykket til å være registrert, deltager i et forskningsprosjekt m.m.
3. Felles sperretjeneste – hvor helsepersonell en innbygger ønsker å sperre innsyn for er registrert. (Sperre innsyn = motsette seg deling av sine helseopplysninger)
4. Felles reservasjonsløsning – Reservasjon mot registrering av helseopplysninger. Hvor en innbygger kan reservere seg mot behandling av sine helseopplysninger i en løsning, basert på rettigheter til dette i en lovhjemmel.

Tjenestene er beskrevet i mer detalj i kapittel 5.3

8.2.1 Fullmakt

Behov for håndtering av fullmakter er avgrenset til bruksområdet "Innbyggers deltagelse og innsyn i sin helsehjelp". Det må ved bruk av datadeling for dette bruksområdet legges til rette for at forespørsler fra innbyggerbenyttede applikasjoner 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.

8.2.2 Samtykke

Å få pasientens samtykke er et mulig rettsgrunnlag for å behandle, dele og/eller lagre helseopplysninger. Vi omhandler i målarkitekturen samtykke relatert til deling og en samtykkebasert tilgangstjeneste er beskrevet i kapittel 5.2.

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 der det ikke foreligger et annet rettslig grunnlag 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.

8.2.3 Sperringer

Sperringer er innbyggerinnstillinger hvor innbygger kan motsette seg deling av sine helseopplysninger ved å be om at hele eller deler av journalen sperres for enkeltpersonell, en gruppe av helsepersonell eller virksomheter. I dag må innbyggere kontakte hver enkelt helsevirksomhet som har en journal om å registrere slike sperringer. I tillegg kan en innbygger gjennom Helsenorge sin personverntjeneste legge inn sperringer på opplysninger i Kjernejournal og resepter på Reseptformidleren.

Når en innbygger ønsker å sperre sin journal for navngitte helsepersonell, bør det forutsettes at pasienten ønsker å sperre alle sine journaler for denne personen, ikke bare i virksomheten som pasienten kontakter (slik det er i dag). 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 innbygger. 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. En utfordring med et nasjonalt sperreregister er at sperringer må, i henhold til dagens praksis, nedtegnes i den enkeltes pasientjournal (av helsepersonell) og det nasjonale sperreregisteret kan da bare inneholde ønsker om sperringer. Dette medførte at det i arbeidet med målarkitekturen ble anbefalt at nasjonalt sperreregister som inneholder alle sperringer ikke etableres nå. Det var enighet om at dette måtte konsekvensutredes nærmere før endelig beslutning tas.

I arbeidet med Akson [17] er det blitt jobbet videre med denne problemstillingen og her anbefales det å etableres det en nasjonal personverntjeneste for sperringer. Mer om dette er beskrevet i kapittel 5.3. Målarkitekturen legger denne anbefalingen til grunn i sin arkitektur.

Overstyre 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.

8.2.4 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.

8.2.5 Oppsummering av vurderingen

I Figur 30 er det gjort en overordnet vurdering av hvilke bruksområder som har behov for de ulike personverntjenestene. I denne figuren er det brukt fargekoder for ulike kategorier av behovsvurderingen og de ulike fargekodene er forklart i Tabell 2.

Figur 30 Behovsvurdering av tillitstjenestene i personvernkomponenten				
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 fullmaktsløsning				
Behov for felles samtykkeløsning				
Behov for felles sperretjeneste				
Behov for felles reservasjonsløsning				

8.3 Vurdering API managementløsning

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

Produktleverandører som leverer API management produkter 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.

8.3.1 Tjenester for felles API management

I arbeidet med målarkitekturen har vi diskutert hvordan felles API managementbehov 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 realisering av tjenester for felles API management 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 tjenester for felles API management 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 tjenester for felles API management dersom de ikke ønsker selv å etablere egne tjenester.

Som en konsekvens av denne konklusjonen må komponentene for å realisere tjenester for felles API management både kunne produksjonssettes som en felleskomponent dersom dette er hensiktsmessig eller som distribuerte komponenter. I tjenester for felles API management 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 tjenester for felles API management vil medføre produksjonssetting av mange distribuerte komponenter vil vi omtale tjenestene som en løsning og som en grunnmurskomponent videre i dette dokumentet.

