Direktoratet for e-helse

Referansearkitektur for datadeling

HITR 1215:2018

Publikasjonens tittel:
Referansearkitektur for datadeling

Versjon:
1.0

Rapportnummer:
HITR 1215:2018

Utgitt:
12/2018

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Innledning

Dette dokumentet utgjør en av flere referansearkitekturer innen elektronisk samhandling i helse- og omsorgstjenesten. Samhandlingsarkitekturene er beskrevet i følgende fire dokumenter:

- *Samhandlingsarkitekturer i helsesektoren* [15]
- *Referansearkitektur for meldings- og dokumentutveksling* [18]
- *Referansearkitektur for dokumentdeling* [17]
- *Referansearkitektur for datadeling (dette dokumentet)*

Dokumentene er basert på arbeid utført i første halvdel 2017 og beskriver i hovedsak situasjonen slik den var på dette tidspunktet. Det pågår også arkitekturutvikling på flere av områdene, og det kan komme endringer i eller tillegg til referansearkitekturene.

Dette dokumentet beskriver nasjonal referansearkitektur for datadeling innen helse- og omsorgstjenesten.

Med datadeling menes i dette dokumentet deling av strukturerte data mellom helseaktører gjennom felles ressurser eller tjenester i sanntid. Med helseaktører menes det både innbyggere og virksomheter innen helse- og omsorgstjenesten inkludert offentlige etater.

Samhandling gjennom datadeling tilrettelegger for at innbyggere og helseaktører kan ha en mer dynamisk informasjonsdeling med andre helseaktører. Slik informasjonsdeling kan enten være at en aktør etterspør eller oppdaterer informasjon hos en annen aktør. Dette gjør at flere aktører kan samarbeide om felles ressurser som er lagret kun ett sted, i motsetning til meldingsutveksling hvor samme data lagres hos alle avsendere og mottakere av en melding.

Dagens behov for datadeling nasjonalt er spesielt drevet av behov knyttet til:

- Mer effektiv deling og oppdatering av helse- og personopplysninger mellom helsepersonell
- Deling av helse- og personopplysninger mellom pasient og helsepersonell (eksempel velferdsteknologi og spesialisthelsetjenesten)
- Behov for å tilgjengeliggjøre grensesnitt fra nasjonale fellesløsninger til tredjeparts programleverandører.

Referansearkitekturen for datadeling baseres på tjenester som tilbys som grensesnitt. Disse grensesnittene, heretter kalt datadelingsgrensesnitt, tilgjengeliggjøres for andre aktører gjennom bruk av webteknologi. Datadelingsgrensesnitt må kunne støtte både lesing og registrering/oppdatering av helse- og personopplysninger, og dette krever tilgangsstyring på tvers av virksomheter, i tillegg til høy tilgjengelighet.

Datadeling mellom helseaktører har i dag en begrenset utbredelse. Dette dokumentet vil beskrive noen eksisterende anvendelser. Mange aktører vurderer bruk av datadeling som

samhandlingsmodell med andre aktører. Gjennom nasjonal styring kan man sikre enhetlig implementering av datadeling i helse- og omsorgstjenesten.

Et datadelingsgrensesnitt kan realiseres som et Web API. Begrepet API betegner i all enkelthet et grensesnitt i en programvare hvor spesifikke deler av denne kan aktiveres (kjøres) fra en annen programvare gjennom kall til grensesnittet. I dette dokumentet er API brukt i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt for andre aktører via webteknologi. Dette er også kalt Web API. Web API benyttes i dokumentet om både SOAP-baserte API-er og REST-baserte API-er.

1.1 Hva er en referansearkitektur?

Difi sin definisjon på referansearkitektur[1] er lagt til grunn for beskrivelsen av referansearkitektur:

Referansearkitekturer er beste praksis for hvordan man løser avgrensede, men gjentakende, problemstillinger.
Et eksempel fra den analoge virkeligheten er at de fleste dører er rektangelformede. Avvik fra denne normen er kostnadsdrivende fordi en må spesialbestille, og har en tendens til å skape problemer for både de som skal bygge huset og de som skal bruke døren etterpå. En referansearkitektur beskriver både forretnings-, applikasjons-, informasjons- og teknologilag. Bruk av referansearkitekturer bidrar til et felles språk, konsistent implementering av tekniske løsninger og etterlevelse av felles standarder. Referansearkitekturer kan ha ulike detaljeringsnivå, fra overordnet til svært spesifikke.

I denne konteksten beskriver en referansearkitektur logiske strukturer og begrepsapparatet som gjelder innenfor ett spesifikt område på et overordnet nivå.

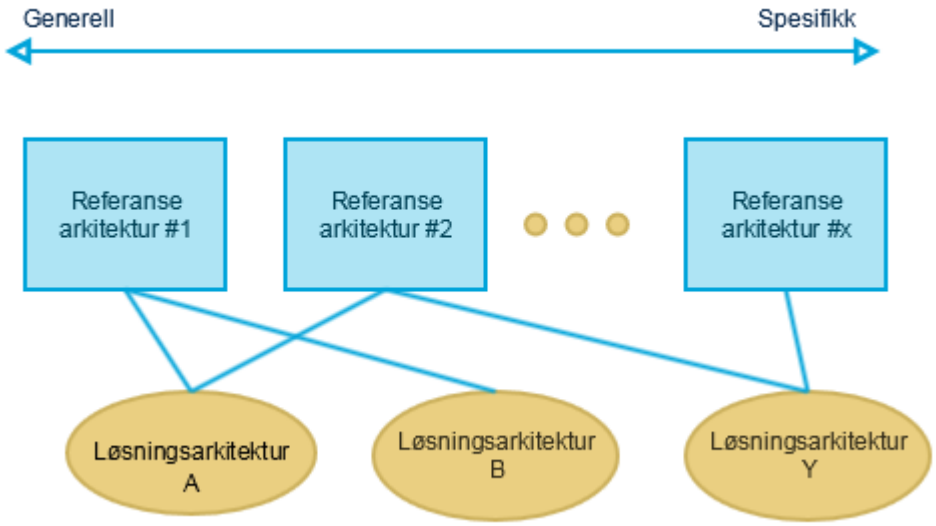
Referansearkitekturen kan også gi eksempler på logiske tjenester, komponenter og hvordan interaksjon skal foregå mellom disse.

Generelt kan en referansearkitektur beskrives på mange ulike abstraksjonsnivåer, fra spesifikk til mer generelle. En løsningsarkitektur kan anvende flere referansearkitekturer da en referansearkitektur kun beskriver et avgrenset problemområde, mens en løsningsarkitektur kan dekke flere problemområder.

En referansearkitektur har dermed et begrenset virkeområde. På øverste nivå beskriver man de forretningsmessige mål for området og beskriver ønskede egenskaper komponentene innen området skal ha. Deretter slår man fast hvilke overordnede prinsipper som må gjelde for komponenter, informasjonselementer og infrastruktur- og fellestjenester. På bakgrunn av dette identifiserer man områdene som kan standardiseres.

En nasjonal referansearkitektur for helse- og omsorgstjenesten gir både virksomheter og leverandører informasjon om felles rammeverk, standarder og profiler som gjelder for utviklingen av området.

[1] http://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur/referansearkitekturer



Figur 1 Forholdet mellom referansearkitekturer og løsningsarkitekturer

1.2 Sentrale begreper for datadeling

Sentrale begreper i dokumenteter beskrevet i Vedlegg A Sentrale begreper for datadeling

1.3 Formålet med en nasjonal referansearkitektur for datadeling

Denne referansearkitekturen har ulike formål for ulike interessenter.

For Direktoratet for e-helse skal referansearkitekturen være retningsgivende for arkitekturstyringen. Bruk av referansearkitekturen skal også gjøre det enklere å ta beslutninger om hvilke standarder og nasjonale profiler som må etableres, gjenbrukes og/eller endres samt behandle eksisterende og nye behov innen elektronisk samhandling.

For aktører innen helse- og omsorgstjenesten som skal realisere datadelingsløsninger vil formålet med referansearkitekturen være at aktørene gjør realiseringen på en enhetlig måte, benytter felles begreper og realiserer og gjenbruker de byggeklossene som inngår i referansearkitekturen.

1.4 Referansearkitekturens innhold

Strukturen i dokumentet er basert på beste praksis for dokumentasjon av virksomhetsarkitekturer (TOGAF). Dokumentet har følgende oppbygning:

- Visjon og målbilde - hva man ønsker å oppnå med elektronisk samhandling ved hjelp av datadeling

- Rammevilkårene for arkitekturen slik som lover, forskrifter og arkitekturprinsipper.
- Eksempler på forretningsmessige anvendelser av datadeling. Her beskrives brukstilfeller som er bakgrunnen for behovet for datadeling
- Begrepsmodeller - som viser sammenheng mellom ulike informasjonsobjekter innen datadeling
- Referansearkitekturen - beskrivelse av hvilke byggeklosser man trenger for å realisere datadeling og hvordan disse er realisert i eksisterende anvendelser.
- Beskrivelse av "AS-IS" arkitektur - teknisk beskrivelse av implementasjonen av arkitekturen for de valgte eksempler på anvendelse av datadeling.

Vi har også valgt å beskrive eksempler på etablerte arkitekturer for datadeling slik som datadeling av kritisk info på Kjernejournal, datadeling benyttet på Helsenorge.no plattformen og eksisterende løsninger innen velferdsteknologiområdet. Ved å beskrive de ulike anvendelsene sammen og med et felles språk, vil ulikheter og likheter komme tydelig frem. Da vil også et fremtidig målbilde være lettere å forstå, samt hva som skal til for å oppnå det.

Det er lagt vekt på å benytte felles begreper og generiske modeller som skal gjelde både for eksisterende anvendelser av datadeling, fremtidige anvendelser samt for sammenligning av ulike samhandlingsmodeller.

Eksisterende anvendelser er en beskrivelse av dagens situasjon og er et viktig utgangspunkt for videreutvikling av arkitekturen. De fungerer også som eksempler på de generiske modellene.

1.5 Anvendelsesområdet til referansearkitekturen

Referansearkitekturen sitt anvendelsesområde er innen helse- og omsorgstjenesten. Datadeling av strukturerte data omfatter i dette dokumentet informasjonsdeling og oppdatering av helse- og personopplysninger mellom helsepersonell, og mellom helsepersonell og innbyggere. Helseopplysninger er sensitive personopplysninger, men helse- og omsorgstjenesten deler også opplysninger av mer administrativ karakter, slik som adresse.

Referansearkitekturen er tenkt benyttet i forbindelse med:

- Digitalisering av helse- og omsorgstjenesten
- Bruk og utarbeidelse/oppdatering av e-helsestandarder og profiler
- Utarbeidelse av kravspesifikasjoner for e-helsekomponenter. Kravspesifikasjonene kan ta utgangspunkt i generelle komponenter, begreper og standarder/profiler som er beskrevet i referansearkitekturen.
- Være grunnlag for referansearkitekturer på andre områder.

1.6 Målgruppe

Referansearkitekturen er primært rettet mot beslutningstakere og arkitekter.

Referansearkitekturen er også relevant for prosjektledere og utviklere innen helse- og omsorgstjenesten.

2 Visjon

> *Samarbeid mellom aktører med umiddelbar, sikker deling og oppdatering av strukturert informasjon*

Det skal være enkelt for aktører å etablere deling og oppdatering av person- og helseinformasjon på en strukturert og standardisert måte, hvor det er tatt høyde for relevante lover og forskrifter.

3 Målbilde for datadeling

Mål for datadeling:

- Få tilgang til strukturerte data hos en annen aktør i henhold til tjenstlige behov
- Kunne oppdatere strukturerte data hos en annen aktør eller i et nasjonalt register
- Gi innbyggere innsyn i og mulighet til å oppdatere egne helseopplysninger

Datadeling skal gjøres i henhold til nasjonale referansearkitekturer, standarder og ved bruk av fellestjenester/ressurser.

Forholdet til nasjonal e-helsestrategi

Nasjonal e-helsestrategi og handlingsplan 2017-2022 [1] har som et av de strategiske områdene å bedre sammenhengen i pasientforløpet. Strategien er nærmere beskrevet i ulike innsatsområder og innsatsområde #2.4 omhandler:

- "Dele viktige helseopplysninger i den akuttmedisinske kjeden".

Innen dette innsatsområde beskrives det følgende:

- "For å få raskere tilgang til nødvendige helseopplysninger trenger derfor helsepersonell å kunne gjøre oppslag i elektroniske journalopplysninger i andre virksomheter."

I nasjonal handlingsplan er følgende tiltak en del av planen for 2017-2022:

Tiltak: Etablere felles samhandlingsarkitekturer for ulike måter å dele informasjon på

I tillegg til samhandlingsarkitekturen for utveksling av meldinger, skal det etableres felles samhandlingsarkitekturer for deling av dokumenter og tilgang på tvers av virksomheter. Det skal utarbeides plattform- og integrasjonsstrategi for utvikling av nødvendig samhandlingsarkitektur på vei mot Én innbygger – én journal.

4 Rammevilkår

4.1 Lover og forskrifter

Datadeling mellom helsepersonell handler om å tilgjengeliggjøre person- og helseopplysninger for lesing og skriving i henhold til tjenstlig behov.

Det er vesentlig at nødvendige helseopplysninger er tilgjengelig for den som yter helsehjelp. Pasientjournalloven § 19 åpner derfor for tilgjengeliggjøring av opplysninger fra behandlingsrettede helseregistre (herunder EPJ etter pasientjournalloven § 8 og samarbeidsløsninger etter pasientjournalloven §§ 9 og 10).

Innenfor rammen av taushetsplikten, jf. helsepersonellovens taushetspliktsbestemmelser, skal den databehandlingsansvarlige 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, jf. pasientjournalloven § 19 første ledd. Dette gjelder både intern og ekstern datadeling. Opplysningene kan uansett bare gjøres tilgjengelig for personell som har et tjenstlig behov for opplysningene, jf. at «relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell»

Det er den databehandlingsansvarlige som bestemmer hvordan opplysningene skal gjøres tilgjengelig, jf. pasientjournalloven § 19 annet ledd. Dette kan skje både ved direkte tilgang og ved at opplysningene utleveres via meldingsutveksling.

Dersom det skal gis direkte tilgang til eksterne virksomheter, gjelder særskilte krav etter forskrift om tilgang mellom virksomheter, jf. pasientjournalloven § 19 tredje ledd. Forskriften krever at det inngås egen avtale som regulerer nærmere bestemte forhold. Etter forskriften er det kun anledning til å gi lesetilgang til opplysninger, ikke skrivetilgang.

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

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

Pasientens eller brukerens rettigheter skal i alle tilfeller ivaretas. Dette innebærer blant annet mulighet til å reservere seg mot at opplysninger gjøres tilgjengelig for andre, jf. pasientjournalloven § 17, og rett til informasjon og innsyn i hvem som har fått tilgang til opplysninger, jf. pasientjournalloven § 18.

Pasientjournalloven § 10 regulerer etablering av nasjonale behandlingsrettede helseregistre som kommer i stedet for virksomheters behandlingsrettede helseregistre etter §§ 8 og 9.

Oppsummert kan man dele datadeling i fem hovedgrupper, hvor datadeling mellom virksomheter er knyttet til tre av hovedgruppene. Hver av disse tre gruppene skiller seg fra hverandre ved at man deler data på ulike måter og har ulike krav knyttet til seg:

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

De siste 2 hovedgruppene er koblet til deling av data med innbyggere. Den ene gruppen dekker der hvor innbygger får tilgang til sine helseopplysninger digitalt. I lovverket finnes det generelle krav om å gi pasienter innsyn i egne data (pasient- og brukerrettighetsloven § 5.1, helsepersonelloven § 41, pasientjournalloven § 18). Den andre gruppen er der hvor innbygger oppdaterer sine helseopplysninger via bruk av for eksempel portal og mobile app-er og hvor innbygger rapporterer inn informasjon om eget helseforhold, for eksempel via velferdsteknologi eller skjemainnrapportering.

4.2 Annet

4.2.1 Norm for informasjonssikkerhet i helse og omsorgstjenesten

Alle virksomheter som er tilknyttet Helsenettet er forpliktet til å følge Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen)[2].

Spesifikke krav til datadeling mellom virksomheter er beskrevet i Normen[3], kapittel 5.2.1, 5.2.2 og 5.2.3. Noen utdrag av krav som er vesentlig for arkitekturen:

Ved tilgang til helseopplysninger mellom virksomheter skal helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet:

- *beskrive rettigheter og plikter som følger av autorisasjonen*
- *være i samsvar med regler om taushetsplikt*
- *dokumenteres i virksomhetens autorisasjonsregister*
- *tidsbegrenses*
- *alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold*

Ved tilgang til helseopplysninger mellom virksomheter kan pasienten/brukeren kreve at tilgang til egne helseopplysninger sperres for helsepersonell fra andre virksomheter enn der opplysningene er nedtegnet. Med sperring menes en teknisk løsning der journalopplysninger gjøres utilgjengelige for enkeltpersoner, grupper av helsepersonell eller helsepersonell i andre virksomheter enn der journalnotatene er registrert.

Ved tilgang til helseopplysninger mellom virksomheter skal begge virksomhetene ha tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger som minst ivaretar at:

[2] http://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
[3] Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

- *helseopplysningene ikke gjøres tilgjengelige dersom pasienten/brukeren har motsatt seg eller motsetter seg det*
- *det kun gis tilgang til helseopplysninger som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til pasienten/brukeren*
- *helsepersonellet er autorisert for slik tilgang, og har autentisert seg ved bruk av sikker autentiseringsløsning*

I tilknytning til Normen er det utarbeidet en rekke veiledere og faktaark. Disse gir forslag til løsninger, men det kan også være andre måter å ivareta kravene på.

Spesielt relevant for datadeling er følgende:

- Faktaark 15 – Logging og oppfølging av logger [2]
- Faktaark 20c – Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter [3]
- Faktaark 24 – Kommunikasjon over åpne nett [4]
- Faktaark 47 – Autorisasjonsregister [5]
- Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter [6]
- Veileder med avtaleeksempler ved samarbeid om felles journal [7]
- Veileder for tilgangsstyring [8]

4.3 Arkitekturprinsipper som er felles for samhandlingsmodellene

Forretningsmessige arkitekturprinsipper

1. Avvik fra referansearkitektur eller vedtatte standarder må være eksplisitt vurdert, begrunnet og godkjent av partene.
2. De ulike lagene i arkitekturen skal være uavhengige av hverandre (informasjonsinnhold, kommunikasjon, infrastruktur og basistjenester).
3. Avvik og feilsituasjoner skal kunne oppdages og følges opp iht. rutiner.

Informasjonsprinsipper

1. Informasjonsinnhold skal være uavhengig av samhandlingsmodell, og være basert på vedtatte standarder, informasjonsmodeller og kodeverk/terminologi der det finnes.
2. Ved utveksling/deling av sensitiv informasjon skal avsender/databehandler forsikre seg om at mottaker/konsument har nødvendig hjemmel eller at det er gjort en avtale om at de kan behandle informasjonen.
3. Journalnotater som deles/utveksles skal være kvalitetssikret og godkjent av den som registrerte informasjonen.
4. Når informasjon deles/utveksles skal også nødvendige metadata om informasjonen, som tidspunkt for registrering, hvem/hva som har registrert den, hvilken status informasjonen har (utkast, godkjent eller automatisk innhentet) gjøres tilgjengelig.