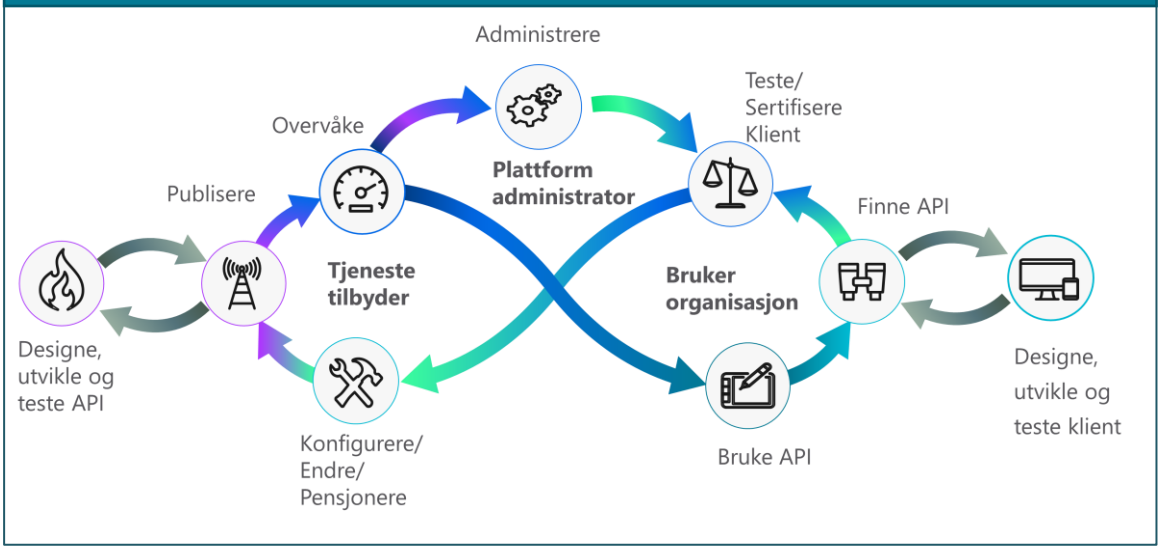
I diskusjonene kom det også innspill på at anskaffelsen av et felles managementprodukt bør gi mulighet for at andre virksomheter bør kunne avrope fra samme avtale for å etablere sin egen API managementløsning. Svaret på dette innspillet er knyttet til realisering av tjenester for felles API management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

8.3.2 Prosesstøtte i felles API management

Tjenester for felles API management 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 anses ikke en del av tjenestene for felles API management.

Figur 31 viser en oversikt over rollene og funksjonalitet som de ulike rollene har behov for på overordnet nivå.

Figur 31 Prosess for bruk av tjenester for felles API management



8.3.3 Bruksområdene for datadeling sine behov for tjenester for felles API management

Alle bruksområdene definert i kapittel 4 kan ha behov for API-management. Men ikke alle har behov for sektorfelles tjenester for API management. Vurderingen er vist i Figur 32 Bruksområdene sine behov for tjenester for felles API management.

Figur 32 Bruksområdene sine behov for tjenester for felles API management		
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 tjenester for felles API management • 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 tjenester for felles API management • Kan gjenbruke samme produkt for å dekke egne behov • Enkelte delkomponenter er det allikevel behov for å ha felles slik som API-katalog

8.4 Vurdering av Pasientinformasjonslokalisator

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 oversikt over hvem som har en pasientjournal for en gitt pasient. For innbygger er det fire sentrale problemstillinger som gir et behov for å vite hvilke systemer som har en pasientjournal for en gitt pasient:

Problemstilling	Behovsbeskrivelse	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 det fremgår hvem som har helseopplysninger om en gitt pasient. 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. Det må vurderes om løsningen skal baseres seg på en sentralisert modell hvor system og pasient kobles i registeret eller en mer desentralisert modell hvor pasienten i det sentrale registeret pasient kobles til hvilke virksomheter som har pasientjournal for den gitte pasienten og virksomhetene må tilby egen tjeneste for å koble system og pasient.

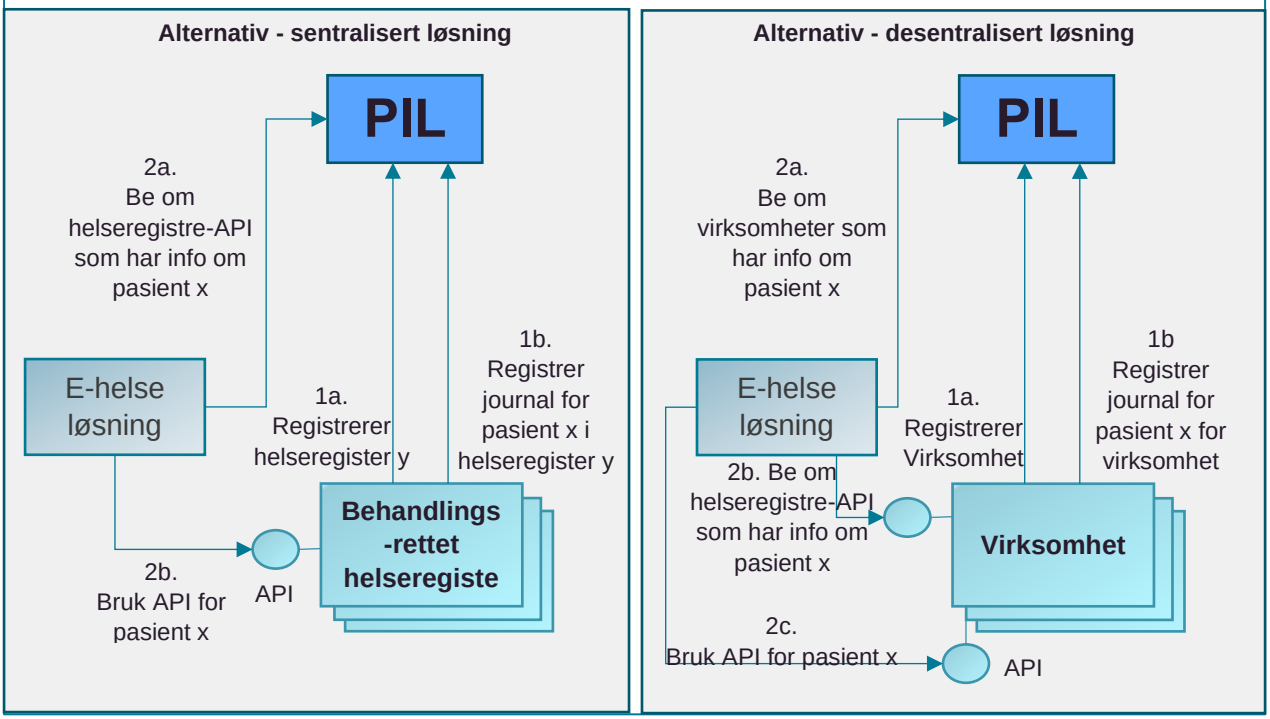
En lignende komponent for helseregisteret er tidligere prøvd etablert, kalt Oppføringsregisteret. Dette registeret hadde som formål å kunne gi oversikt over hvilke

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 33 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 33 Konseptuell skisse over PIL



8.5 Vurdering av 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 som har hvilket 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 omsorgssektoren 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.

9 Veien videre

9.1 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 hvilken konsekvens innføring av målarkitekturen har for helsehjelpen, og hvordan realiseringen skal gjennomføres.

9.2 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. Flere av bruksområdene beskrevet i kapittel 4 trenger somt nevnt tidligere 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 av innbyggerbenyttede applikasjoner ha en databehandleravtale med API-eier som er dataansvarlig?
    c. Godkjenning av 3.parts leverandører. Det er i kapittel 7.3.1 beskrevet en prosess for å godkjenne 3.parts leverandører av innbyggerbenyttede applikasjoner som skal kalle API-er som deler helseopplysninger. Hva består en slik godkjenning av?
    d. Skal innbyggerbenyttede applikasjoner 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 pågående 2020/2021.
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 "Veileder for åpne API-er" [15] er det beskrevet anbefalinger om at testing av bruk av API-er bør være mulig uten at leverandøren er involvert.