4.4 Arkitekturprinsipper for datadeling

4.4.1 Forretningsmessige arkitekturprinsipper

Nr	Forretningsmessige arkitekturprinsipper	Kommentar
1	Forretningsprosesser må beskrives for de enkelte anvendelsene av referansearkitekturene	
2	Datadelingsgrensesnitt skal fortrinnsvis være basert på åpne internasjonale standarder eller andre vedtatte standarder	Et datadelingsgrensesnitt er et grensesnitt som tilgjengeliggjøres av en aktør for andre aktører gjennom bruk av webteknologi
3	Nasjonale datadelingsgrensesnitt skal gjøres tilgjengelig gjennom felles plattformer, der dette er etablert	Med felles plattform menes en kombinasjon av teknologiske infrastrukturprodukter og -komponenter som forenkler tilgang for klienter gjennom at nasjonale datadelingsgrensesnitt kan aksesseres via en felles plattform.
4	Nasjonale datadelingsgrensesnitt skal inngå i nasjonal arkitekturstyring og forvaltning	

4.4.2 Informasjons- og sikkerhetsprinsipper for datadeling

Nr	Informasjons- og sikkerhetsprinsipper	Kommentar
1	Kun autentiserte brukere (eller virksomheter) kan gis tilgang til tjenester som inneholder person- og helseopplysninger	Virksomheter som gis tilgang må ha en intern tilgangsstyring som gir tilgang iht. tjenstlige behov og avtaler
2	Det må være en sikker brukerautentisering (konsumentautentisering) som virksomhetene som tilbyr datadelingsgrensesnitt har tillit til.	
3	Virksomheten som ber om tilgang skal kontrollere at brukeren (konsumenten) har nødvendige autorisasjoner for det aktuelle datadelingsgrensesnittet	Unntak kan være der man har et sentralt autorisasjonsregister og brukeren aksesserer tjenesten direkte
4	Det skal skilles mellom lese- og skriverettigheter til forskjellige informasjonselementer basert på den enkelte brukers autorisasjon	En bruker kan for eksempel gis leserettighet, men ikke skriverettighet.
5	Unødvendig mellomlagring skal unngås	

6	Det må være mulig for klienter å kunne verifisere legitimiteten til datadelingsgrensesnittet og virksomheten som tilbyr den.	
7	Felleskomponenter for autentisering av konsument skal benyttes der det er tilgjengelig	

4.4.3 Tekniske arkitekturprinsipper for datadeling

Nr	Tekniske arkitekturprinsipper	Kommentar
1	All kommunikasjon mellom virksomheter skal være sikret for konfidensialitet (kryptering) og integritet.	Virksomhet inkluderer også nasjonale felleskomponenter/-løsninger
2	Datadelingsgrensesnitt skal være i henhold til anbefalte eller obligatoriske tekniske standarder	Når mange virksomheter skal ta i bruk datadeling, vil man oppnå store gevinster ved å bruke felles tekniske standarder.
3	Datadelingsgrensesnitt skal være uavhengig av den enkelte konsumenten	Man skal unngå å lage et datadelingsgrensesnitt som er tilpasset et produkt/løsning som er konsument, og dermed er vanskelig å gjenbruke for andre
4	Når nye versjoner av et grensesnitt innføres, skal tidligere versjon(er) opprettholdes i en forutbestemt periode	Versjonshåndtering av grensesnitt skal følge en predefinert, og dokumentert prosess slik at det skapes forutsigbarhet hos konsumentene
5	Alle tekniske grensesnitt skal gis et forståelig navn og versjonsnummer; dette angis som en del av grensesnittet	
6	Fellestjenester for publisering av grensesnitt skal benyttes der det er tilgjengelig	
7	Bruken av datadelingsgrensesnitt skal logges	Det må logges hvilken konsument som har brukt hvilket datadelingsgrensesnitt og når.
8	Alle datadelingsgrensesnitt skal være dokumenterte, og de ulike operasjonene som tilbys må beskrives	Denne dokumentasjonen skal være rettet mot konsumentenes utviklingspersonell og fungere som implementasjonsguide for disse.

9	Det skal gis anvendbare feilmeldinger når datadelingsgrensesnitt ikke er tilgjengelig/feiler	Med anvendbare menes her at de er forståelig, gir verdi for og kan tolkes av konsumentene
10	Datadelingsgrensesnitt må være tilgjengelige, robuste og skalerbare	Kravene vurderes for tjenestens kritikalitet og omfang.

5 Utvalgte eksempler på brukstilfeller hvor datadeling er aktuell

Dette kapittelet er informativt og basert på brukstilfeller beskrevet i 2017, så det kan ha skjedd endringer i tjenestene eller måten tjenestene blir benyttet etter dette.

5.1 Helsepersonells tilgang til pasientens journalinformasjon

Når virksomheter er pliktig til å gi helsepersonell hos andre virksomheter helseopplysninger om en pasient, kan dette gjøres på ulike måter: muntlig, skriftlig, ved hjelp av elektronisk meldingsutveksling eller ved styrt tilgang til nødvendig og relevante opplysninger til pasientens elektroniske journal. Dette avsnittet omhandler den siste metoden.

Fra EPJ standard del 2: Tilgangsstyring, redigering, retting og sletting [9]:

> *«Tilgang til helseopplysninger i elektronisk pasientjournal (EPJ) skal i utgangspunkt kun gis til helsepersonell i den grad dette er nødvendig for å yte pasienten helsehjelp og i den grad pasienten ikke motsetter seg det».*

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

Tilgang til sensitive opplysninger kan styres ved at en person gir andre tilgang per dokument, eventuelt at en hel gruppe kollektivt blir autorisert for all sensitiv informasjon. Dette er en modell som er lite egnet i helse- og omsorgssektoren. Helsepersonells hverdag består av både planlagt arbeid og uforutsette situasjoner som må håndteres der og da. Det er derfor ikke praktisk gjennomførbart at en eksplisitt må autorisere helsepersonells tilgang til en pasients journal når uforutsette hendelser oppstår. Samtidig kan man ikke gi alt helsepersonell, normalt basert på rolle, tilgang til alle helseopplysninger, siden dette strider med lover og forskrifter. Internt i helseforetak løses dette ofte ved at det gis en grunntilgang basert på roller, men at man før åpning av journalen for en spesifikk pasient må oppgi hvorfor tilgang er nødvendig (det tjenstlige behovet).

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

Det ligger en beslutning til grunn for all helsehjelp

En slik beslutning kalles normalt for et besluttet tiltak og er normalt opphavet til det tjenstlige behovet. Dette tiltaket kan være både eksplisitt (for eksempel kommunalt vedtak) og implisitt (for eksempel pasient bestiller time hos fastlegen sin).

Før en beslutning om å yte helsehjelp kan tas, har helsepersonell behov for å vurdere pasientens helseopplysninger og må da ha tilgang til all relevant informasjon.

Det skal kun gis tilgang til helseopplysninger i forbindelse med gjennomføring av besluttede tiltak

Det er i helse- og omsorgtjenesten et krav at det skal kun gis tilgang til helseopplysninger i forbindelse med gjennomføring av et besluttet tiltak.

Enhver tilgang til helseopplysninger skal ha et uttrykkelig angitt og saklig begrunnet formål

Lovgivningen legger stor vekt på at enhver tilgang til helseopplysninger skal ha et uttrykkelig angitt og saklig begrunnet formål, jf. personopplysningsloven § 11 bokstav b. Et besluttet tiltak skal derfor alltid knyttes til en eller flere formål.

Helsepersonell skal ikke gis tilgang til flere helseopplysninger enn det som er nødvendig

Ved all tilgjengeliggjøring av helseopplysninger gjelder at det ikke skal tilgjengeliggjøres flere opplysninger enn det som er nødvendig for formålet med tilgjengeliggjøringen.

All tilgang skal være tidsbegrenset

Når et besluttet tiltak opphører, skal også tilgangen opphøre.

En pasient har rett til å motsette seg helsepersonells tilgang til sine helseopplysninger

En pasient kan fremsette krav om sperring av deler av en journal (ikke hele journalen) og kunne sperre for innsyn for navngitte helsepersonell, grupper eller virksomheter. Alle pasientjournaler skal ha en journalansvarlig. Dersom pasienten har sperret visse journalopplysninger, skal helsepersonell varsles om dette og skal kunne be pasient om innsyn (be om samtykke for innsyn i sperret del). Før et slik innsynsforespørsel gjøres, kan man be journalansvarlig om sperrede opplysninger er relevant for det aktuelle tilfellet.
En pasients rett til å motsette seg tilgang til sine helseopplysninger er i tillegg ikke absolutt. Det følger av pasient- og brukerrettighetsloven § 5-3 tredje ledd og helsepersonelloven § 23 nr. 4, at helseopplysninger kan utleveres tross pasientens motstand dersom tungtveiende grunner taler for dette, for eksempel dersom det er fare for liv eller alvorlig helseskade.

5.2 Sikker tilgang til data på tvers av virksomheter.

Forskrift om tilgang til helseopplysninger mellom virksomheter gir mulighet for at en virksomhet kan dele pasientjournalopplysninger med andre virksomheter ved at det inngås avtale om dette og at det gjøres på en sikker måte. En metode for å dele pasientjournalopplysninger kan være at virksomheten som er databehandleransvarlig tilbyr en datadelingstjeneste basert på API-er.

Å gi eksterne brukere tilgang til aktuelle pasientjournalopplysninger er derfor nødvendig for å tilby datadelingstjenester til andre samarbeidende virksomheter, men dette har flere utfordringer. Hvis hver databehandleransvarlig skal håndtere autentisering av eksterne brukere medfører det at brukere får mange identiteter og mange passord samt at det blir en utfordring å administrere eksterne brukere i henhold til lover og forskrifter.

Ved å innføre tillitsforhold mellom en som utsteder identiteter og en virksomhet sine tjenester, kan man frakoble autentiseringsmekanismer fra applikasjoner og tjenester og brukere kan gjenbruke en eksisterende identitet hos flere samarbeidende virksomheter.

5.3 Brukstilfeller hvor kun helsepersonell er involvert

5.3.1 Samarbeid om pasient

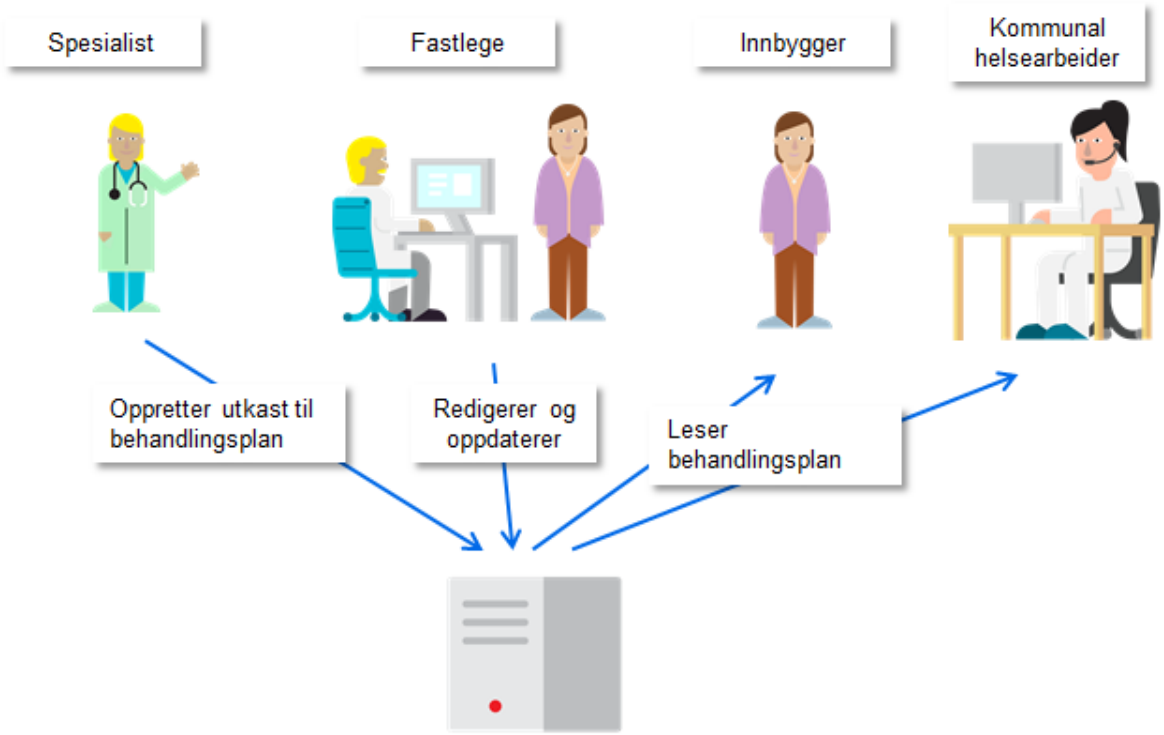
Fra EPJ standard del 2 [9] «2.2.1. Helsepersonelloven» og «2.2.2. Pasientjournalloven»:

> *«Helsepersonelloven § 25 regulerer helsepersonells adgang til å gi helseopplysninger til personell de samarbeider med i forbindelse med den helsehjelp som ytes. Opplysningene kan gis til samarbeidende helsepersonell både innenfor og utenfor virksomheten. Helsepersonelloven § 45 gjør det klart at helsepersonell som skal yte eller yter helsehjelp til pasient, skal gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. Opplysninger kan etter begge disse bestemmelsene gis både muntlig, skriftlig, som elektronisk melding og som styrt tilgang til nødvendige og relevante opplysninger i en pasients EPJ. ... Pasientjournalloven § 19 pålegger virksomheten å sørge for at relevante og nødvendige helseopplysninger er tilgjengelig for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den pasienten. Bestemmelsen er ikke begrenset til personell i egen virksomhet og den gjelder også dersom flere virksomheter benytter et felles pasientjournalsystem»*

Samhandlingsreformen [10] gir sykehus og kommuner en plikt til å samarbeide om behandlingen og forebygging av sykdom hos innbyggeren. Det ligger som en forutsetning for godt samarbeid at aktørene også kan samarbeide om behandlingsplaner og andre helseopplysninger. Samarbeidet kan inkludere deling av dokumentasjon fra den ene virksomheten til den andre, deling av opplysninger som innbygger selv har produsert (for eksempel fra velferdsteknologisk utstyr og skjema), og kan også inkludere interaktivt samarbeid om dokumenter som for eksempel egenbehandlingsplaner. For mer avanserte samarbeidsformer rundt en pasient vil ikke meldings- og dokumentutveksling være tilstrekkelig for å kunne lage fleksibel og gode samarbeidsløsninger. Her vil samarbeidsprosesser og arenaer kreve datadeling der aktørene kan samarbeide om både dokumenter og mindre informasjonselementer.

En egenbehandlingsplan for avstandsoppfølging av kroniske sykdommer er et eksempel som krever at flere aktører er aktivt med i utarbeidelse og bruk av helseopplysninger. Egenbehandlingsplanen inneholder symptomer som pasienten og behandlere skal se etter, kategorisert i henhold til flere kategorier av forverring. Den inneholder også tiltak som pasient og behandler bør ta, inkludert medisinkurer og andre type aktiviteter som pasienten bør gjennomføre (for eksempel typer trening, "Gå en tur hver dag" eller "Ta det med ro"). Planen kan også inneholde informasjon om hvilke målinger og skjema pasienten skal fylle inn og rapportere til behandlere. Etableringen av en slik egenbehandlingsplan inkluderer typisk spesialisthelsetjenesten, fastlegen, kommunen og pasienten selv, men kan også involvere andre aktører som for eksempel fysioterapeut og pårørende. Planen kan ofte ikke anses som ferdig før alle aktørene har kommet med sine innspill, og den bør kunne endres fleksibelt avhengig av endringer i pasientens tilstand. Samhandling rundt en egenbehandlingsplan er derfor et scenario som passer godt for datadeling, fordi flere aktører er med i prosessen om å utarbeide en felles plan. Planen kan bestå av informasjonselementer som forskjellige aktører bidrar med. En bør kunne kommentere og diskutere innholdet av planen utenfor selve planen, informasjonen må kunne endres over tid og flere må ha tilgang til å se status og innholdet på ethvert tidspunkt. Det er vanskelig å få til det nødvendige nivået av

interaktivitet ved bruk av meldingsformidling eller dokumentutveksling, og dokumentdeling dekker heller ikke scenarioet helt.



Figur 2 Samhandling om behandlingsplan

5.3.2 Oppslag sentral tjeneste eller i annen virksomhet

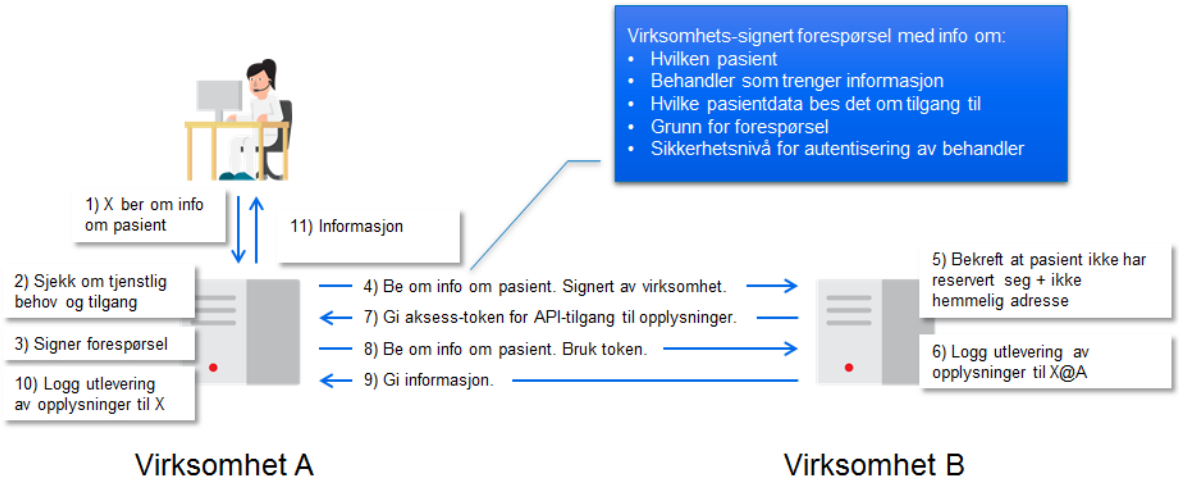
Stortingsproposisjon om pasientjournalloven og helseregisterloven [11] peker eksplisitt på at virksomhetsgrenser ikke skal være til hinder for deling av helseopplysninger:

> *«Departementet mener at helsepersonell bør kunne gis tilgang uavhengig av hvor pasienten tidligere har fått helsehjelp. Med tilgang menes at autorisert helsepersonell gis adgang til selv å søke etter relevant informasjon om konkrete pasienter i virksomhetens journalsystem. Virksomhetsgrenser bør ikke være et rettslig hinder for at helsepersonell kan gis tilgang til helseopplysninger når de skal gi helsehjelp.»*

Samarbeid om informasjonsressurser og dokumenter på tvers av virksomheter er komplisert. Det trengs derfor gode retningslinjer og sentrale føringer for referansearkitektur for deling for at løsningene skal være både kostnadseffektive og sikre. Lovgrunnlaget og Pasientjournalloven §19 peker på at det skal være mulig for helsepersonell med tjenstlig behov å gjøre oppslag i andre virksomheters systemer dersom de har tjenstlig behov. For at dette skal kunne gjøres må det opprettes avtaler mellom virksomhetene og en teknisk løsning må etableres som ivaretar sikker deling av data. Deling av data på tvers av virksomheter forutsetter at pasienten ikke har motsatt seg slik deling.

Veileder for deling av helseopplysninger mellom virksomheter [8] beskriver forskjellige scenarioer for hvordan deling kan implementeres. Brukerscenarioet er at en behandler i en virksomhet (A) trenger helseopplysninger som er lagret i en annen virksomhet (B). Behovet for opplysninger er basert på tjenstlig behov, som for eksempel kan være at pasienten er innlagt til behandling i virksomhet A og behandleren trenger å se hvilken behandling og hvilke vurderinger som ble gjort i virksomhet B. Slik lovgrunnlaget er formulert er tilgangen

mulig gitt at det er tjenstlig behov for tilgang, virksomhetene har avtaler og virksomhetene har riktig tilgangsstyring og logging av tilgang. Systemet i virksomhet A bør ikke basere tilgangen kun på roller, men kan også legge andre data til grunn, for eksempel at pasienten er registrert i systemet til A som pasient, at pasienten er innlagt, at pasienten har en time for behandling, at helsepersonell sannsynliggjør hvorfor tjenstlig behov er tilstede eller lignende. Akkurat hva som er grunnlaget for tilgangen er utenfor omfanget til denne referansearkitekturen, men det antas at virksomhet A har rutiner og tekniske løsninger på plass som gir tilstrekkelig tilgangsstyring.



Figur 3 Eksempel på tilgangskontroll

Figur 3 viser et eksempel på at tilgangskontrollen gjøres av Virksomhet A, og hvor virksomhet B her høy grad av tillit til Virksomhet A.

Selv om utleverende virksomheter kan delegere mye av tilgangsstyringen til mottagende virksomheter, så kan det være tilfeller der også virksomhet B ønsker å ha sterkere tilgangsstyring, for eksempel ved bruk av eksterne registre. B kan også være en nasjonal løsning for lagring av helseopplysninger, for eksempel basert på pasientjournalloven § 10.

5.3.3 Oppdatering/registrering sentral tjeneste eller i annen virksomhet

Samhandlingen som er hjemlet i pasientjournalloven § 19 er i utgangspunktet begrenset til oppslag og uthenting av informasjon i andre virksomheter, og dekker ikke oppdateringer og registreringer av informasjon i den andre virksomheten. For å muliggjøre at helsepersonell skal dokumentere i en annen virksomhet sine systemer krever dette i utgangspunktet etableringen av en felles journal i henhold til pasientjournalloven §9 eller §10.

Et eksempel der helseopplysninger registreres i en sentral tjeneste er kjernejournal, som er hjemlet i pasientjournalloven§ 13 og i egen forskrift. Her kan behandlere og pasienten selv lagre kritiske helseopplysninger som er viktig å dele med forskjellige helseaktører. Hvilke data som kan lagres i kjernejournalen er begrenset i kjernejournalforskriften.