10 Referanser

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

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

[3] "Rammeverk for digital samhandling", Digitaliseringsdirektoratet, (https://www.digdir.no/nasjonal-arkitektur/rammeverk-digital-samhandling/2148)

[4] Normeringsnivå og dokumenttyper, Direktoratet for e-helse, https://ehelse.no/standarder/om-standardisering-i-e-helse/normeringsniva-og-dokumenttyper

[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 (Direktoratet for e-helse, HITR 1215:2018 12/2018), https://ehelse.no/standarder/ikke-standarder/referansearkitektur-for-datadeling

[9] Retningslinjer for logging ved data- og dokumentdeling (Direktoratet for e-helse, 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 (Direktoratet for e-helse, HITR 1223:2019) https://ehelse.no/standarder/ikke-standarder/anbefaling-av-tillitsmodell-for-data-og-dokumentdeling .

[11] Generisk referansearkitektur for Datautveksling (per høst 2019 under arbeid), DigDir med flere, https://nasjonal-arkitektur.github.io/architecture-repository/data-exchange-ra/book-data-exchange-ra.html

[12] Anbefaling om bruk av SMART on FHIR – (Direktoratet for e-helse, HITR 1225:2019) https://ehelse.no/standarder/ikke-standarder/anbefaling-om-bruk-av-smart-on-fhir

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

[14] Krav til sikkerhetsbillett ved deling av helseopplysninger – (Direktoratet for e-helse, HITS 1220:2019) https://ehelse.no/standarder/ikke-standarder/krav-til-sikkerhetsbillett-ved-deling-av-helseopplysninger

[15] Veileder for åpne API i helse- og omsorgsektoren (Direktoratet for e-helse, HITR 1229:2020) https://ehelse.no/standarder/ikke-standarder/veiledning-for-%C3%A5pne-api-i-helse-og-omsorgssektoren

[16] Samhandlingsarkitekturer i helse- og omsorgssektoren (Direktoratet for e-helse, HITR 1212:2018) https://ehelse.no/standarder/ikke-standarder/samhandlingsarkitekturer-i-helse-og-omsorgssektoren

[17] Sentralt styringsdokument Akson: Helhetlig samhandling og felles kommunal journalløsning, Bilag G2 Helhetlig samhandling (Direktoratet for e-helse, IE-1056) https://ehelse.no/publikasjoner/sentralt-styringsdokument-akson-helhetlig-samhandling-og-felles-kommunal-journallosning

[18] Standardiserte tjenestegrensesnitt (API) for helseregistre (Direktoratet for e-helse, IE-1025:2018) https://ehelse.no/publikasjoner/standardiserte-tjenestegrensenitt-api-for-helseregistre

[19] Felles offentlig API katalog https://data.norge.no/dataservices

[20] Målarkitektur for dokumentdeling (Direktoratet for e-helse, HITR 1222:2019) https://ehelse.no/standarder/ikke-standarder/malarkitektur-for-dokumentdeling

[21] Handlingsplan for regjeringens digitaliseringsstrategi (KS, Skate og Digitaliseringsdirektoratet, 2020) https://www.digdir.no/digitalisering-og-samordning/handlingsplan-regjeringens-digitaliseringsstrategi/1229

[22] Veileder om bruk av NS-EN 17269 Health informatics - The International Patient Summary (Direktoratet for e-helse, HITR 1240:2020) https://ehelse.no/standarder/veileder-om-bruk-av-ns-en-17269-health-informatics-the-international-patient-summary

Vedlegg A Juridiske rammer

Tilgjengeliggjøring av opplysninger via datadeling innebærer behandling av personopplysninger, herunder helseopplysninger. Enhver behandling av personopplysninger skal ha en eller flere dataansvarlige. For å behandle personopplysninger må den dataansvarlige ha et behandlingsgrunnlag. For å tilgjengeliggjøre pasientopplysninger for andre enn de som har nedtegnet disse, må det foreligge et unntak fra helsepersonells taushetsplikt.