Helsepersonell kan i visse tilfeller dokumentere i andre virksomheters løsninger som hjemlet i pasientjournalloven§ 8, for eksempel hvis den ene virksomheten har databehandleravtale og er innleid til å utføre en behandling på vegne av den som eier det behandlingsrettede helseregisteret. Et eksempel på dette er når en kommune har gitt en virksomhet som leverer responssentertjenester for trygghetsalarmer oppgaven å følge opp trygghetsalarmer på

vegne av kommunen. I slike tilfeller kan ansatte i den eksterne virksomheten få tilgang til å dokumentere helsehjelp i kommunens EPJ uten at dette er en fellesjournal i henhold til pasientjournalloven§ 9.

5.3.4 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 mulig å søke etter tjenester, enheter og annen informasjon i ulike registre og søketjenester som:

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

Grunndata vil også bli benyttet som grunnlag for attributtbasert tilgangsstyring, som autorisering av en person eller et system.

5.3.5 Søknadsbehandling

Det finnes flere eksempler på søknadsbehandling innen helse- og omsorgstjenesten. Helsepersonell skal kunne sende inn søknader på vegne av seg selv og pasienter hvor mottagende part gjør en behandling av søknaden og sender svar på søknaden tilbake. Ved innlevering av søknad ønskes ofte aksept av at søknad er mottatt og akseptert i sanntid (må ikke forveksles med applikasjonskvittering). Søknadsbehandlingen kan være manuell og automatisk. Ved automatisk behandling forventes normalt et svar på søknad i sanntid og som respons på innsendelse av søknad. Der hvor det er en viss saksbehandlingstid så kan det være ønskelig å kunne spørre om status på behandlingen.

Eksempler på eksisterende søknadsbehandling er "Godkjenningsfritak for legemidler" og "søknad om individuell refusjon til viktige legemidler"

5.4 Brukstilfeller hvor pasient er involvert

5.4.1 Innsyn i egne helseopplysninger

Brukere har rett til informasjon og innsyn i egne helseopplysninger som følge av personopplysningsloven § 18 og presisert i helseregisterloven § 24 Rett til informasjon og innsyn.

Eksempler er at pasient ønsker innsyn i hvilke opplysninger som finnes om seg selv og egne barn i et forskningsregister eller behandlingssted.

For å gjøre dette elektronisk kan det benyttes datadeling i form av API-er som kan konsumeres av portalløsninger som Helsenorge.no og app-er for mobiltelefoner.

5.4.1.1 Innsyn i egen journal

Innsyn i egen journal er en spesialisering av innsyn i egne helseopplysninger. Informasjon i journalen kan være strukturert som et dokument. For å gjøre dette elektronisk kan det benyttes datadeling i form av API-er som returnerer dokumenter eller strukturerte data. Slike API-er kan konsumeres av portalløsninger som Helsenorge.no og app-er for mobiltelefoner.

5.4.2 Deling av egne helsedata til helsepersonell

Egne helsedata er knyttet til egenregistrerte data (se «Innrapportering av medisinske måledata» under), eller data fra andre møter med helsetjenesten, for eksempel fra utlandet. Innbygger ønsker å dele egne helsedata med helsepersonell, for eksempel til sin fastlege. Innbygger må aktivt gi samtykke til delingen til helsepersonellet. Selve delingen kan gjøres på ulike måter. Ved bruk av datadeling må fagsystemet kunne hente informasjon fra løsningen hvor pasienten har lagret sine helsedata. Personlig helsearkiv (PHA) er en lagringsløsning som egner seg for lagring av egne helsedata. Per dags dato er det foreløpig ingen hjemmel i lov for å dele informasjon med helsepersonell fra PHA.

5.4.3 Innrapportering av medisinske måledata

Velferdsteknologi skal bidra til at brukere skal kunne mestre egen helsesituasjon på best mulig måte. Spesielt gjelder dette personer med kronisk sykdom, men også oppfølging før og etter behandling. Et økende antall type utstyr knyttet til mobil- eller smarthusteknologi tas i bruk, herunder sensorer for måling av kroppsmasse, blodtrykk og oksygenmetning.

Målinger skal kunne sendes automatisk til de som skal ha informasjonen, eller som en del av et elektronisk spørreskjema. Mottagere vil være kommunale responssentre, fastleger, spesialisthelsetjenesten, pårørende og personlig helsearkiv.

Pasienter med KOLS (kronisk obstruktiv lungesykdom) er ofte på sykehus. Gruppen kan rapportere inn dagsform og oksygenmetning ved hjelp av nettbrett og sensor. Tett oppfølging vil kunne forebygge forverring av helsetilstand, og varsle om akutt forverring slik at helsevesenet kan vurdere videre tiltak og behandling.

5.4.4 Skjemadialog

I mange tilfeller ønskes det dialog med pasienter i forbindelse med medisinsk oppfølging av primær- eller spesialisthelsetjeneste, helseundersøkelser over tid, enkel innrapportering av medisinske måledata, brukerundersøkelser med mer. Dialogen kan være repeterende (svar på samme spørsmål repetitivt over en viss periode) eller som en engangshendelse.

Det er en fordel at dialogen er strukturert og tilpasset pasientens behandling, tjeneste eller sykdom. Man benytter da standardiserte skjema som beskriver hvilke spørsmål som pasientene skal svare på. Det kan også være behov for at skjemaet er forhåndsutfylt med eksisterende informasjon om pasienten. Pasienten må på en eller annen form (typisk SMS eller epost) få beskjed om at han/hun må fylle ut skjemaet og adresse til hvor pasienten må gå til for å fylle det ut. Pasienten må identifiseres sikkert før han/hun starter å svare. Ved repetisjon, så kan gjenbruk av tidligere innlogget sesjon vurderes. Utfyllingen må kunne mellomlagres før endelig innsendelse. Når pasienten har svart på spørsmålene, vil dette normalt være sensitiv informasjon som må håndteres konfidensielt og sikres mot uautorisert tilgang.

I dette brukerscenarioet kan det benyttes flere typer samhandlingsmodeller hvor datadeling kan benyttes til flere av funksjonene, slik som varsling, mellomlagring og innsendelse av svarene.

6 Begrepsmodeller

Vi har valgt å etablere et par begrepsmodeller slik at en referansearkitektur kan beskrives på en ensartet måte. Det er lagt vekt på at begrepsmodellene kan relateres til ulike anvendelser hvor datadeling benyttes samt eksisterende tekniske standarder.

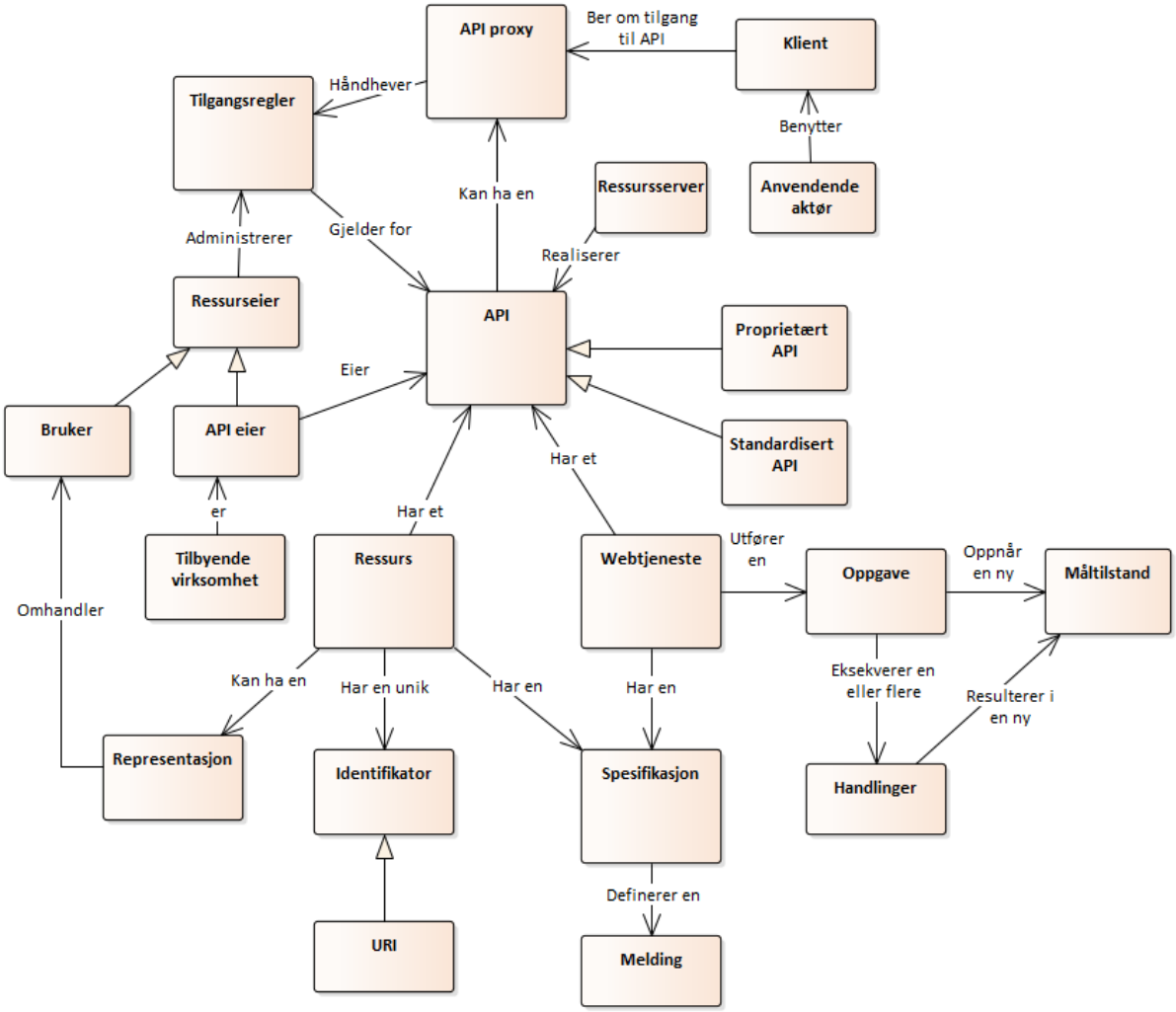
De to begrepsmodellene som er beskrevet under er for datadelingsgrensesnitt og for tilgangsstyring. I datadeling er tilgangsstyring veldig sentralt; den skal regulere hva som deles med hvem, samt hva brukeren får lov til å gjøre med dataene.

6.1 Begrepsmodell datadelingsgrensesnitt

Et datadelingsgrensesnitt kan realiseres som et API. Bruken av begrepet API benyttes ulikt i forskjellige kontekster. I dette dokumentet er API brukt i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt i en programvare for andre aktører via web. Dette er også kalt Web API. API benyttes i dokumentet som både SOAP-baserte API-er og REST-baserte API-er. Arkitekturmessig er det stor forskjell på om arkitekturen er REST-basert eller SOA-basert. REST-basert arkitektur kalles også for ROA - Resource Oriented Architecture som i likhet med SOA (Service Oriented Architecture) er et arkitekturmønster.

Figur 4 viser en konseptuell modell over begreper innen datadeling. Modellen er inspirert av W3C sin referansearkitektur for web service arkitektur[4].

[4] W3C Web Service Architecture



Figur 4 Konseptuell begrepsmodell for datadeling

Forklaring på begrepene i modellen i Figur 4:

Begrep i modell	Beskrivelse
API	Begrepet API betegner et grensesnitt i en programvare hvor spesifikke deler av denne kan aktiveres (kjøres) fra en annen programvare gjennom kall til grensesnittet. I dette dokumentet er API brukt i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt i en programvare for andre aktører via web. Dette er også kalt Web API. API benyttes i dokumentet som både SOAP-baserte API-er og REST-baserte API-er.
Standardisert API	Et API hvor innholdsformatet er basert på en nasjonal eller internasjonal standard. Eksempel kan være FHIR.
Proprietært API	Et API hvor innholdsformatet er skreddersydd for kun en bestemt løsning og ikke basert på en standard.

API proxy	En tjeneste som videresender forespørsler til API-et og fungerer som et slags filter hvor man kan legge inn type handlinger som kan håndteres sentralt og gjør det enklere for ressurseiere å tilby API-er. Handlinger kan være å håndheve tilgangsregler, dvs. kun slippe igjennom forespørsler som aksepteres av reglene, logging, sjekke om sesjon er gyldig, rute forespørsler til riktig API osv.
API eier	En API eier er den som forvalter API-et.
Tilbyende virksomhet	Den tilbyende virksomhet er ansvarlig for tilgjengeliggjøringen av informasjonen og dermed hvem som skal ha tilgang til denne informasjonen.
Ressurstjener	Typisk en applikasjonstjener som tilgjengeliggjør API-et.
Ressurseier	Eier av ressursen eller webtjenesten.
Tilgangsregler	Regler som er forhåndsdefinert skal gjelde for et API og baserer seg på informasjon om brukeren, kalt attributter.
Ressurs	I henhold til RFC2396 [12] så kan en Ressurs være alt mulig så lenge det har en id. I vår kontekst så kan man si at ressurs er en fellesbetegnelse for en eller flere entiteter som deles med andre virksomheter/personer, og som er representert med et navn, har en eier og kan kontrolleres gjennom et API. Eierskapet er sterkt knyttet til retten til å bestemme tilgangsreglene til en ressurs.
Representasjon	En representasjon er dataobjekter som representerer en bestemt tilstand av en ressurs (identisk med klasse og objekt forholdet: ressurs er klassen og representasjon er objektet)
Identifikator	Identifikatorer benyttes for å unikt identifisere ressurser.
Webtjeneste	En webtjeneste er en virksomhetskapabilitet som er bygd opp av å utføre oppgaver som består av et sett med handlinger og som fremstår for den anvendende aktør som en sammensatt funksjon. I motsetning til en ressurs, så har ikke en webtjeneste en representasjon, men er nær knyttet til funksjonelle oppgaver som anvendende aktører ønsker å få utført for å oppnå en måltilstand.
Oppgave	En webtjeneste utfører en oppgave. En oppgave har som formål å oppnå en tilstand og består av å orkestrere en eller flere handlinger.
Handlinger	Handlinger er typisk å utføre deler av et program.
Måltilstand	En måltilstand er en predefinert tilstand som sier noe om hvorvidt en webtjeneste er fullført vellykket.
Spesifikasjon	Metadata om en ressurs eller webtjeneste. En spesifikasjon vil typisk beskrive det semantiske innholdet som normalt vil være definert som en melding
Melding	En melding i denne konteksten er en sammenstilt gruppe data definert av en spesifikasjon.

Anvendende aktør	Helsepersonell fra annen virksomhet eller en innbygger. Også kalt konsument eller bruker.
Klient	Det programmet som anvendende aktør benytter og som håndterer forespørsel om tilgang til API på vegne av den anvendende aktør.

6.2 Begrepsmodell for tilgangsstyring

Det er i dette kapittelet valgt en tilnærming hvor vi ser på ulike referansemodeller som ulike internasjonale sikkerhetsrammeverk benytter samt hvilke begreper disse bruker. Ved å basere seg på begreper fra deres referansemodeller kan en referansearkitektur også være mer gjenkjennbar for de som kjenner de internasjonale modellene og begrepene.

Før en ser på de internasjonale referansemodellene for tilgangsstyring, så beskrives hva som menes med tilgangsstyring, tilgangskontroll og påstandsbasert identitet.

Vil har lagt til grunn Normens faktaark nr. 14 sin definisjon på tilgangsstyring:

"Sikre at helse- og personopplysninger kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere (og system) autentiseres på en betryggende måte og at tilganger tildeles administreres, kontrolleres og fjernes"

6.2.1 Hva er tilgangskontroll?

En tilgangskontroll avgjør:

- hvem som skal få tilgang,
- på hvilke betingelser og
- hva den som har tilgang har lov til å gjøre (lese, skrive etc.).

Tilgangskontroll for helse- og personopplysninger bygger generelt på 5 mekanismer

1. Autentisering: en person eller applikasjon må bevise hvem de er.
2. Tjenstlig behov: Helsepersonell må ha et tjenstlig behov for å få tilgang til en pasients helse- og personopplysninger.
3. Autorisering: personen eller applikasjon må ha rettighetene som ressursen (eller ressurseier) krever.
4. Innebygd personvern: mulighet for samtykke, sperring og reservasjon
5. Sporbarhet: alle tilgangsbeslutninger skal logges og kunne være etterprøvbare.

Beslutningen om tilgang gjøres basert på en kombinasjon av de fire første mekanismene over for å avgjøre om en forespørsel om tilgang skal godkjennes.

6.2.2 Påstandsbasert identitet

En identitet kan sies å bestå av fakta om en bruker som er relevant i en gitt kontekst. Eksempler på fakta kan være: er myndig, er autorisert lege, jobber på Ahus. Disse fakta er påstander om en bruker (engelsk: *Claims*) og utgjør en påstandsbasert identitet (engelsk:

Claim based identity). En applikasjon må tro på en påstandsbasert identitet gjennom å stole på den som utstedte påstandssettet.

Et sett med påstander pakkes sammen i en sikkerhetsbillett (på engelsk *security token*). En sikkerhetsbillett signeres digital av den som har utstedt billetten. En applikasjon vil akseptere brukere dersom de kan fremvise en gyldig, signert sikkerhetsbillett fra en utsteder man har et tillitsforhold til.

Påstandsbasert identitet vil gjøre det enklere for applikasjonene å håndtere faktaopplysninger om brukere da de slipper å håndtere brukeradministrasjon og be brukere legge inn fakta om seg selv. I tillegg gjør det enklere for brukere da de kan gjenbruke en identitet og muliggjør "single sign-on".

Faktaene i sikkerhetsbilletten gjør det også mulig for applikasjonene å implementere en mer finkornet autentisering- og autoriseringsmekanisme.

Føderert identitetshåndtering

En utsteder av sikkerhetsbilletter kan selv ha ansvar for autentisering og selv være en identitetstilbyder (engelsk: *identity provider*). En annen mulighet er at den kan delegere dette til en eller flere andre identitetstilbydere som det er opprettet tillit til. Delegeringskonseptet kalles føderering. Med føderering kan et domene gi brukere i andre domener man har et tillitsforhold til (ofte kalt føderingspartnere) tilgang til sine egne applikasjoner. På den måten kan man oppnå sikker tilgang på tvers.

Internasjonale referansemodeller

Det finnes mange ulike internasjonale standarder for håndtering av påstandsbasert tilgangsstyring. De viktigste er:

- OAuth 2.0
- OpenId Connect
- User-managed Access
- SAML
- WS-Federation
- Xacml

Disse er nærmere beskrevet i Vedlegg B Internasjonale referansemodeller innen tilgangsstyring.

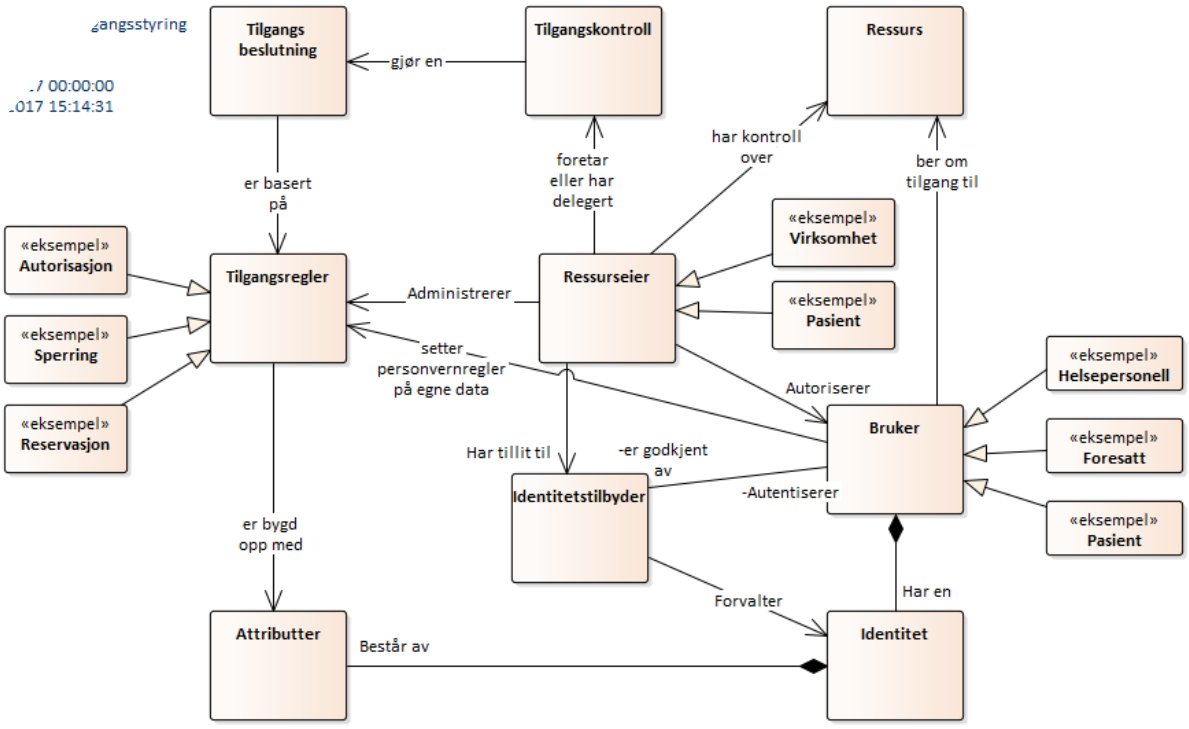
6.2.3 Begrepsmodell for tilgangsstyring

Tilgangsstyring er noe alle aktører som er tilkoblet til Helsenettet må ha for sine interne brukere av sine systemer, i henhold til Normen. Men hva må man ha av tilgangsstyring når en aktør skal tilgjengeliggjøre sine systemer gjennom datadeling til andre aktører og brukere?

I henhold til Normen (versjon 5.3) kapittel 5.2 omhandler tilgangsstyring:

- *Autorisering som er tildeling av rettigheter til å kunne lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger*
- *Autentisering som sikrer identifisering av autorisert bruker*

- *Tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter/brukere for autorisert personell*
- *Tilgjengeliggjøring av helse- og personopplysninger til annet personell enn virksomhetens eget personell.*
- *Regulering av privat bruk av virksomhetens informasjonssystemer*
- *Kontrollerende tiltak*



Figur 5 Konseptuell begrepsmodell for tilgangsstyring mellom virksomheter og innbyggere

Figur 5 viser en konseptuell modell over begreper som benyttes i forbindelse med tilgangsstyring på tvers av virksomheter og til innbyggere.

En *ressurs* er knyttet til en eller annen form for helse- og personopplysninger, og *ressurseier* er den som administrerer tilgang til ressursen gjennom å utforme regler for hvem som skal ha tilgang. En *ressurseier* kan være en pasient som skal ha mulighet til å legge inn reservasjon mot å dele sine ressurser til andre virksomheter og det kan være en virksomhet som har en avtale med en annen virksomhet om deling av ressurser og må styre tilgang til den andre virksomhetens ressurser.

En *ressurseier* er ansvarlig for tilgangskontroll av brukerforespørsler for tilgang til ressursen. Ressurseier kan delegere dette ansvaret. Ved tilgangskontroll må det gjøres en tilgangsbeslutning om brukeren skal gis tilgang til ressursen. En tilgangsbeslutning benytter tilgangsregler for å bestemme dette.

En *tilgangsregel* kan være at brukeren er autorisert for å få tilgang til å lese ressursen. Tilgangsregler baserer seg på attributter om brukeren. Dette kan være fødselsnummer, navn, arbeidssted, rolle, helseautorisasjon osv. Attributter er egenskaper om brukerens identitet. Attributtene kan være lagret i ulike informasjonskilder og koblet sammen ved hjelp av felles ID som i Norge er fødselsnummer. Identitetstilbydere forvalter brukerens identiteter og må godkjenne brukerens identitet før den kan autentisere brukeren. Ressurseier har tillit til at identitetstilbyder forvalter og autentiserer brukernes identitet korrekt.

7 Referansearkitektur for datadeling

En arkitektur hvor datadeling benyttes krever ulike byggeklosser. Ved hjelp av en referansearkitektur kan man både forstå og snakke om ulike byggeklosser som må på plass i en løsningsarkitektur. Byggeklossene er generiske komponenter som kan inngå i andre komponenter eller realiseres selvstendig. Byggeklossene kan realiseres lokalt i en virksomhet, eller de kan realiseres i felles løsninger som enten kan være nasjonale eller et samarbeid mellom virksomheter. Ikke alle byggeklossene er obligatoriske å realisere; det vil være avhengig av konteksten de skal benyttes i.

Referansearkitekturen er først beskrevet overordnet hvor alle perspektiver rundt datadeling er inkludert. Den overordnede arkitekturen er så vist i ulike scenarioer hvor byggeklossene er satt inn i den konteksten som scenarioet skal vise.

Videre er det valgt å vise noen viktige perspektiver med datadeling. Dette er tilgangskontroll, API management og personvern.

7.1 Introduksjon til arkitektur for datadeling

Datadeling er i dette dokumentet definert som deling av strukturerte data mellom helseaktører gjennom felles ressurser eller tjenester i sanntid. Med helseaktører menes både innbyggere og virksomheter innen helse- og omsorgstjenesten, inkludert offentlige etater.

Referansearkitekturen for datadeling baseres på at datadeling håndteres gjennom tjenester som tilbys som grensesnitt. Disse grensesnittene, kalt datadelingsgrensesnitt, gjøres tilgjengelig for andre aktører gjennom bruk av webteknologi. Datadelingsgrensesnitt må støtte både lesing og registrering/oppdatering av helse- og personopplysninger. Et datadelingsgrensesnitt kan realiseres som et web-API.

Historisk har web API vært synonym med webservices (Simple Object Access Protocol (SOAP) basert), men den senere trend har medført at mange har gått fra å bruke SOAP og tjenestebasert arkitektur(SOA) til direkte «representational state transfer» (REST) baserte webressurser (RESTful API-er) og «Resource oriented Architecture» (ROA). Referansearkitekturen som er beskrevet i dette dokumentet dekker web API-er realisert som både webservices og REST. Selv om det ofte er mest fokus på det tekniske rundt web-API-ene, så er det viktig å forstå at SOA og ROA er to ulike arkitekturmønstre som ikke bare påvirker design av API-ene, men også hele løsningsarkitekturen.

SOA velges ved at en virksomhet ønsker å tilby forretningstjenester og tilgjengeliggjøre dem for andre som web API-er. Dette er også omtalt som RPC - Remote Procedure Calls. Eksempler på forretningstjenester: hent ledige timer, bestill time, avbestill time.

I en ROA arkitektur handler det om at en virksomhet ønsker å samarbeide med andre om felles ressurser (informasjon). Virksomheten som deler vil da tilby API-er for å behandle ressursene. Et eksempel er at man tilbyr å behandle ressursen Avtale gjennom en forhåndsdefinert liste med operasjoner: les (GET) som normalt henter en liste av ressurser; opprett (POST) som oppretter en ny representasjon av en ressurs; oppdater (PUT) oppdaterer en ressurs med egen id; og slett (DELETE) som sletter en gitt ressurs.

Siden REST-begrepet ikke er knyttet til en bestemt standard benyttes begrepet i en videre betydning. Det hersker derfor noe uklarhet om hva REST innebærer. Derfor er det blitt

utarbeidet en modenhetsmodell for REST-baserte API-er[5] hvor det er definert fire nivåer hvor det laveste nivået defineres som at man kun bruker HTTP som transportkanal og man benytter fortsatt forretningstjenester (RPC-kall).

Fordeler med datadeling er:

1. Bruk av datadeling i en-til-mange konsepter slik som mobile app-er og velferdsteknologi er enkelt, effektivt og skalerbart.
2. I kontrast til meldingsutveksling krever datadeling mindre overhead rundt adressering, feilhåndtering og garantert levering/transaksjonshåndtering
3. Når datadelingsgrensesnitt er implementert riktig vil inkludering av nye klienter være enkelt og effektivt.
4. Med datadeling vil klienten bestemme hvilken informasjon som den vil motta av tjenesten, istedenfor at avsender sender informasjonen som den tror mottaker har behov for.

Det finnes også noen ulemper med datadeling som er viktig å tenke på ved valg av løsning:

1. Datadeling er ikke løsning for alle typer integrasjonsbehov. Man må normalt kombinere datadeling med andre type integrasjonsteknikker og/eller samhandlingsmodeller.
2. Datadeling har ikke transaksjonsstøtte som koordinerer klientens transaksjoner automatisk med tjeneren sin transaksjon (distribuerte transaksjoner).
    a. Med webservices finnes det noen muligheter, men dette er lite utbredt.
    b. Ved bruk av REST finnes det ingen slike muligheter. Dette vil si at klientene selv må implementere kompenserende logikk for sine transaksjoner når feil i kall til datadelingstjenester oppstår. Spesielt er dette en utfordring når klienter må gjøre mange kall på ulike ressurser for å oppdatere tilstanden til tjeneren. Dersom disse oppdateringene ansees av klienten til å være en atomisk operasjon, må klienten selv håndtere koordineringen av alle feilsituasjoner. Et løsningsalternativ er at tjeneren åpner for at klienter kan sende inn mange ressursoppdateringer i samme kall (Bundle i FHIR), som så håndterer alle ressursoppdateringene i en transaksjon.
3. Datadeling støtter sanntidshendelser dårlig da det kun har støtte for "pull"-baserte tjenester og ikke push (fra server til klient). Dette må kompenseres med bruk av polling, oppsett av egne datadelingstjenere hos klientene eller bruk av meldingsutveksling eller andre push-teknologier (subscription).

Ved behov for datadeling må man normalt ta et arkitekturvalg om man skal basere datadeling på ROA eller SOA.

Ulikhetene mellom ROA/REST og SOA/SOAP baserte arkitekturer:

1. REST benytter forutsigbare metoder å manipulere informasjon på.
    a. Med REST kan du hente, lage nye, oppdatere og fjerne informasjon

[5] Richardson Maturity Modell for REST
https://martinfowler.com/articles/richardsonMaturityModel.html

   b. Denne måten å manipulere informasjon er svært utbredt og dermed svært enkelt for utviklere å implementere.

   c. Metodene kan også være en begrensning ut fra hva man ønsker å oppnå.

2. ROA gir klientene mer styring over implementering av hva som de trenger å implementere

   a. Når et web API fullt ut implementerer REST, vil det være mulig for klientene å manipulere alle typer ressurser som støttes. Det vil være opptil klientene hva de ønsker å støtte.

   b. Det krever langt mindre innsats hos de som tilbyr web API-ene når klientene skal legge til støtte for flere ressurser som allerede er tilbudt i et REST-API.

3. ROA gir mindre behov for dobbellagring

   a. REST baserte web API-er gir klientene små, men presise mengder informasjon som ikke gir behov for å lagre dataene lokalt hos klientene.

4. REST har støtte for flere formattyper for innhold, slik som XML og JSON.

   a. Det er normalt enklere å utvikle grensesnitt som benytter JSON.

   b. Flere applikasjoner på mobile enheter foretrekker kombinasjonen REST+JSON på grunn av raskere overføring og parsing.

5. Med SOAP er det mer effektivt å håndtere store dokumenter. Med REST må man normalt sette sammen mange ressurser til et dokument, og dette er ofte ikke REST-tjenere optimalisert for.

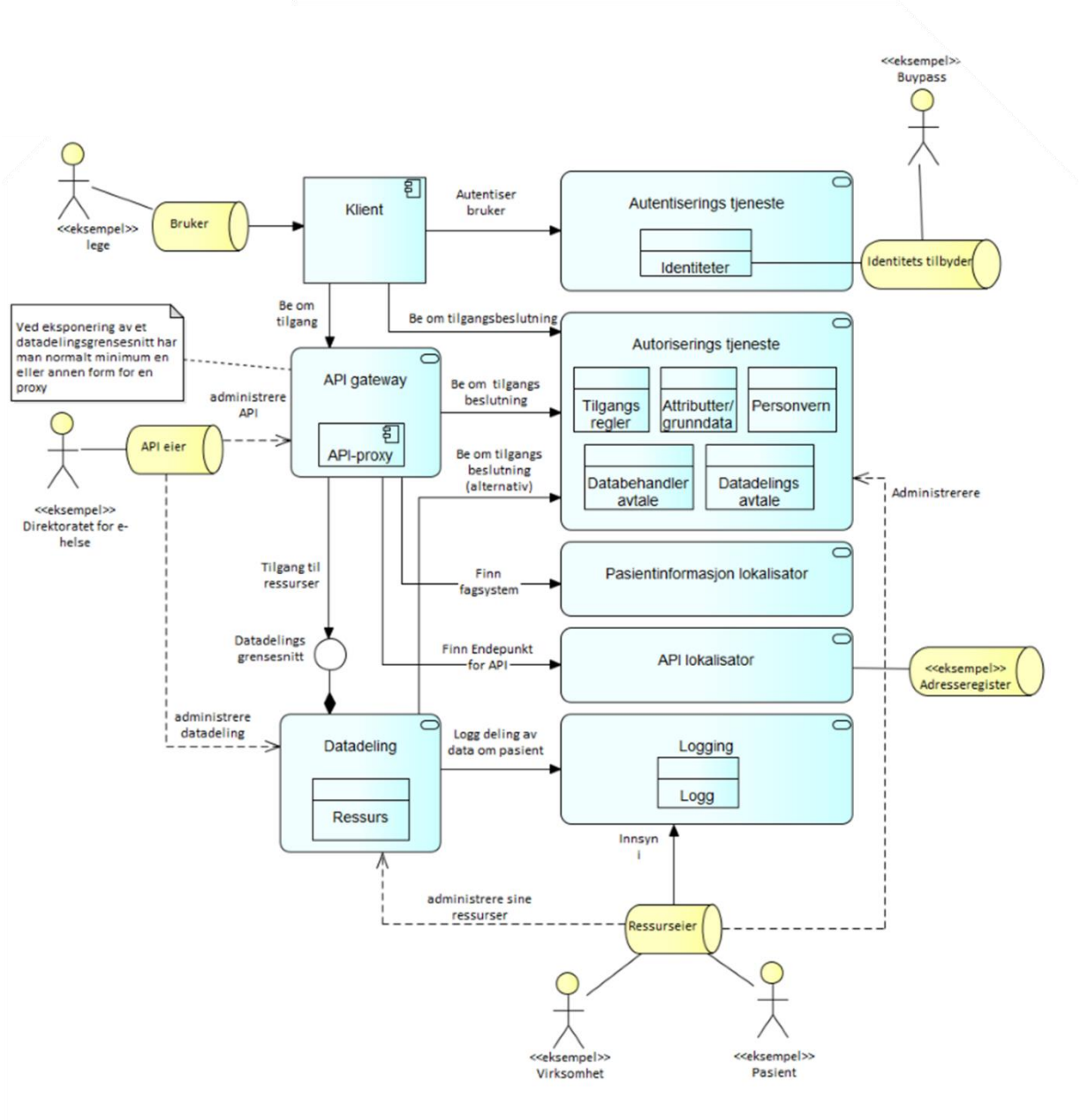
6. Med SOA kan man designe forretningstjenester hvor man legger inn mange operasjoner som eksekveres i et kall. ROA er optimalisert for kommunikasjon med små mengder data og dette vil medføre at klientene må spørre mange ganger for å oppnå ønsket måltilstand.

7. Med SOA overlater man orkestrering av operasjoner til tjeneren. I ROA overlater man orkestrering til klientene. Klienten må selv implementere logikk for å håndtere konversasjoner (flere kall for å oppnå ønsket måltilstand). Det er derfor høyere risiko for at de ulike klienter benytter REST API-ene feil eller på en ensartet måte.

8. Med "contract-first" mønster og bruk av XML er SOA med SOAP lettere å standardisere. REST er lite standardisert og det er helt opp til de som lager REST-baserte API-er hva de implementerer av støtte for operasjoner (GET, PUT, POST, DELETE), og hvilke responser og responskoder en tjener benytter. Det er også større risiko for at klienters feil bruk av et REST-API kan få uforutsette konsekvenser. Nasjonal bruk av REST baserte API-er krever standardisering. Den internasjonale standarden HL7 FHIR har langt på vei standardisert bruken av REST.

9. SOA med SOAP er mer fleksibel på design av forretningstjenester. "Ekte" REST har en sterk kobling til http-protokollen (GET, PUT, POST, DELETE) og kan virke i noen kontekster for begrensende. Hvis man har behov for å benytte tjenesteorientering med REST, så er alternativet å sende med tjenestekallet som en del av innholdet. Dette kan sies å være identisk med hvordan man gjør det innen meldingsutveksling.

7.2 Overordnet arkitektur for datadeling



Figur 6 Sentrale byggeklosser for datadeling

Figur 6 viser sentrale byggeklosser for datadeling. Figuren tar ikke stilling til om byggeklossene realiseres lokalt hos klient eller serverside, sentralt eller nasjonalt.

Det er vist noen roller og eksempler på aktører som kan tre inn i rollen. Figuren viser at pasient kan være ressurseier. Eier-begrepet her er relatert til tilgangsstyring. En pasient skal kunne sette regler på hvem som kan få tilgang til sine data. Pasienten kan da sies å være en type ressurseier over egen informasjon.

Forklaring på de sentrale byggeklosser i datadeling:

Byggekloss	Beskrivelse
Klient	Den programvarekomponenten som på vegne av en bruker ønsker å benytte et API.
Autentiseringstjeneste	Tjeneste som har som formål å sikkert identifisere brukeren. Dette vil normalt gjøres ved at brukeren ber om å logge seg inn hos en identitetstilbyder. Byggeklossen kan realiseres på mange måter, fra lokalt til nasjonalt. Ved delegering av ansvaret må API eier ha tillit til at brukere blir sikkert identifisert.
Autoriseringstjeneste	Tjenesten har som formål å bestemme hvilken tilgang klienten og brukeren av klienten skal få til API-et. Tilgang kan styres gjennom mange ulike typer regler. Eksempler: Finnes det sperringer om å dele pasientens data? Er bruker autorisert helsepersonell? Er klienten fra en virksomhet som API-eier har en avtale med?
API gateway	En inngangsport for API-et som kan styre om klientforespørsler slippes igjennom eller ikke. Vil inneholde en API-proxy som normalt er identisk med API-et. Denne byggeklossen kan tillegges ulikt ansvar, for eksempel ha ansvar for at klientene er autentisert og autorisert, eller for eksempel kun ha ansvar for transportsikkerheten (typisk en revers proxy). I noen tilfeller kan forespørsler gå igjennom flere API gateways. En API gateway kan også være en del av en API management løsning.
Datadeling	Byggeklossen som eksponerer et datadelingsgrensesnitt og har ansvar for å kontrollere at alle bruker/forespørsler er autentisert og autorisert, samt logge deling av data om pasienter. Også kalt for Ressursserver.
Datadelingsgrensesnitt	Grensesnitt som gjøres tilgjengelig for andre aktører gjennom bruk av web. Datadelingsgrensesnitt kan dekke både lesing og registrering/oppdatering av helse- og personopplysninger, og dette krever tilgangsstyring på tvers av virksomheter i tillegg til høy tilgjengelighet. Et datadelingsgrensesnitt kan realiseres som et API.
Pasientinformasjon lokalisator	Byggeklossen er tenkt å gi informasjon om hvilke virksomheter/systemer som har helseopplysninger om en pasient. Dette kan være nyttig i noen situasjoner: Situasjon 1: I dag er lagring av informasjon om pasienter desentralisert. Normalt scenario for datadeling er at de som deler, ofte samarbeider om en pasient på en eller annen måte. Det er da forutbestemt hvem som skal slå opp/oppdatere hvor. I de tilfellene hvor flere virksomheter har gått sammen, men det ikke er

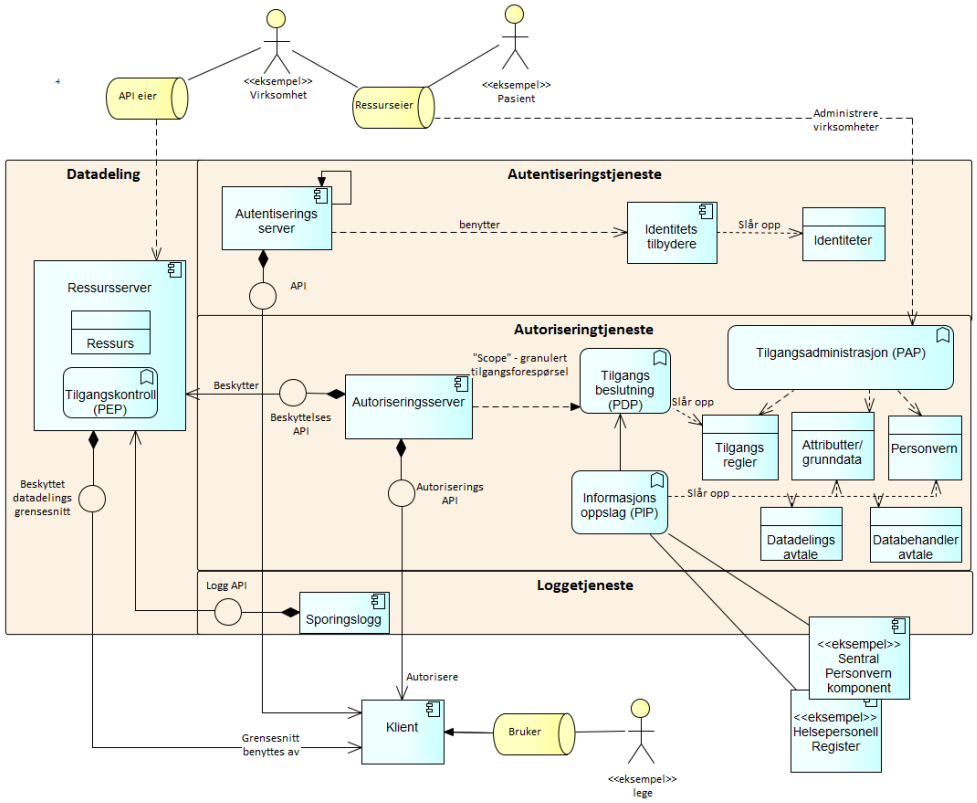
	forutbestemt hvem som "eier" pasienten eller har en pasientjournal, må de som søker etter informasjon spørre alle for å sjekke opp hvem som har pasientinformasjonen. Med denne byggeklossen kan man redusere denne kompleksiteten ved at pasientjournal lokalisator-byggeklossen gir en liste over dette. Dette krever at alle samarbeidende virksomheter implementerer identiske datadelingsgrensesnitt slik at klientene ikke trenger å forholde seg til ulike API-er. Hver virksomhet må gi informasjon til denne byggeklossen ved opprettelse av nye pasientjournaler. Situasjon 2: Hvis pasienters innsynstjenester er implementert via datadeling, må innsynstjenestene enkelt kunne spørre virksomhetene som har pasientinformasjon. Pasientjournal-lokalisator kan gi en liste over systemer som har slik informasjon og som da innsynstjenestene kan benyttes.
API lokalisator	Byggeklossen kan gi informasjon om hvordan man når et datadelingsgrensesnitt (endepunktet) og hvilke kapabiliteter det støtter. Samme funksjon som Adresseregisteret har innenfor meldingsutveksling.
Logg	Det er et lovmessig krav å logge all innsyn i en pasients journal. Denne byggeklossen dekker ansvaret for å motta hendelser om innsyn og lagre dette sikkert og slik at det er uforanderlig.