I dette vedlegget gjengis hovedpunkter i det juridiske rammeverket.

A.1 Behandlingsgrunnlag

For å behandle personopplysninger må det foreligge et behandlingsgrunnlag etter personvernforordningen artikkel 6. Behandling av helseopplysninger krever i tillegg at et av vilkårene i personvernforordningen artikkel 9 nr. 2 er oppfylt. Behandling av helseopplysninger for å yte helsehjelp skal i tillegg ha hjemmel i norsk lov, jf. pasientjournalloven § 6. Aktuelle behandlingsgrunnlag for behandlingsrettede helseregistre er personvernforordningen artikkel 6 nr. 1 bokstav d (nødvendig for å verne den registrertes vitale interesser) og artikkel 9 nr. 2 bokstav h (nødvendig i forbindelse med yting av helsetjenester).

Etter pasientjournalloven § 6 kan *"helseopplysninger i behandlingsrettede helseregistre bare behandles når det er nødvendig for å kunne gi helsehjelp, eller for administrasjon, internkontroll eller kvalitetssikring av helsehjelpen."* Virksomheter som yter helsehjelp skal ha et behandlingsrettet helseregister for at helsepersonell kan gjennomføre dokumentasjonsplikten etter helsepersonelloven § 39, jf. pasientjournalloven § 8. Helsepersonelloven § 40 setter rammene for hva en pasientjournal kan og skal inneholde.

A.2 Dataansvar

Ansvaret for behandlingen av opplysningene ligger til en **dataansvarlig**. Dataansvarlig er den eller de som bestemmer formålet og midlene med behandlingen av personopplysningene. Virksomheten der helsehjelpen ytes, er som oftest dataansvarlig. Når en dataansvarlig velger å overlate hele/deler av behandlingen av personopplysningene til en annen virksomhet, vil denne være en databehandler, jf. nedenfor.

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. Den enkelte virksomhet er dataansvarlig for all behandling av opplysninger som skjer i sine respektive registre og systemer. Der tilgjengeliggjøring av opplysninger skjer ved utlevering, vil dataansvaret overføres. 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.

Dersom virksomheten som er dataansvarlig benytter en **databehandler**, kan denne gis tilgang/behandle opplysninger i tråd med hva den dataansvarlige bestemmer i databehandleravtale, jf. personvernforordningen artikkel 28. 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 dataansvarlige og databehandleren skal i alle tilfeller sørge for tilfredsstillende informasjonssikkerhet, jf. pasientjournalloven § 22 og personvernforordningen artikkel 32.

A.3 Tilgjengeliggjøring av pasientopplysninger

Taushetsplikt er det klare utgangspunkt for all behandling av helseopplysninger. Pasientjournalloven § 15 pålegger enhver som behandler helseopplysninger etter pasientjournalloven taushetsplikt etter de generelle taushetspliktreglene i helsepersonelloven §§ 21 flg.

Relevante og nødvendige helseopplysninger skal likevel være tilgjengelig for den som yter, administrerer eller kvalitetssikrer helsehjelp, uavhengig av hvor pasienten har fått behandling tidligere. Pasientjournalloven § 19 pålegger derfor den dataansvarlige en plikt til, innenfor rammen av taushetsplikten, å sørge for tilgjengeliggjøring av opplysninger når dette er nødvendig for å yte helsehjelp. Den som får tilgang til opplysningene må ha behandlingsgrunnlag for behandlingen, jf. A1 over.

Det fremgår av pasientjournalloven § 19, første ledd at:

" [..] dataansvarlige [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".

Dette korresponderer med helsepersonelloven § 45 som 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".*

Også helsepersonelloven § 25 åpner for at opplysninger kan gjøres tilgjengelig uten hensyn til taushetsplikt:

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

Dataansvarlig bestemmer på hvilken måte opplysningene skal tilgjengeliggjøres, jf. pasientjournalloven § 19 annet ledd, og dermed hvorvidt dette skal gjøres via datadeling.