7.3 Perspektiv Tilgangsstyring

Som beskrevet i kapittel om begrepsmodell for tilgangsstyring, så sier Normen at tilgangsstyring skal dekke:

- *Autorisering som er tildeling av rettigheter til å kunne lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger*
- *Autentisering som sikrer identifisering av autorisert bruker*
- *Tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter/brukere for autorisert personell*
- *Tilgjengeliggjøring av helse- og personopplysninger til annet personell enn virksomhetens eget personell.*
- *Regulering av privat bruk av virksomhetens informasjonssystemer*
- *Kontrollerende tiltak*

Figur 7 viser referansearkitektur for tilgangsstyring når en virksomhet innen helse- og omsorgstjenesten skal tilgjengeliggjøre helse- og personopplysninger om bestemte pasienter/brukere til autoriserte personeller eller pasienten selv. I dette perspektivet er API gateway holdt utenfor.



Figur 7 Perspektiv tilgangskontroll

Byggekloss	Beskrivelse	Eksempler på realiseringer
Ressurs	I henhold til [RFC2396] kan en Ressurs være alt mulig så lenge det har en id. Konseptuelt kan man mappe en ressurs til en eller flere entiteter. I denne konteksten kan man si at ressurs er en fellesbetegnelse for en eller flere entiteter som deles med andre virksomheter/personer	Legens Kalender, Timeavtale
Ressurstjener	Tjener som har ansvaret for å tilby operasjoner på objektet samt å beskytte det.	Kjernejournal, EPJ
Beskyttet datadelingsgrensesnitt	Et webbasert grensesnitt som er tilgjengelig for andre virksomheter/personer og som er beskyttet av tilgangskontroll	
Tilgangskontroll (PEP)	Funksjon som beskytter ressursene ved hjelp av tilgangskontroll.	
Klient	Programvare som benyttes av brukeren	Tjenerapplikasjon,

	og som ønsker å benytte et datadelingsgrensesnitt.	Nettleser, Mobil app
Autentiseringstjener	Ansvarlig for å sikkert identifisere brukeren enten selv eller delegert til en identitetstilbyder.	HelseID, AD, ID-Porten
Identitetstilbyder	Utsteder og kontrollerer identiteter	Buypass, BankID
Autoriseringstjener	Sentral komponent som er ansvarlig for å gjennomføre tilgangskontrollen.	
Beskyttelses API	API som Autoriseringstjeneren tilbyr til Tilgangskontroll-byggeklossen for å håndheve tilgangsreglene for datadelingsgrensesnittet	
Autoriserings API	API som benyttes av Klienten for å be om tilgang til å kalle et datadelingsgrensesnitt.	
Tilgangsbeslutning (PDP)	Funksjon som evaluerer tilgangsreglene for et API og foretar en beslutning om tilgang basert på tilgjengelige attributter samt attributer hentet via funksjonen for informasjonsoppslag.	
Informasjonsoppslag (PIP)	Funksjon som bistår Tilgangsbeslutning med å tilføre beslutningsgrunnlaget med flere attributter slik at tilgangsregler kan bli riktig evaluert.	Personvernkomponent, HPR, RESH
Tilgangsadministrasjon	Byggekloss hvor API-eiere administrerer tilgangsregler for datadelingsgrensesnittet, pasienter administrerer tilgang til sine data, og administrasjon av grunndata om autoriserte brukere. Når virksomheter samarbeider må det også eksistere avtaler, og man skal kun gi tilgang til de virksomheter man har avtale med.	
Sporingslogg	Tilbyr API for lovpålagt logging når en virksomhet gir tilgang til en pasients helse- og personopplysninger.	

7.4 Perspektiv API gateway og Full life cycle API Management

Det overordnede perspektivet inkluderer byggeklossen API gateway. Denne kan være alt fra en reverse proxy til en del av API management løsning. API management omtales både som Application Services Governance (ASG) og Full Life Cycle API management. Gartner endret navn på konseptet i 2016 fra ASG til Full Life Cycle API management[6].

I dette perspektivet beskrives byggeklossene som utgjør konseptet i API management[7]. Arkitekturen her tar ikke stilling til hvorvidt byggeklossene realiseres internt i en virksomhet, sentralt for flere virksomheter eller nasjonalt.

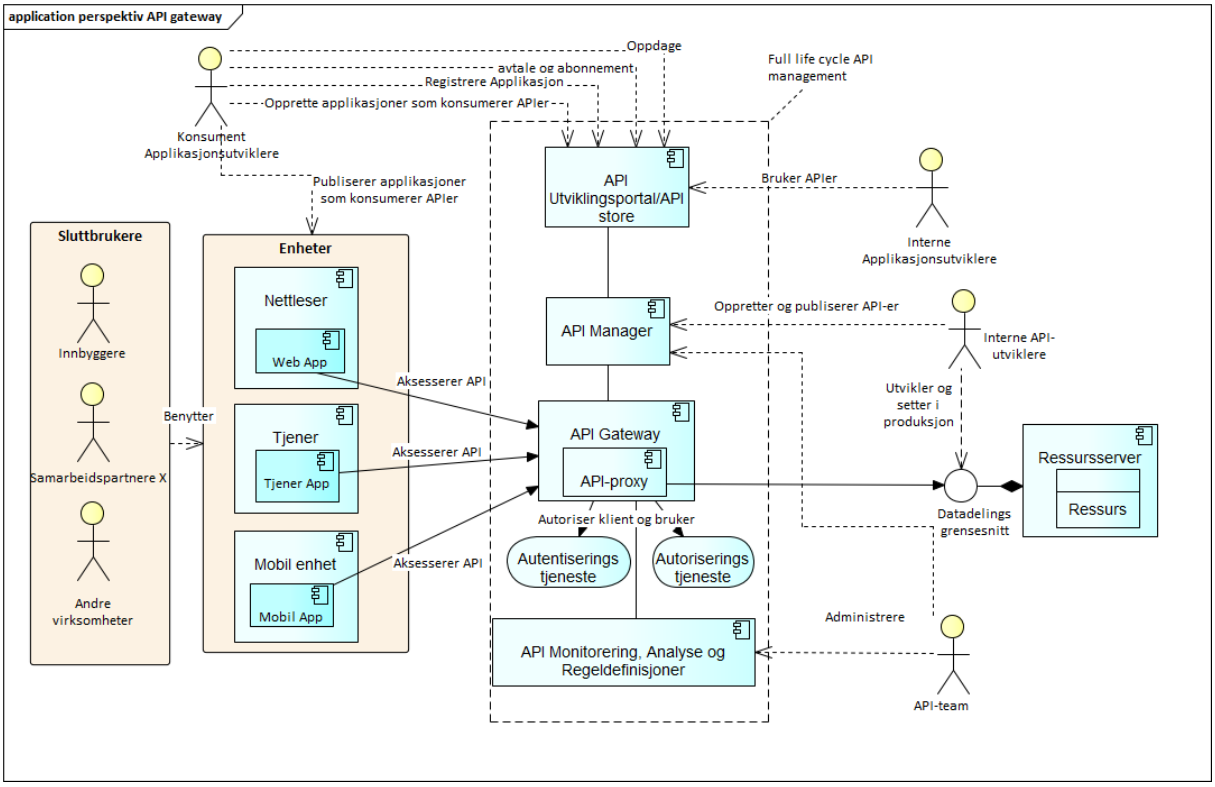
I en API management løsning vil man ha ulike klienter. I det overordnede perspektivet forenklet vi dette. Klientene kan være en applikasjon som kjører i en nettleser, en annen tjenerapplikasjon, eller en mobil enhet. Sluttbrukere kan være innbyggere, helsepersonell fra samarbeidende virksomheter eller helsepersonell fra andre virksomheter.

API management perspektivet har en kjøretidsdel og en designtidsdel. Kjøretidsdelen er det som brukes ved faktiske kall på datadelingsgrensesnittene, mens designtidsdelen beskriver det som brukes når datadelingsgrensesnittene blir utviklet samt når andre applikasjoner utvikles til å ta i bruk datadelingsgrensesnittene.

Kjøretidsdelen
Klienter vil aksessere et datadelingsgrensesnitt gjennom å kalle på API-proxyer som er realisert på en API gateway. API gatewayen vil normalt ha ansvar for å sikre bruken av datadelingsgrensesnittet slik at man kun slipper igjennom autentiserte sluttbrukere samt at de er autorisert for tilgang til datadelingsgrensesnittet (både sluttbruker og klient). Dette gjør API-gatewayen ved å benytte autentiserings- og autoriseringstjenester som beskrevet i forrige kapittel.

Et API-team vil forvalte API management-løsningen og vil ha verktøy for å overvåke trafikken gjennom API gatewayen, samt gjøre analyser av trafikkdataene.

[6] Magic Quadrant for Full Life Cycle API Management 2016
https://www.gartner.com/doc/reprints?id=1-3KZGFI4&ct=161031
[7] Inspirert av Security Reference Architecture, New Zealand Government
https://www.ict.govt.nz/guidance-and-resources/standards-compliance/api-standard-and-guidelines/api-standard-and-guidelines-part-b-technical/1-api-security/1-2-security-reference-architecture/



Figur 8 Perspektiv API gateway

Designtidsdel
API-utviklere designer, utvikler, dokumenterer og setter datadelingsgrensesnitt i produksjon på en Ressursserver. API-utviklere vil også opprette og publisere API-proxy inkludert dokumentasjon ved hjelp av API Manager-byggeklossen.

API-teamet vil definere tilgangsregler for API-et i autoriseringstjenesten og koble reglene til API-proxyen som godkjennes og gjøres tilgjengelig for sluttbrukere på API-gatewayen.

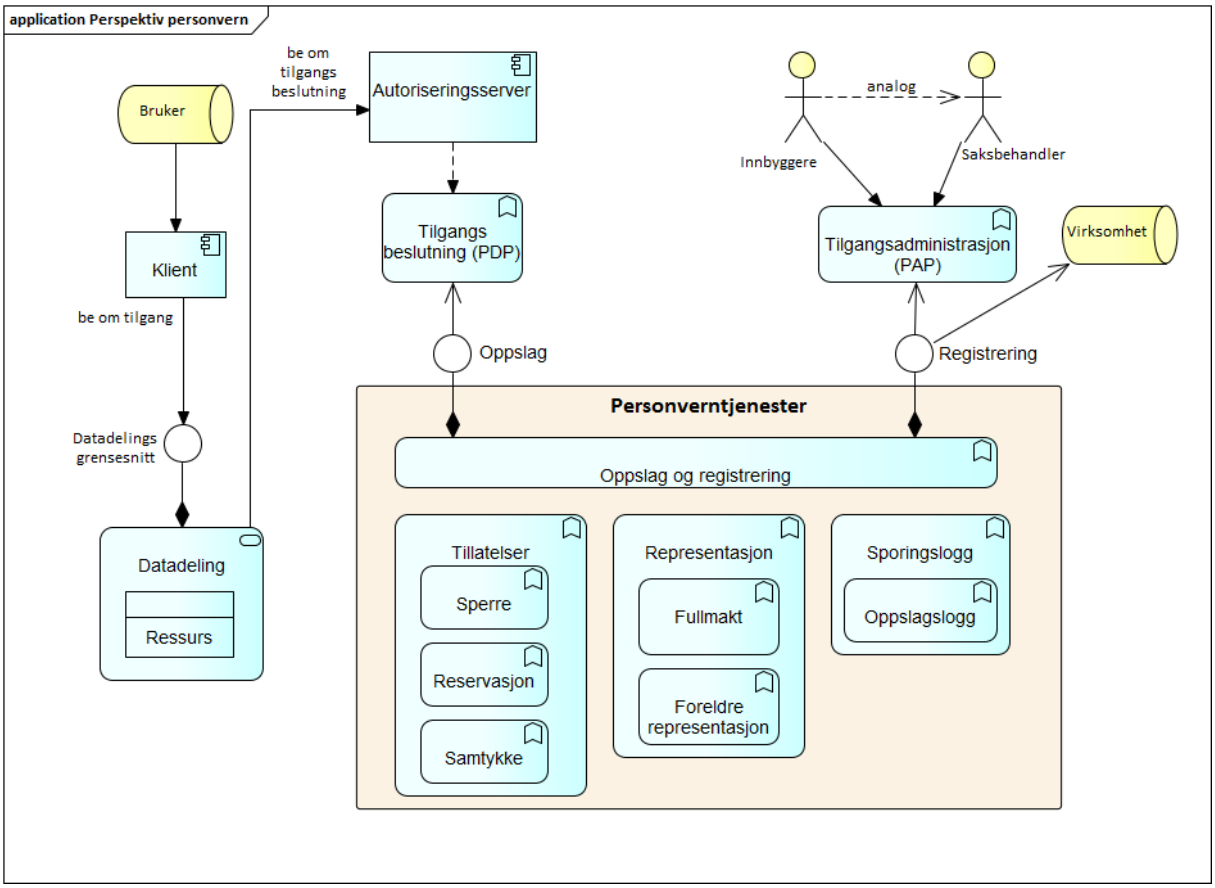
Konsument (klient) applikasjonsutviklere utvikler applikasjoner som benytter datadelingsgrensesnittene. For å få tilgang til dokumentasjon og testmiljøer må det inngås avtale og abonnement på API-utviklingsportalen. En API-utviklingsportal vil også normalt tilby testmiljøer hvor de konsumerende applikasjonene kan teste bruken av datadelingsgrensesnittene. Når de konsumerende applikasjonene skal tas i bruk, må de registreres i API-utviklingsportalen. Alle kjørende klienter som skal kalle datadelingsgrensesnitt gjennom API-gatewayen må normalt også få tilgang til å kalle et datadelingsgrensesnitt. Dette kan gjøres som en manuell eller dynamisk prosess (dette er ikke vist i Figur 8).

Byggekloss	Beskrivelse
API gateway	Vil typisk ha følgende ansvar: • 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 datadelingsgrensesnittene
API Manager	Har følgende ansvar: • Sentralisert API administrasjon og forvaltning av datadelingsgrensesnittkatalogen • Håndtering av registrerings- og introduksjonsprosesser for API utviklere • Håndtere livssyklusen til datadelingsgrensesnitt • Tilgangsstyringsadministrasjon
API Monitorering og analyse	Har følgende ansvar: • Monitorere bruken av datadelingsgrensesnitt • Generere rapporter og analyser over bruk som eventuelt kan kobles til fakturering av bruk • Konsekvensutrede versjonsendringer (oppdatere, utfase osv.)
API Utviklingsportal	Har følgende ansvar: • Håndtere abonnement og avtaler • Datadelingsgrensesnittkatalog • Informasjon om dagens bruk • Dokumentasjon av datadelingsgrensesnittene • Diskusjonsfora, support og testmiljøer

7.5 Perspektiv Personvern

I henhold til lover og forskrifter har pasienter både rett til å reservere seg mot deling av sine helse- og personopplysninger, samt sperre for innsyn for navngitte helsepersonell. Pasienter har også rett til innsyn i hvem som har sett på pasientens journal.

I all tilgangsstyring må det derfor alltid legges inn kontroll om pasienten har registrert reservasjoner eller sperringer. Denne kontrollen kan sees på som en allmenngyldig tilgangsregel som byggeklossen Tilgangsbeslutning må evaluere.



Figur 9 Perspektiv personvern

Det er virksomheten som tilbyr datadelingsgrensesnitt som er pliktig etter loven å håndheve personvernregler. For å håndheve slike regler er det behov for en personvernbyggekloss som vist i figuren over. Arkitekturen er basert på målbilde for personvernkomponent for Helsenorge.no. Byggeklossen må støtte både oppslag (en Informasjonsoppslags-byggekloss (PIP) i perspektiv tilgangsstyring) samt administrasjon av personvernregler. Hver virksomhet er selv ansvarlig for å overholde personvernet. Administrasjon av regler kan tenkes å gjøres sentralt. Ved oppdateringer sentral er det en stor verdi for pasientene at slike oppdateringer også distribueres til aktuelle virksomheter.

8 Referansearkitekturen i kjente scenarioer

Byggeklossene i en referansearkitektur kan realiseres på ulike måter. I 4.1 ble det oppsummert fem ulike hovedgrupper av datadelingsscenarioer:

1. Tilgang til helseopplysninger mellom virksomheter hvor en av virksomhetene tilgjengeliggjør helseopplysninger fra sitt lokale behandlingsrettede helseregister (jf. definisjonen i pasientjournalloven § 2 d)
2. Tilgang til og oppdatering av helseopplysninger mellom virksomheter hvor det eksisterer en databehandleravtale, eller hvor det eksisterer et samarbeid om felles journal etter pasientjournalloven § 9 hvor datadeling benyttes som teknikk for deling.
3. Tilgang til og oppdatering av helseopplysninger mellom virksomheter og en nasjonal løsning basert på pasientjournalloven §10 eller egen forskrift.
4. En innbyggers tilgang til sine helseopplysninger via bruk av f.eks. portal og mobile app-er
5. En innbyggers innrapportering og oppdateringer av sine helseopplysninger

8.1 Hovedgruppe 1: Datadeling mellom to virksomheter hvor en av virksomhetene tilgjengeliggjør helseopplysninger

Denne hovedgruppen av scenarioer forutsetter at datadeling foregår mellom to databehandleransvarlige hvor den ene tilbyr oppslagstjenester (kun lese) til den andre.

Forskrift om tilgang til helseopplysninger mellom virksomheter, § 7, stiller konkrete krav til tilgangsstyring ved tilgang mellom virksomheter. Den pålegger begge virksomhetene å ha løsninger som ivaretar at opplysningene ikke gjøres tilgjengelige dersom pasienten har motsatt seg slik tilgang, at tilgangen begrenses til det som er nødvendig og relevant for formålet, at helsepersonell er autorisert for tilgang og at de autentiseres ved bruk av sikker autentiseringsløsning.

Avtale
For denne type datadeling setter forskriften krav om at det inngås avtale på virksomhetsnivå.

Avtalepartene skal vurdere risiko for pasientens personvern som uautorisert tilgang kan føre til. Vurderingene skal minst omfatte risiko for brudd på taushetsplikt og svekket informasjonssikkerhet. Videre må de databehandlingsansvarlige i virksomhetene ha prosedyrer, systemer og journalstruktur som gir tilfredsstillende informasjonssikkerhet, og tilgangsstyring som minst ivaretar kravene i §§ 5 til 11. Tekniske muligheter for sperring av helseopplysninger samt dokumentasjon, autentisering og oppfølging, og kontroll av tilgang skal minst ivareta kravene i §§ 5 til 11.

Relevant og nødvendig helseopplysninger

Løsningene for tilgang til helseopplysninger mellom virksomheter må ivareta at helsepersonell kun skal ha tilgang til helseopplysninger som er relevante og nødvendige for å gi helsehjelp til den enkelte pasient. Begrepet "relevante og nødvendige" vil i denne sammenheng være de opplysningene som det i den aktuelle undersøkelses- og behandlingssituasjonen er behov for å ha tilgjengelig, for å kunne gi helsehjelp. Det er kun helsepersonell med tjenstlig behov som skal få tilgang til opplysningene, og de skal ikke få

tilgang til flere opplysninger enn det som er relevant og nødvendig for å kunne gi helsehjelpen.

Den tilbyende virksomhet vil ikke kjenne forholdene til den aktuelle undersøkelses- og behandlingssituasjonen hvor det er behov for helseopplysningene i den anvendende virksomhet. Dette vil si at det må være den anvendende virksomhet sitt ansvar å vurdere hva som er relevant og nødvendige helseopplysninger. Mulige løsninger hvor EPJ-løsningen kan vurdere behov for tilgang:

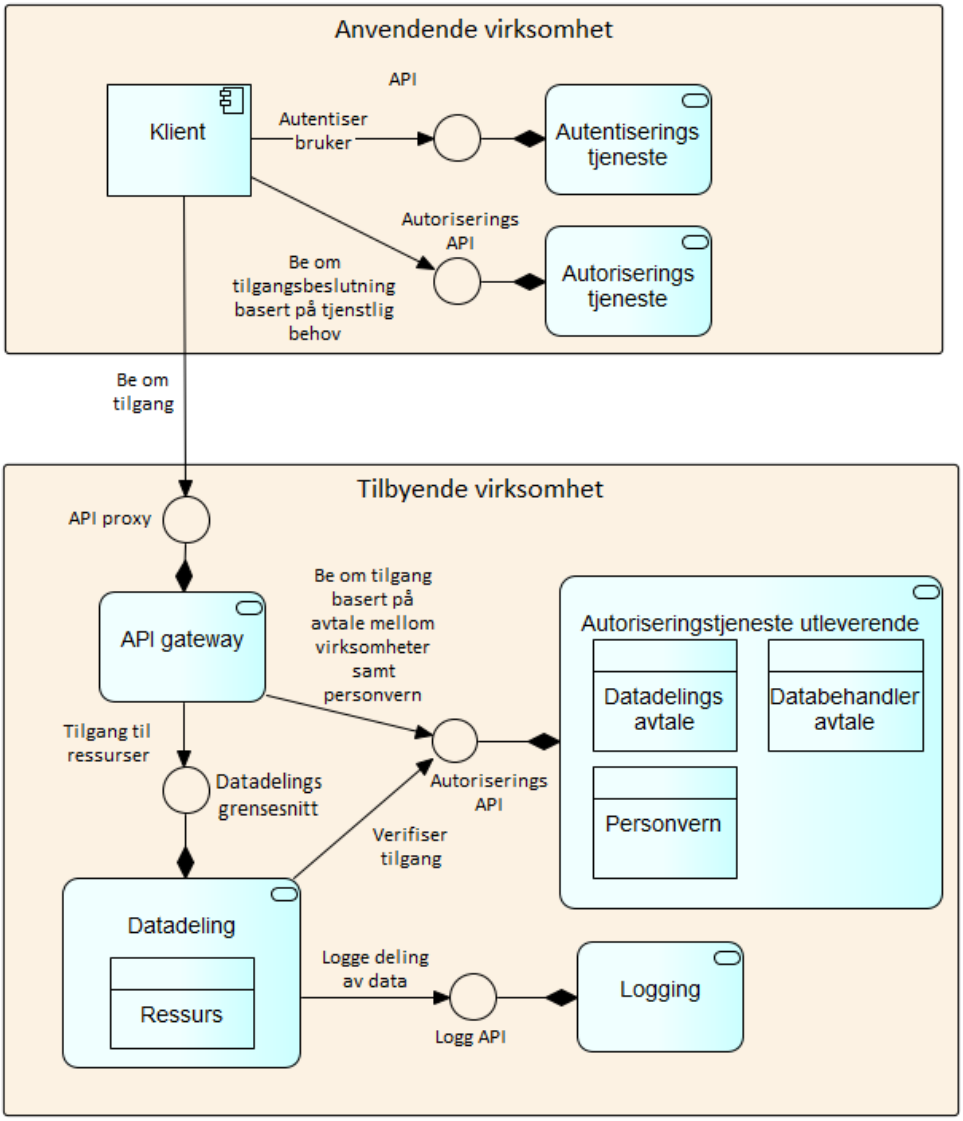
1. Finnes journal eller avtale på pasient?
2. Hvis ikke kan helsepersonell selv autorisere seg (beslutningsbasert tilgang) ved å begrunne behovet for tilgang. En slik selvautorisering skal dokumenteres ved hver bruk gjennom at:
    a. Begrunnelsen må logges
    b. Begrunnelsen må være etterprøvbar

Bruk av selvautorisering skal ha mulighet for automatisk rapportering

8.1.1 Arkitektur uten sentrale komponenter

Dette scenarioet beskriver datadeling mellom virksomheter når ingen sentrale komponenter benyttes.

Klienten hos den anvendende virksomhet må autentisere og autorisere brukeren når den ønsker å benytte den tilbyende virksomhetens API. I tillegg må klienten avklare om bruk av datadelingsgrensesnittet vil gi relevante og nødvendig helseopplysninger. Tilbyende virksomhet må autentisere og autorisere virksomheten som kaller datadelingsgrensesnittet. Autentisering av virksomhet gjøres normalt ved bruk av virksomhetssertifikater. Autoriseringsoppgaver legges normalt til en API-gateway som henter ut virksomhetens identitet fra sertifikatet, slår opp i en tjeneste som holder en liste over hvilke virksomheter man har avtale med og gjør en tilgangsbeslutning om hvorvidt virksomheten skal få tilgang. Neste steg vil så være å kontrollere personvernrelatert tilgang. Har pasienten motsatt seg datadeling? Finnes det noen sperringer på fremvisning av pasientens helseopplysninger? Tilgang til datadelingsgrensesnittet må også logges i en oppslagslogg.



Figur 10 Datadeling hos virksomheter uten sentrale komponenter

8.1.2 Arkitektur med sentrale komponenter

Figur 11 viser et eksempel hvor alle byggeklossene som kan være sentrale er trukket ut fra virksomhetene og vist som sentrale byggeklosser. Det finnes flere varianter/alternativer hvor kun enkelte byggeklosser er realisert som en sentral komponent. Figuren viser at anvendende virksomhet selv må være ansvarlig for å gjøre tilgangsbeslutning om hvorvidt en medarbeiders behov er relevant for den helsehjelpen som han/hun yter.

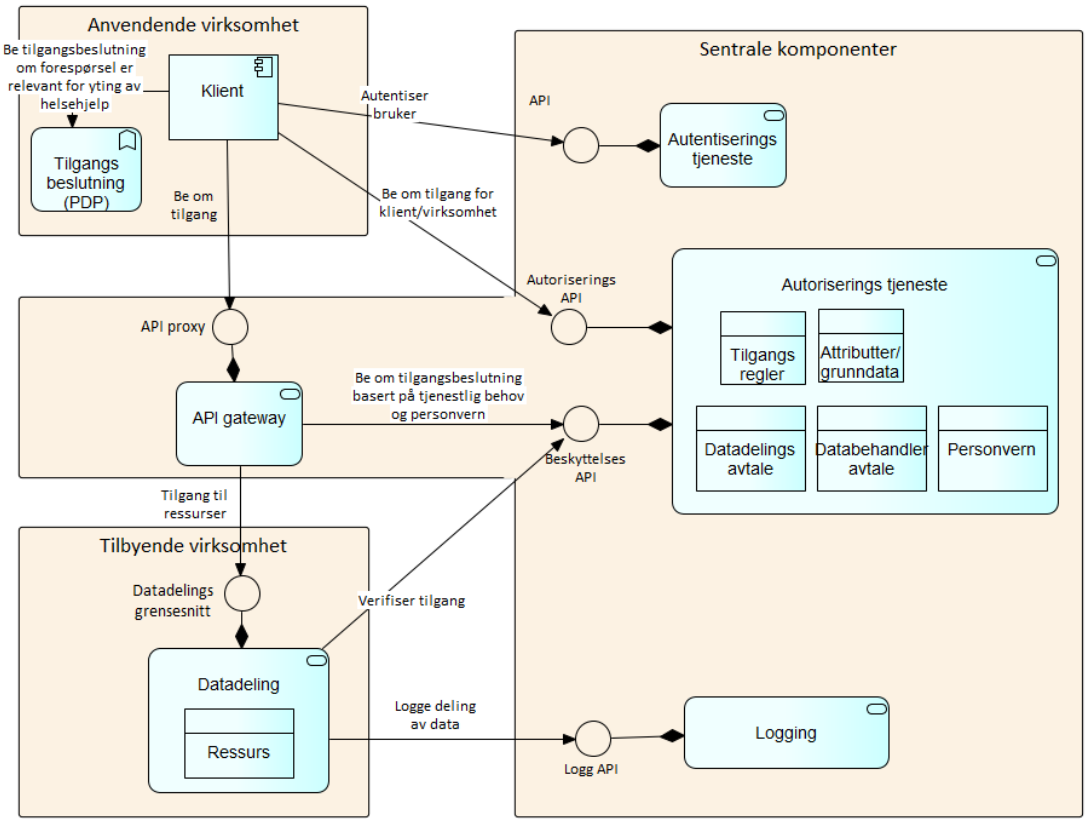
Klienten må på forhånd være registrert hos den sentrale autoriseringstjenesten og ha mottatt en hemmelig nøkkel eller utvekslet sertifikater som klienten skal benytte når den ber om tilgang til datadelingsgrensesnittet. For at klienten skal få tilgang må også et scope (omfang) være definert for datadelingsgrensesnittet, og klienten må være autorisert for dette scopet.

Bruker hos anvendende virksomhet må autentisere seg via en sentral autentiseringstjeneste og klienten motta en identitetsbillett som bevis på autentiseringen. Klienten må be om tilgang til datadelingsgrensesnittet (bruker unik klient-id samt hemmelig nøkkel). Klienten skal da

motta en tilgangsbillett. I billetten kan alle påstander være inkludert og signert av autoriseringstjenesten. Dette betyr at API-gateway i prinsippet kan gjøre en selvstendig beslutning basert hvilke scope som er godkjent av autoriseringstjenesten. Billetten kan også inneholde kun en referanse til hvor de godkjente påstandene er lagret i autoriseringstjenesten. Tilgangsbeslutningen kan også delegeres til autoriseringstjenesten hvor API gateway må spørre autoriseringstjenesten om den skal gi tilgang eller ikke.

For overholdelse av krav til personvern, kan tilbyende virksomhet delegere tilgangsbeslutningen som inkluderer evaluering av personvernregler til den sentrale autoriseringstjenesten. Dette krever at tilbyende virksomhet vedlikeholder personvernregler for sine helseopplysninger i den sentrale tjenesten.

Tilbyende virksomhet må kunne verifisere forespørsler som er sluppet igjennom av API gatewayen. Dette trenger ikke å være annet enn å sjekke gyldigheten til API-gatewayens sertifikat.



Figur 11 Datadeling hos virksomheter med sentrale komponenter

8.1.3 Eksempel på bruk av HelseID

HelseID vil støtte føderering av identitet samt autorisering av klienter. Figur 12 viser hvordan to virksomheter kan utnytte HelseID til datadeling. Autorisering av klienter kan kobles til autorisering av anvendende virksomheter, noe som er påkrevd for hovedgruppe 1-tilfeller.

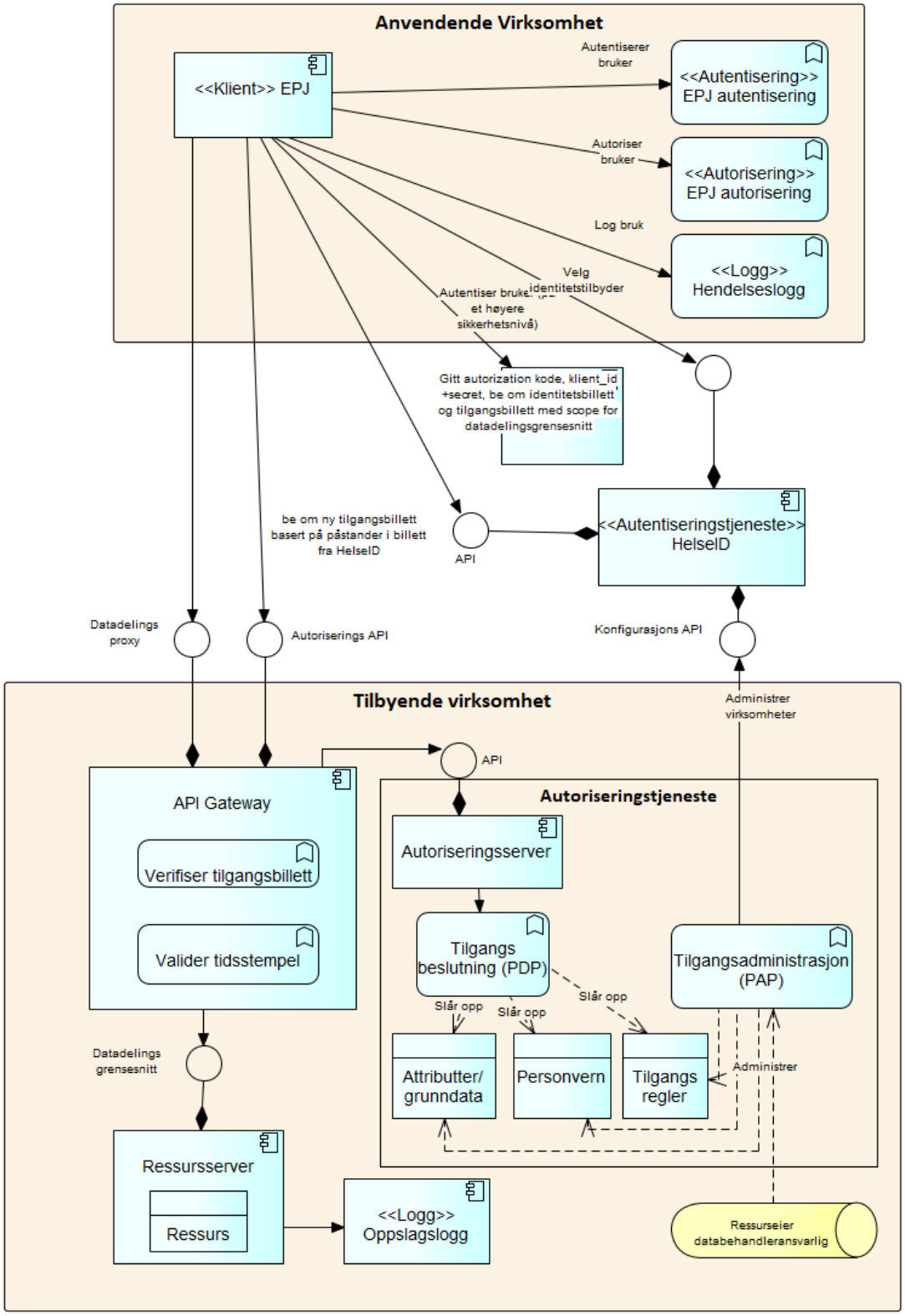
Hvordan klienter og virksomheter kobles, er foreløpig ikke avklart (hvem gjør kobling av klient id og organisasjonsnummer?). Klientautorisering forutsetter at ressurseier først konfigurerer

klienten i HelseID og tildeler klienten den hemmelige nøkkelen. Ressurseier må også konfigurere HelseID for å gi klienten tilgang til predefinerte scopes som er definert for det bestemte datadelingsgrensesnittet.

I henhold til forskrift om tilgang til helseopplysninger mellom virksomheter, skal brukere autentiseres på et høyt sikkerhetsnivå. Dersom ikke anvendende virksomhet autentiserer sine brukere på et slikt høyt nivå, eller tilbyende virksomhet ikke har tillit til autentiseringen av brukere hos anvendende virksomhet, vil det naturlig å benytte HelseID for dette. Klienten kontakter HelseID og får opp en liste med mulige identitetstilbydere (kan også være forhåndskonfigurert). Bruker velger identitetstilbyder og brukeren blir sendt videre til denne tilbyderen som autentiserer brukeren. Klienten mottar en autentiseringskode som den, sammen med klient-id og hemmelig nøkkel, presenterer for HelseID og ber om tilgang til et scope. HelseID validerer forespørsel, sjekker om klienten kan få tilgang til scopet. Dersom dette er ok, blir identitetsbillett og tilgangsbillett utstedt. Dette inkluderer godkjente påstander og scope, eventuelt en referanse til disse.

Klienten kaller deretter tilbyende virksomhet sin autoriseringtjeneste med tilgangsbillettt og identitetsbillett fra HelseID for å be om tilgang til datadelingsgrensesnittet. Denne autoriseringstjenesten må ta en tilgangsbeslutning basert på tilgangsregler satt for datadelingsgrensesnittet og personvernregler som pasienten har bedt om skal gjelde for sine helseopplysninger. Ved positiv tilgangsbeslutning utsteder autoriseringstjenesten en ny tilgangsbillett som klienten presenterer for API-gatewayen med identitetsbillett. API-gateway kan verifisere at kallet kommer fra en virksomhet med avtale samt autorisert bruker ved å sjekke at tilgangsbilletten er signert av virksomhetens autoriseringstjeneste og inneholder riktig scope.

Dersom tilgangsbilletten er gyldig slipper API-gateway kallet igjennom til datadelingsgrensesnittet.

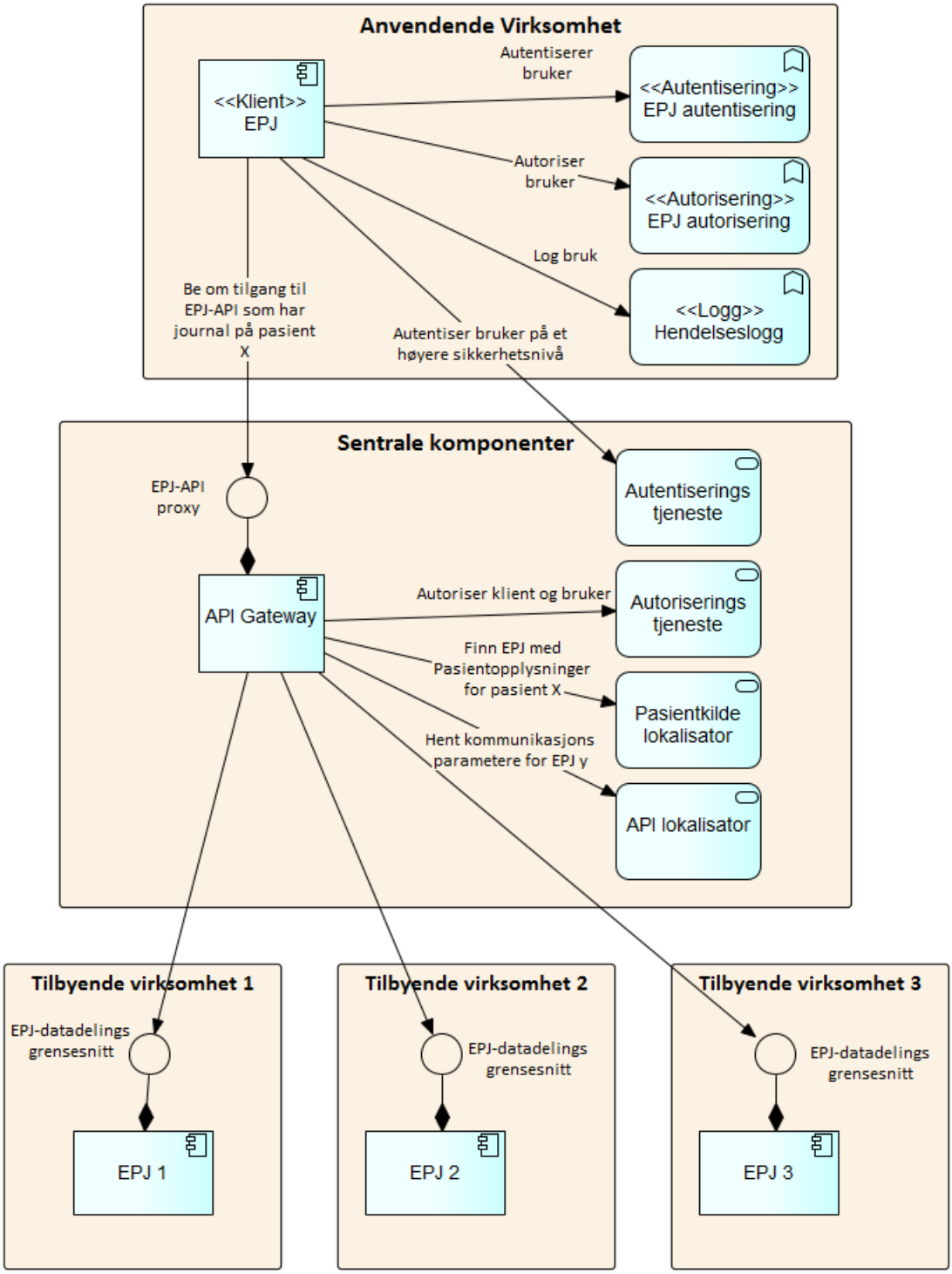


Figur 12 Integrasjon mellom to virksomheter med HelseID

8.1.4 Eksempel: Bruk av standardisert datadelingsgrensesnitt for EPJ-er med sentrale komponenter

I dette fremtidsscenarioet har EPJ-løsningene implementert et felles standardisert datadelingsgrensesnitt for å lese pasientjournaler. Informasjon om at en virksomhet har en informasjonskilde for en pasient må publiseres til Pasientinformasjonlokalisatoren, og informasjon om fagsystemgrensesnittet må være registrert i API-lokalisatoren. Da kan den sentrale API-gatewayen kalle datadelingsgrensesnittet til tilbyende virksomhet når klienten etterspør helseopplysninger om en pasient hos tilbyende virksomhet. Alle forespørsler må gå via den sentrale API-gatewayen, da det i utgangspunktet kun er API-gatewayen som kan kalle datadelingsgrensesnittet hos tilbyende virksomhet. Det forutsettes også at alle tilbyende og anvendende virksomheter har inngått avtale og oppfyller kravene til å gi og få tilgang til å lese helseopplysninger til/fra andre virksomheter.