Dataansvarlig har også ansvar for at opplysningene tilgjengeliggjøres på en slik måte at informasjonssikkerheten ivaretas. Kravene til informasjonssikkerhet følger av pasientjournalloven § 22. Vilkårene er de samme for intern og ekstern informasjonsdeling, men hvordan opplysningene skal deles internt i de enkelte virksomhetene og mellom virksomheter kan slå ulikt ut i en risikovurdering. I forarbeider til helsepersonelloven § 45 og pasientjournalloven § 19 er det lagt til grunn at det kan gjøres en forhåndsvurdering av vilkårene i helsepersonelloven § 45, og at det kan etableres tekniske løsninger slik at helsepersonell selv kan tilegne seg opplysninger basert på forsvarlig tilgangskontroll. Dette innebærer blant annet at enhver dataansvarlig må sørge for at sikkerheten i egen virksomhet ivaretas. Videre innebærer det at dataansvarlig må vurdere risikoen ved deling av

opplysninger med eksterne og ha iverksatt nødvendige tiltak for å begrense risikoen slik at den er akseptabel for dataansvarlig.

Hvilke tiltak dataansvarlig må gjøre for at kravene for tilgjengeliggjøring etter helsepersonelloven §§ 25, 45 og pasientjournalloven § 19 er oppfylt, er en konkret vurdering. Tiltakene skal ivareta opplysningenes integritet, tilgjengelighet og konfidensialitet. Dette innebærer blant annet at dataansvarlig og databehandler skal sørge for god og treffsikker tilgangsstyring, tilfredsstillende krav til autentisering, autorisasjon, logging og etterfølgende kontroll.

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 at opplysningene tilgjengeliggjøres og konsekvensene av dette, jf. pasientjournalloven § 17. Etter pasient- og brukerrettighetsloven § 5-3 kan opplysningene heller ikke tilgjengeliggjøres dersom det er grunn til å tro at pasienten vil motsette seg dette. Et unntak fra pasienters adgangen til å motsette seg tilgjengeliggjøring av opplysninger er når «tungtveiende grunner» taler for at opplysningene allikevel skal deles etter pasient- og brukerrettighetsloven § 5-3.

Tilgjengeliggjøring av opplysninger kan også være særregulert. Etter helsepersonelloven § 23 nr. 6 er taushetsplikten ikke til hinder for "*at opplysningene gis videre etter regler fastsatt i lov eller i medhold av lov når det er uttrykkelig fastsatt eller klart forutsatt at taushetsplikt ikke skal gjelde"*.

Tilgjengeliggjøring av opplysninger fra behandlingsrettede helseregistre til andre formål enn helsehjelp, må skje etter samtykke eller hjemmel i lov, jf. pasientjournalloven § 20.

A.4 Innbyggers innsynsrett

Innbygger har en lovfestet rett til innsyn i opplysninger som er registrert om seg i behandlingsrettede helseregistre. Dette følger av pasientjournalloven § 18 og pasient- og brukerrettighetsloven § 5-1, jf. også personvernforordningen artikkel 15.

Retten til innsyn i pasientjournal følger også direkte av helsepersonelloven § 41.

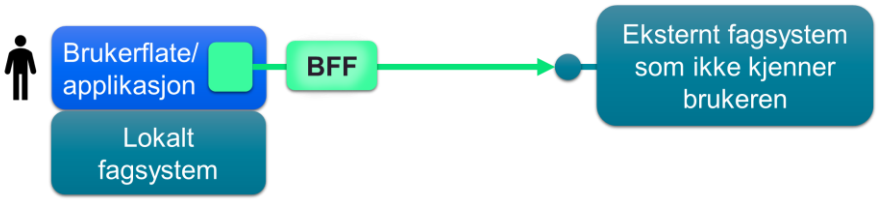
Vedlegg B Integrasjonsmønstre for datadeling

B.1 Standard integrasjonsmønster

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 34: 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 B.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 34. Vi har valgt å kalle oppskriften for et integrasjonsmønster for datadeling. 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.