En bruker i anvendende virksomhet har behov for å få tilgang til helseopplysninger og ber sin klient om tilgang. Klienten må autorisere bruker om den har tjenstlig behov, og om det er relevant for den helsehjelpen som bruker utfører. Siden det er krav om et høyere sikkerhetsnivå på bruk av datadelingsgrensesnittet som klienten skal kalle, må klienten sørge for at bruker blir autentisert på et høyere sikkerhetsnivå via sentral autentiseringstjeneste. I tillegg må klienten få tillatelse til å kalle datadelingsgrensesnittet på API-gatewayen ved å motta en tilgangsbillett fra autoriseringstjenesten (ikke vist i figuren). Klient kaller datadelingsgrensesnitt proxyen på API-gatewayen og ber om tilgang. API-gateway vil kontrollere tilgangsbillett og bruke identitetsbilletten til å autorisere bruker. API-gateway vil slå opp i Pasientinformasjonlokalisatoren for å finne tilbyende virksomheter som har helseopplysninger om pasienten det spørres etter. Ved treff, hentes API-informasjon fra API-lokalisator og API-gatewayen kaller det respektive datadelingsgrensesnittet hos virksomheten som har helseopplysninger om pasient. API-gatewayen signerer tilgangsbilletten og fagsystemet-en som tilbyr fagsystem-datadelingsgrensesnitt kontrollerer at kallet kommer fra API-gatewayen. I tillegg må den også verifisere at pasienten ikke har lagt inn noen personvernregler (ikke vist i Figur 13) før den returnerer helseopplysningene.



Figur 13 Eksempel - standardisert EPJ-API-arkitektur

8.2 Hovedgruppe 2: Datadeling mellom to eller flere virksomheter – samarbeid om felles journal eller databehandleravtale

I denne hovedgruppen kan virksomhetene som har inngått visse typer avtaler dele helseopplysninger. Anvendende virksomhet kan ved disse type avtaler både lese og skrive til behandlingsrettet register hos tilbyende virksomhet.

Samme type arkitektur som hovedgruppe 1 kan også benyttes for hovedgruppe 2. Eneste forskjell vil være at datadelingsgrensesnittet også må støtte oppdatering av informasjon for hovedgruppe 2-samarbeid.

Avtale om Samarbeid om felles journal
Pasientjournalloven § 9 regulerer samarbeid mellom virksomheter om behandlingsrettede helseregistre. Normen har i tillegg utgitt en veileder til bruk av denne paragrafen [6]. Den gir veiledning til etterlevelse av kravene som pasientjournalloven §9 oppstiller til avtalen mellom virksomhetene, herunder krav om hva samarbeidet omfatter, hvordan pasientens eller brukerens rettigheter skal ivaretas, hvordan helseopplysningene behandles og sikres, også ved opphør eller endring av samarbeidet og databehandlingsansvaret. Normalt vil slikt samarbeid bli løst ved bruk av felles løsning, men et slikt samarbeid kan også løses ved hjelp av datadeling. Det vil si at virksomhetene kan benytte egne applikasjoner for presentasjon av informasjonen. Eksempel kan være bruk av mobile applikasjoner hos en virksomhet og som kaller på datadelingstjenester mot en felles journal.

Et viktig prinsipp ved denne type avtaler er at samarbeidet skal erstatte behovet for egne journaler innenfor det gitte området, slik at ingen virksomheter i samarbeidet skal dobbeltlagre informasjon.

Avtale om Tjenesteutsetting
En virksomhet kan tjenesteutsette helse- og omsorgstjenester til andre virksomheter. Dette er nærmere beskrevet i Normens "Faktaark 46 - Databehandlingsansvar og avtaler i forbindelse med tjenesteutsetting" [13]. En tjenesteyter er definert som en virksomhet som har påtatt seg å utføre definerte helse- og omsorgstjenester for en annen virksomhet.

I dette faktaarket beskrives to modeller som har forskjellige konsekvenser når den databehandlingsansvarlige og tjenesteyter skal samarbeide gjennom bruk av datadeling.

- Modell 1: Virksomhet A inngår avtale om tjenesteutsetting med virksomhet B og inngår samtidig avtale om samarbeid om felles journal etter pasientjournalloven § 9 med virksomhet B. Virksomhet A beholder databehandlingsansvaret og råderett over helse- og personopplysninger som Virksomhet B behandler. Virksomhet A og B kan benytte datadeling hvor Virksomhet B kan både benytte datadelingstjenester for lesing av og skriving til den felles journalen som Virksomhet A er databehandlingsansvaret for (eventuelt omvendt).
- Modell 2: Virksomhet A inngår avtale om tjenesteutsetting med virksomhet B, men inngår ingen avtale om samarbeid om felles journal. Virksomhet B vil da være databehandlingsansvaret for de helse- og personopplysninger de selv behandler og Virksomhet A har ingen råderett over disse opplysningene. Virksomhet A kan da kun få utlevert helseopplysninger fra virksomhet B etter normale regler om utlevering av helseopplysninger i forbindelse med helsehjelp, jf. hovedgruppe 1, og kan ikke oppdatere opplysninger hos virksomhet B.

Avtale om Databehandler

I henhold til Normen er en databehandler en virksomhet som behandler helse- og personopplysninger på vegne av den databehandlingsansvarlige. Normens "Faktaark 10 - Bruk av databehandler" [14] beskriver bruk av databehandler. Det sentrale her er hva som menes med "behandling". Dette er i faktaarket definert slik:

Med behandling av helse- og personopplysninger menes enhver formålsbestemt bruk av helse- og personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Annen bruk som krever databehandleravtale er konvertering, bearbeiding, kobling mot andre registre, analyse, rapportering, test, avhending og sletting.

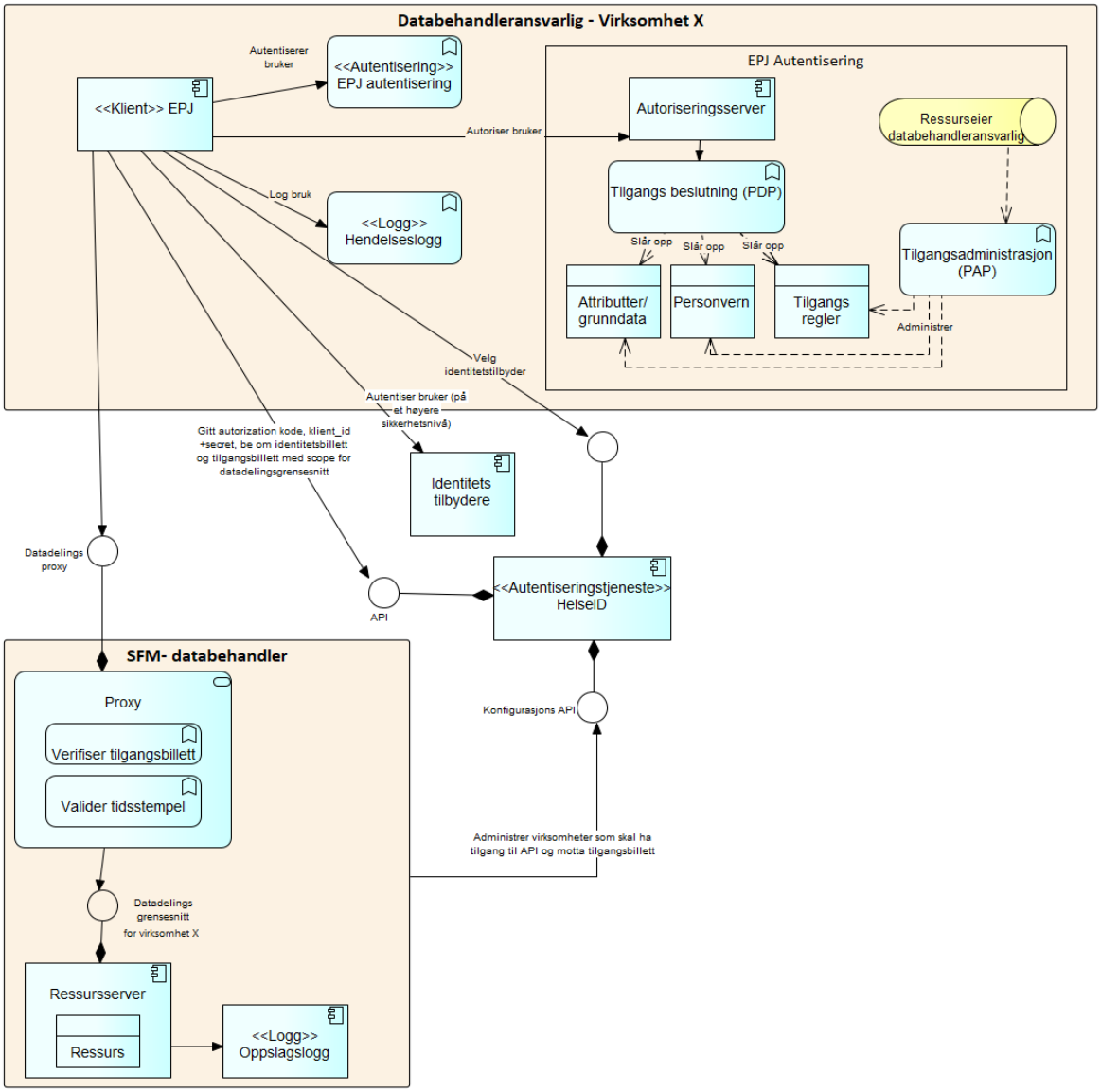
Når to virksomheter har inngått en databehandlingsavtale, kan de benytte datadelingstjenester for å dele data seg imellom. Avtalen må regulere hvilke opplysninger som databehandler kan behandle og hvordan de skal behandles. De samme regler for tilgangsstyring og informasjonssikkerhet vil gjelde for personell hos databehandleren som hos databehandlingsansvarlige.

Dersom databehandler også behandler helseopplysninger for flere virksomheter skal databehandler [14]:

ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at:

- det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering, dette både i database hvor data er lagret og i kommunikasjon

- ingen andre enn databehandleren, de som arbeider under databehandlerens instruksjonsmyndighet og virksomheten selv har tilgang til opplysningene



Figur 14 Integrasjon mellom databehandleransvarlig og databehandler med HelseID

8.3 Hovedgruppe 3: Datadeling mellom virksomheter og nasjonale løsninger.

Nasjonale løsninger som går under definisjonen om behandlingsrettet helseregister i pasientjournalloven § 2d vil etter §§ 10 og 11 behøve hjemmel i egen forskrift. Reseptformidleren og Kjernejournal er to eksempler på nasjonale løsninger, og er spesielt omhandlet i pasientjournalloven §§ 12 og 13. Nasjonal forskrivningsmodul er et annet eksempel som kan løses ved å opprette en nasjonal løsning i henhold til §10, men i dag mangler dette hjemmelsgrunnlaget.

Nasjonale behandlingsrettede helseregistre er spesielt egnet til datadeling, da de normalt tilbyr funksjonalitet som er tilgjengelig for alle virksomheter som yter helsehjelp og derfor blir sentrale, nasjonale tjenester. Datadeling er i liten grad tatt i bruk i nasjonale løsninger. For behandling av helseopplysninger har normalt portalbaserte løsninger vært hovedvalget. Her må helsepersonell logge inn i den nasjonale løsningen.

Reseptformidleren

Reseptformidleren er tilbyr tjenester som kan karakteriseres som datadeling selv om vi i referansearkitektur for meldingsutveksling har karakterisert dette som meldingsutveksling. Bakgrunnen for dette er at tjenestene Reseptformidleren tilbyr er av typen "mottak av melding", hvor selve tjenestekallet er innbakt som en del av meldingen, og ikke er eksplisitt i datadelingsgrensesnittet. Samhandlingen med Reseptformidleren er i Reseptformidlerforskriften regulert av at ulike aktørgrupper har "meldeplikt" til Reseptformidleren i forbindelse med behandling av resepter.
Tilgangsstyring er ikke direkte beskrevet i forskriften, men kan sies å være delvis regulert av §§ 2-4 og 2-6:

> *Alle meldinger som sendes Reseptformidleren, skal være elektronisk signert på den måten databehandlingsansvarlig fastsetter og i henhold til lov om elektronisk signatur. Resepter skal være signert av autorisert helsepersonell med rekvireringsrett.*
>
> *Databehandlingsansvarlig skal sikre at opplysningene som blir meldt inn og behandlet i Reseptformidleren er relevante og nødvendige for bruk til formål som nevnt i § 1-2.*
>
> *Databehandlingsansvarlig skal sikre at opplysninger som lagres i Reseptformidleren er meldt på format fastsatt av direktoratet, herunder at resepter har gyldig elektronisk signatur, jf. § 2-4.*
>
> *Dersom de innsendte opplysningene ikke er meldt i henhold til de krav som følger av første ledd og § 2-4 skal opplysningene ikke tas inn i Reseptformidleren. Dersom Reseptformidleren ved kontroll av resepter ikke kan konstatere om avsender er autorisert helsepersonell med rekvireringsrett, skal opplysningene ikke tas inn i Reseptformidleren. Reseptformidleren skal sende varsel til avsender om dette.*

Kjernejournal

Kjernejournal samler viktige helseopplysninger og gjør dem tilgjengelig som en online tjeneste for journalsystemet (EPJ-systemet) slik at helsepersonell kan få tilgang til oppdaterte helseopplysninger før en behandling starter.

Integrasjonen mellom systemene gjøres per i dag (Leveranse17.3, september 2017) igjennom:

1. En kjernejournal-webservice som tilbyr en indikasjon på hva kjernejournal for en pasient inneholder, kalt helseindikatortjenesten. Dette anses som ikke-sensitiv informasjon og bruker trenger ikke å signere forespørsel.
2. Et sett av web-grensesnitt for å åpne og lukke helsepersonellportalen som EPJ-systemet benytter igjennom en integrert nettleser
3. Klargjøring av grensesnitt med sensitiv informasjon hvor brukere må signere med personlige sertifikater samt bruk av meldingskryptering.

Kjernejournalforskriften regulerer tilgangsstyring (§ 9):

Tilgang til den nasjonale kjernejournalen skal skje gjennom autorisasjons- og autentiseringsløsningen i egen virksomhet. Hver virksomhet skal etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner for tilgang til helseopplysninger i nasjonal kjernejournal. En autorisasjon skal knyttes til en entydig identifisert person i en bestemt rolle og være tidsbegrenset.

Den som gis elektronisk tilgang til helseopplysninger i nasjonal kjernejournal skal autentiseres på et høyt sikkerhetsnivå.

Den databehandlingsansvarlige for den nasjonale kjernejournalen kan sette vilkår for tilgang, oppbevare oversikt over utstedte autorisasjoner og føre kontroll med at tilgang skjer i samsvar med reglene for tilgangsstyring.

8.3.1 Eksempel på anvendelse uten sentrale komponenter: Kjernejournal sin helseindikatortjeneste

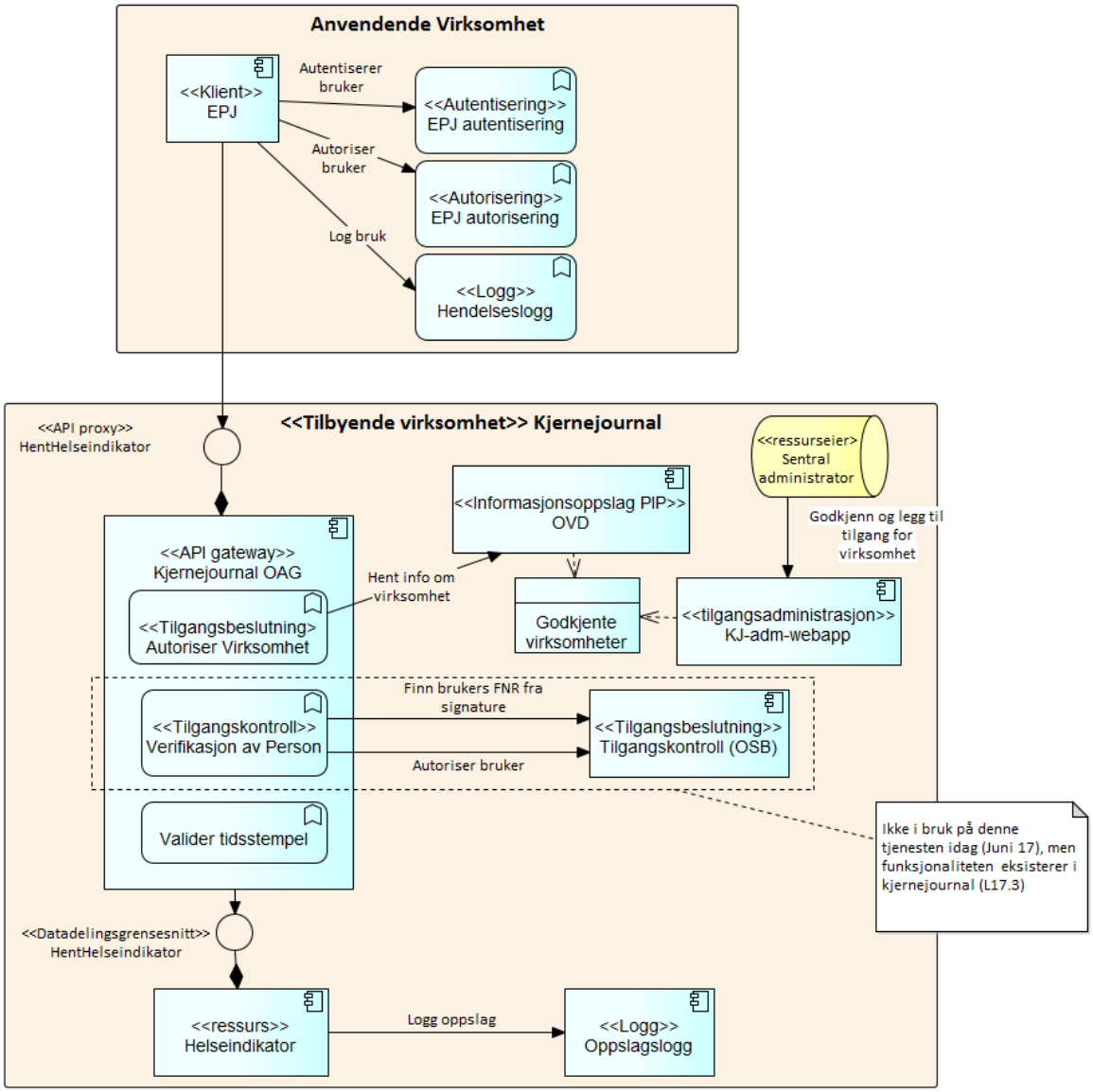
Dette er en webservice som kjernejournal tilbyr for at EPJ-systemene kan vise en status på innholdet av kritisk informasjon i Kjernejournal. Forespørsler blir signert med virksomhetssertifikater. I tillegg returnerer tjenesten en billett som EPJ-løsningen må benytte når bruker skal ha tilgang til den kritiske informasjonen i Kjernejournal. Dette foregår i dag via portalløsningen til Kjernejournal, og er ikke beskrevet i eksempelet.

Figur 15 viser løsningsarkitekturen for helseindikatortjenesten med relasjon til referansearkitekturen (<<navn>> viser relasjonen). Funksjonelt fungerer tjenesten ved at en bruker hos en virksomhet har logget seg inn i EPJ-løsningen. Autentisering av brukeren er virksomhetens ansvar. Bruker ønsker å åpne en pasients journal. EPJ-løsningen autoriserer brukeren for dette. EPJ-løsningen gjør så et kall til kjernejournal sin HentHelseindikator API-proxy.

Sikring av helseindikatortjenesten er gjort med hensyn på tre områder: Konfidensialitet, integritet og ikke-benekt. Konfidensialitet er kun sikret på transportlaget ved at tjenesten tilbys over enveis SSL fra kjernejournal. SSL-sertifikat er utstedt av Buypass. Det benyttes ikke klientautentisering for TLS (toveis SSL) eller meldingskryptering. Integritet og ikke-benekt er sikret ved tidsstempling og signering av både forespørsel fra EPJ og svar fra Kjernejournal.