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.

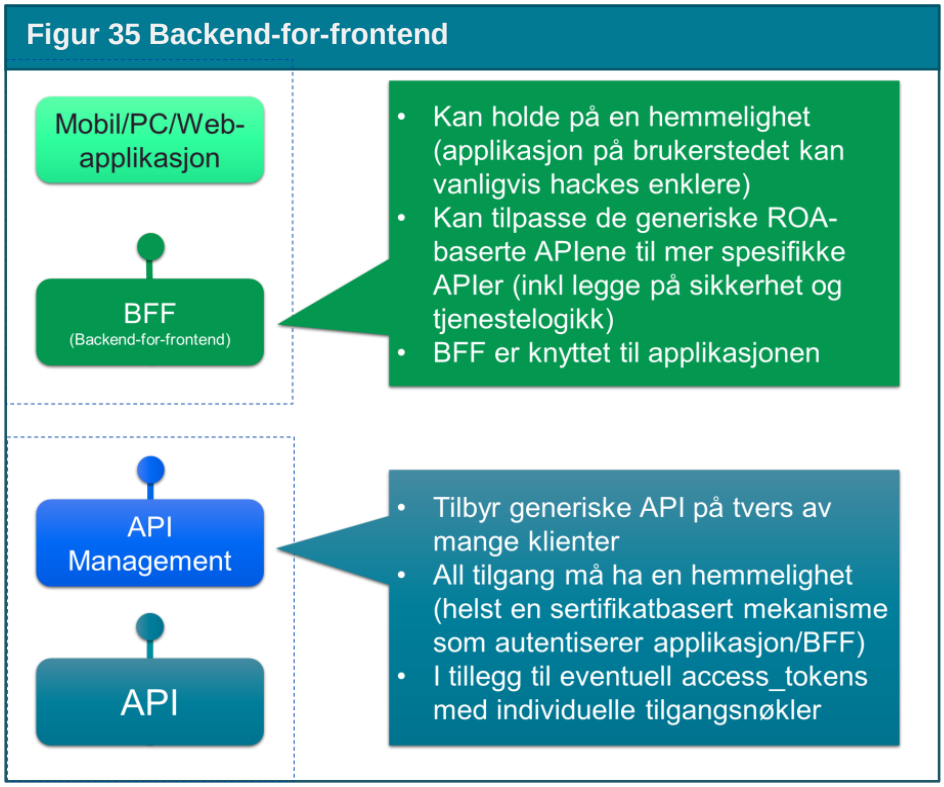
Ved bruk av API-er som eies av andre virksomheter settes det krav til at klientene MÅ støtte sikker lagring og behandling av hemmeligheter for å sikre konfidensialitet og integritet ved overføring av sensitive personopplysninger mellom klientene og API-et.

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 35 Backend-for-frontend



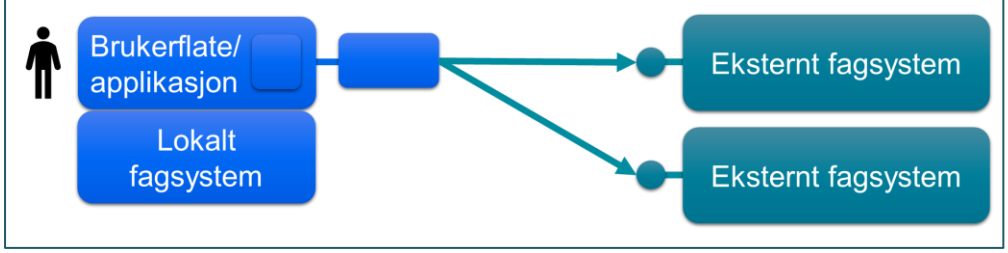
B.2 Integrasjonsmønstre for brukerapplikasjoner

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 målbildet, 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 36. Men dette har flere utfordringer:

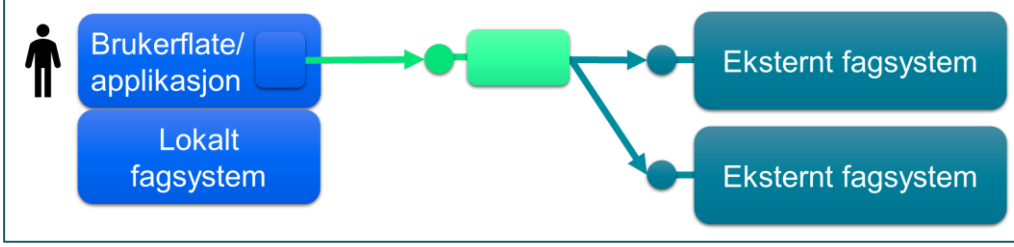
1. Hvert enkelt system må realisere samme funksjonalitet samt påkrevd støtte for sikkerhet og personvern for bruk av andres API-er. Hvert av API-ene kan i tillegg ha ulike autentiseringsmekanismer osv.
2. Systemleverandører har begrenset kapasitet og det kan ta lang tid før alle samhandlende systemer 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 å yte helsehjelp. Det kan da være behov for å innføre klientsertifiseringsordninger.

Figur 36 Dagens modell:
EPJ leverandører utvikler klienter mot eksterne systemer



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

Figur 37 En API managmenttjeneste oversetter



Se Figur 37. Her vil EPJ-leverandører kunne implementere klienten selv, men jobben vil være enklere fordi API-ene er likere og følger samme arkitektur, autentisering etc.

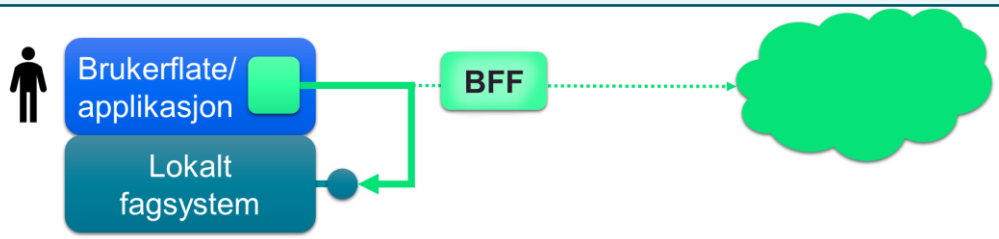
Et annet alternativ er at EPJ-leverandører tillater andre aktører å utvikle funksjonalitet tett integrert med deres systemer. Vi skal se på to alternative integrasjonsmønstre for datadeling som åpner opp for en raskere og kostnadseffektiv bredding og ibruktagelse av funksjonalitet for samhandling mellom helsepersonell og mellom innbyggere og helsepersonell. Mønstrene er vist i Figur 38.

Den første har vi valgt å kalle "*A1 - nedlastbar webapp*" og er basert på standarden "SMART on FHIR" [12]. Dette mønsteret 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.

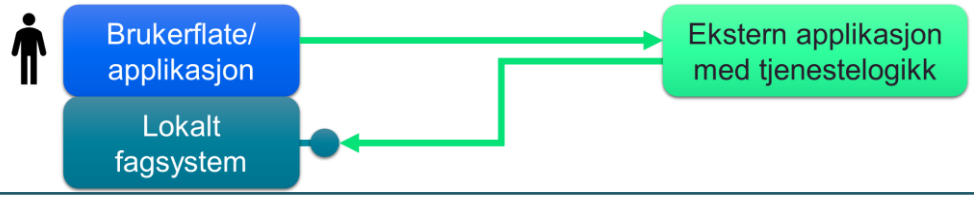
Det andre mønsteret har vi kalt "*A2 - ekstern applikasjon med forretningslogikk gis tilgang til lokalt system*" og er basert på standarden "CDS Hooks". Dette mønsteret gjør det mulig for virksomheter å benytte felles ekstern funksjonalitet, men med å benytte lokale data. Den eksterne applikasjonen kjøres 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.

Figur 38 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.



B.3 Integrasjonsmønster 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..

Figur 39 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.

Vedlegg C 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