Kjernejournal sin API-gateway, OAG, mottar forespørsel og autoriserer virksomheten. Dette gjør den ved at den først gjør et kall til komponenten OVD, som er en informasjonsoppslags-byggekloss for å hente informasjon om virksomheten. Deretter foretar den, basert på informasjonen, en tilgangsbeslutning om hvorvidt den skal slippe forespørselen igjennom til

selve datadelingsgrensesnittet. Det forutsettes at en administrator har lagt inn virksomheten i listen over godkjente virksomheter



Figur 15 Integrasjon mellom kjernejournal og EPJ-løsninger

I figuren er også autorisering av bruker vist. Dette er ikke i bruk i dag på denne tjenesten, men kjernejournal har støtte for dette. Bruk av denne funksjonaliteten forutsetter at bruker har signert forespørselen med en identitet som Kjernejournal stoler på. Da kan Kjernejournal hente ut sertifikat-id og benytte tjeneste hos sertifikatutsteder (IDP) for å finne brukerens fødselsnummer. Basert på fødselsnummer kan Kjernejournal gjøre en autorisering av brukeren og foreta en tilgangsbeslutning. En slik beslutning ville da ha blitt utført av komponenten "Tilgangskontroll (OSB)".
Tilgangsbeslutningene som tas i denne komponenten er (forenkling av Tilgangskontroll):

1. Gitt kildesystem og rolle til bruker: har bruker tilgang til tjenesten iht. tilgangsmatrise?
2. Har pasient lagt inn reservasjoner på deling eller visning internett?
3. Har pasient lagt inn sperringer på helsepersonell

8.4 Hovedgruppe 4: Datadeling når innbygger er mottaker av helseopplysninger

I de andre hovedgruppene er det alltid helsepersonell som er mottakere av helseopplysninger. I denne hovedgruppen er det *innbygger* som er mottaker.

En innbyggers rett til innsyn i helseopplysninger er regulert i lov om pasient- og brukerrettigheter. Kapittel 3 i loven beskriver generelle rettigheter når det gjelder rett til informasjon og medvirkning ved gjennomføring av helse- og omsorgstjenester. Kapittelet beskriver ikke spesielle krav til hvordan informasjonen skal gis: i § 3-5 heter det at "*Informasjonen skal gis på en hensynsfull måte*". § 3-2 beskriver en pasients rett til informasjon. § 3-3 om pasientens pårørendes rett til informasjon. § 3-4 om rettigheter når pasienten er mindreårig. Kapittel 5 beskriver en pasients rett til innsyn i egen journal. Regler om innsyn følger også av pasientjournalloven § 18, helsepersonelloven § 41 og personopplysningsloven §§ 18 flg.

Når innbygger benytter sin rett til innsyn i helseopplysninger digitalt kan dette skje enten via portaler slik som helsenorge.no, eller via mobile applikasjoner. Disse løsningene vil i referansearkitekturen for datadeling være klienter, og disse klientene kan benytte datadeling som samhandling for å få tilgang til innbyggerens helseopplysninger, eller for personer som innbygger har rett til innsyn for.

Datadeling her gjelder kun lesetilgang. Innbyggere har ingen rettigheter til å gjøre endringer direkte i sine helseopplysninger. Helsepersonelloven §§ 42 og 43 regulerer innbyggers rett til retting og sletting i sin journal, men dette må behandles og utføres av helsepersonell.

Behandling av helseopplysninger er regulert i lov om behandling av personopplysninger, hvor helseopplysninger er definert som sensitive personopplysninger. Paragraf 9 beskriver vilkårene for behandlingen av sensitive personopplysninger hvor en av vilkårene må være oppfylt (i tillegg til en av vilkårene i § 8). Normalt må klienten be om samtykke fra innbygger om denne behandlingen. I tillegg må klientene be om samtykke fra innbygger om at den kan be om tilgang til helseopplysninger i andre virksomheter. Et slikt samtykke bør utformes til å være tidsbegrenset og avhenge av hvilken informasjon som gis til innbygger

Innbygger må identifisere seg på et høyt sikkerhetsnivå hos en identitetstilbyder som tilbyende virksomhet har tillit til for at virksomheten skal dele helseopplysninger.

Hvis innbygger skal ha innsyn i andre pasienters helseopplysninger, må innbygger ha lovmessig rett til innsyn, for eksempel ved at det finnes en fullmakt fra pasienten eller at, hvis innbygger er pasientens foresatte og pasient er mindreårig.

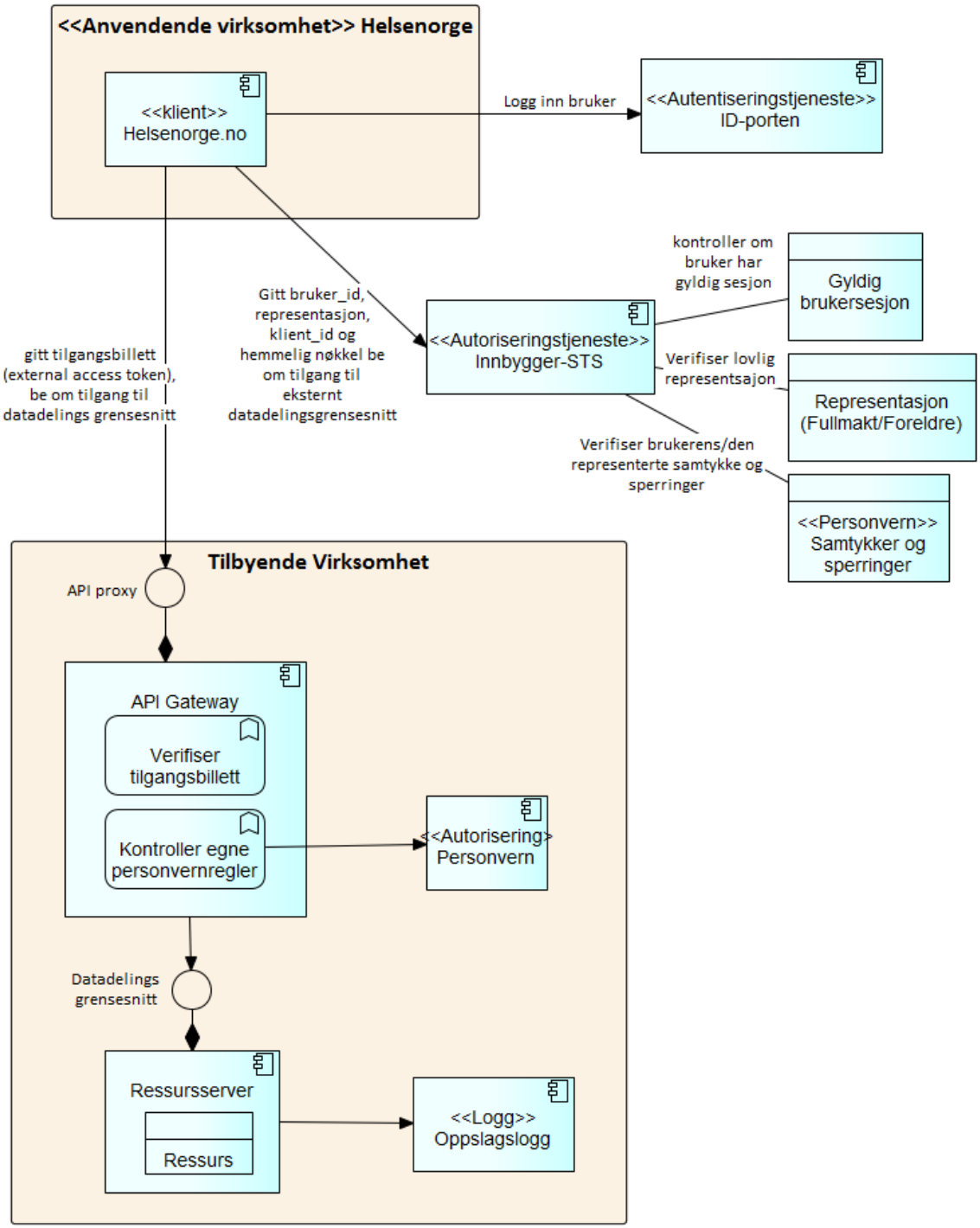
8.4.1 Eksempel: Innsynstjenester på Helsenorge.no

Helsenorge.no tilbyr mange typer innsynstjenester slik at innbygger kan se helseopplysninger om seg selv eller den han/hun representerer. Alle brukere må logge seg inn via ID-porten for å bruke tjenestene, og det blir da opprettet en gyldig brukersesjon i Helsenorge.no. Dersom en bruker kan representere andre personer, vil det være tilgjengelig funksjonalitet slik at bruker kan velge å representere andre enn seg selv.

Innbygger kan administrere sine personvernregler på Helsenorge.no. Slike regler må det tas hensyn til ved innsynstjenester. Hvis en innbygger representerer en annen pasient, er det denne pasientens personvernregler som gjelder.

Når bruker velger en innsynstjeneste som krever at helsenorge.no gjør et datadelingsgrensesnitt-kall til en annen virksomhet, har dette tidligere vært løst ved at forespørselen blir signert av Helsenorge.no, og ingen informasjon om den påloggede bruker har vært sendt med. For fremtidige løsninger vil dette gjøres slik at tilbyende virksomhet kan kontrollere datadelingsgrensesnitt-forespørsler både mot brukerens personvernregistreringer, samt logge bruken av datadelingsgrensesnittet. Dette vil bli løst ved å introdusere en Secure Token Server som utsteder tilgangsbilletter for forespørsler på tilgang til eksterne datadelingsgrensesnitt (eksternt for helsenorge.no). Dette er vist som Innbygger-STS i figuren under. Når Helsenorge.no på vegne av brukeren skal kalle et eksternt datadelingsgrensesnitt, blir Helsenorge.no en klient, og må få en tilgangsbillett av Innbygger-STS med riktig tilgangsrettigheter for å få tilgang til det eksterne datadelingsgrensesnittet. Datadelingsgrensesnittet (ressursen), scopene for grensesnittet og tilgangsregler for de ulike scopene må være konfigurert i Innbygger-STS. Ved tilgangsforespørsler vil denne serveren kontrollere at bruker har gyldig brukersesjon (det vil si er innlogget via ID-porten), verifisere at brukeren eventuelt kan representere den aktuelle pasienten samt kontrollere brukers/representert pasients personvernsinnstillinger. Basert på forespurt scope og kontroller vil Innbygger-STS foreta en tilgangsbeslutning på forespørselen og utstede en signert tilgangsbillett.

Tilbyende virksomhet må ha tillit til Innbygger-STS og de tilgangsbeslutninger som den foretar, og vil kun verifisere at tilgangsbilletten er signert av Innbygger-STS samt at det er en gyldig billett. Tilbyende virksomhet har nå tilstrekkelig informasjon til selv å foreta kontroll mot sine registrerte personvernregler dersom det er relevant. Uthenting av helseopplysninger skal logges. Tilbyende virksomhet kan da logge at helseopplysninger er blitt hentet ut av pasienten selv, eller av noen som representerer pasienten.



Figur 16 Innsynstjenester Helsenorge.no

8.5 Hovedgruppe 5: Datadeling når innbygger oppdaterer eller innrapporterer helseopplysninger

Denne hovedgruppen skal dekke de brukerscenarioer der innbygger gir fra seg eller oppdaterer helseopplysninger.

Det finnes ulike situasjoner hvor innbyggere kan tenkes å gi fra seg eller oppdatere opplysninger.

En situasjon er der hvor innbyggere har rett til medvirkning og dette er regulert i lov om pasient- og brukerrettigheter. Kapittel 3 beskriver generelle rettigheter for medvirkning ved gjennomføring av helse- og omsorgstjenester. Paragraf 3-1 sier "*Pasient og bruker har rett til å medvirke ved gjennomføring av helse- og omsorgstjenester. Pasienten har herunder rett til å medvirke ved valg mellom tilgjengelige og forsvarlige undersøkelses- og behandlingsmetoder. Medvirkningens form skal tilpasses den enkeltes evne til å gi og motta informasjon*." Medvirkningens form kan være digital. Eksempler kan være å gjennomføre digital dialog mellom pasient og behandler og legge til relevante opplysninger for opplysninger som det er gitt innsyn i.

En annen situasjon er der hvor innbygger avgir medisinske opplysninger til utførende helsepersonell tilknyttet besluttet helsehjelp. Denne formen for innrapportering er ikke regulert i lovverket og er derfor ikke en plikt innbygger har. Helsepersonell må derfor innhente samtykke for deltagelse fra innbygger for slik innrapportering. Eksempler er innrapportering av helsetilstand basert på et skjema for å få informasjon om tilstand til pasienter som er hjemmeværende under rehabilitering etter utført behandling, eller innrapportering av blodtrykk fra en blodtrykksmåler som er festet til pasienten. Et eksempel på oppdatering av informasjon er kritisk informasjon i kjernejournal hvor innbyggere kan legge til helseopplysninger som innbygger ønsker skal være kjent for andre helsepersonell.

En tredje situasjon er der hvor innbygger benytter sitt personlige arkiv (PHA) for å lagre egenmålinger som innbygger på sikt kan tenkes å dele med helsepersonell.

Når innbygger oppdaterer eller innrapporterer helseopplysninger digitalt, kan dette skje via portaler slik som helsenorge.no, via mobile applikasjoner eller via velferdsteknologi. Disse løsningene vil i referansearkitekturen for datadeling anses som klienter, og disse klientene kan benytte datadeling som samhandling for å sende innbyggerens helseopplysninger til relevante systemer.

Referanser

[1] Direktoratet for e-helse, «Nasjonal e-helsestrategi og handlingsplan 2017-2022,» 2017.

[2] Norm for informasjonssikkerhet, *Faktaark 15 - Logging og oppfølging av logger,* 2018.

[3] Norm for informasjonssikkerhet, *Faktaark 20c - Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter,* 2018.

[4] Norm for informasjonssikkerhet, *Faktaark 24 - Kommunikasjon over åpne nett,* 2018.

[5] Norm for informasjonssikkerhet, *Faktaark 47 - Autorisasjonsregister,* 2018.

[6] Norm for informasjonssikkerhet, *Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter,* 2016.

[7] Norm for informasjonssikkerhet, *Veileder med avtaleeksempler ved samarbeid om felles journal.*

[8] Norm for informasjonssikkerhet, *Veileder for tilgangsstyring,* 2017.

[9] Direktoratet for e-helse, «EPJ Standard del 2: Tilgangsstyring, redigering, retting og sletting (HIS 80506:2015),» 2015.

[10] Helse- og omsorgsdepartementet, «Samhandlingsreformen i kortversjon,» 2014. [Internett]. Available: https://www.regjeringen.no/no/tema/helse-og-omsorg/helse--og-omsorgstjenester-i-kommunene/samhandlingsreformen-i-kortversjon1/id650137/.

[11] Helse- og omsorgsdepartementet, *Prop. 72 L (2013–2014) Pasientjournalloven og helseregisterloven.*

[12] IETF, *RFC2396 - Uniform Resource Identifiers (URI: Generic Syntax https://ietf.org/rfc/rfc2396.txt.*

[13] Norm for informasjonssikkerhet, «Faktaark 46 - Ansvar og avtaler ved felles journal i forbindelse med tjenesteutsetting i kommunal sektor,» 2018. [Internett].

[14] Norm for informasjonssikkerhet, «Faktaark 10 - Bruk av databehandler,» 2018. [Internett].

[15] Direktoratet for e-helse, *Samhandlingsarkitekturer i helsesektoren (HITR 1212:2018),* 2018.

[16] Direktoratet for e-helse, «Referansearkitektur for dokumentdeling,» 2018.

[17] Direktoratet for e-helse, «Referansearkitektur for meldings- og dokumentutveksling,» 2018.

Vedlegg A Sentrale begreper for datadeling

Begrep	Beskrivelse
API	API (Application Programming Interface) betegner et grensesnitt i en programvare slik at spesifikke deler av denne kan aktiveres (kjøres) fra en annen programvare. API-er finner man i mange ulike systemer. Noen eksempler er: i webbaserte systemer, i operativsystemer, i databasesystemer, og i programvarebiblioteker. Eksempler er: Microsoft Windows API, C++ Standard Template Library, Webservice API-er, REST API-er og Java API-er. Vi bruker API i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt i en programvare for andre parter. Se også Web API
Web API	API som kan nås via web. Historisk har Web API vært synonym med webservices (Simple Object Access Protocol (SOAP) basert), men den senere trend har medført at man har gått fra SOAP og tjenestebasert arkitektur(SOA) til direkte «representational state transfer» (REST) basert webressurser og «Resource oriented Architecture» (ROA). Vi bruker Web API for både SOAP-baserte API-er og REST-baserte API-er.
Standardisert API	Et API hvor innholdsformatet er basert på en nasjonal eller internasjonal standard. Eksempel kan være FHIR.
Proprietært API	Et API hvor innholdsformatet er definert av enkeltaktører
Datadelings-grensesnitt	Et datadelingsgrensesnitt er et grensesnitt som tilgjengeliggjøres av en aktør for andre aktører gjennom bruk av web
API Management / Application Services Governance	API Management er prosessen for publisering, dokumentering og overvåking av programmeringsgrensesnitt (API-er) i et sikkert og skalerbart miljø. Application Services Governance er en tilnærming som sikrer god leveranse av både API-er (gjennom en API-orientert arkitektur) og tjenesteorientert arkitektur (SOA), for å støtte forretningsstrategien bedre, raskere og på en mer effektiv måte.
REST	REST er en programvarearkitekturstil eller et designmønster bestående av retningslinjer for å skape skalerbare webtjenester. Det gjør at alle komponenter koblet til et nettverk kommuniserer med hverandre via en delt felles kommunikasjonsprotokoll kjent som Hypertext Transfer Protocol (HTTP). Representational state transfer (REST) eller RESTful Web-tjenester er en måte å sørge for interoperabilitet mellom datasystemer på internett. REST -kompatible webtjenester tillater

	spørrende systemer å få tilgang til og manipulere tekstlige representasjoner av webressurser ved hjelp av en enhetlig og forhåndsdefinert sett av tilstandsløse metoder.
RESTful API	Et RESTful /REST API er et bestemt type API som muliggjør kommunikasjon mellom separate programmer over nettet, uavhengig av teknologien de ble laget i.
Service Oriented Architecture (SOA)	Service Oriented Architecture (SOA) (på norsk: tjenesteorientert arkitektur) er en arkitekturstil som brukes for å integrere datasystemer på en mer kostnadseffektiv måte.
Økosystem	Et digitalt økosystem er et distribuert, adaptivt, åpent sosioteknisk system med egenskapene til selvorganisering, skalerbarhet og bærekraft inspirert av naturlige økosystemer. Digitale økosystemmodeller er inspirert av kunnskap om naturlige økosystemer, spesielt for forhold knyttet til konkurranse og samarbeid mellom ulike enheter.
Felles plattform	Med felles plattform menes en kombinasjon av teknologiske infrastrukturprodukter og -komponenter som forenkler tilgang for klientene gjennom at nasjonale datadelingsgrensesnitt kan aksesseres via den felles plattformen.
Profilering	Detaljert tilpassing av en standard for en gitt anvendelse, for eksempel nasjonalt eller fagområde.
Brukergrensesnitt	Kontaktflaten mellom brukeren og programvare/maskinvare.
Velferdsteknologi (VFT) I Norge benyttes også begreper som m-helse, omsorgsteknologi, hverdagsteknologi, telemedisin, smarthusteknologi mv. Disse definerer delområder som omfattes av, eller er en del av, ovenstående definisjon av begrepet velferdsteknologi.	Med velferdsteknologi menes først og fremst teknologisk assistanse som bidrar til økt trygghet, sikkerhet, sosial deltakelse, mobilitet og fysisk og kulturell aktivitet, og styrker den enkeltes evne til å klare seg selv i hverdagen til tross for sykdom og sosial, psykisk eller fysisk nedsatt funksjonsevne. Velferdsteknologi kan også fungere som teknologisk støtte til pårørende og ellers bidra til å forbedre tilgjengelighet, ressursutnyttelse og kvalitet på tjenestetilbudet. Velferdsteknologiske løsninger kan i mange tilfeller forebygge behov for tjenester eller innleggelse i institusjon. Helsedirektoratet og Direktoratet for e-helse anbefaler at Personal Connected Health and Care benyttes som engelsk betegnelse for velferdsteknologi som integreres i helse- og omsorgstjenestene. *Kilde: NOU 2011:11 "innovasjon i omsorg"*
VFT-tjeneste	En helse- og omsorgstjeneste som baserer seg på en bestemt type velferdsteknologi. Eksempler: Avstandsoppfølging, (Elektronisk) Medisindispenser, Trygghetsalarm, GPS lokalisering osv.

Avstandsoppfølging	En VFT-tjeneste basert på teknologiløsninger for medisinske egenmålinger, typisk i form av en app (på nettbrett eller mobil) som kommuniserer med ulike typer måleutstyr/sensorer. Avstandsoppfølging er en helse- og omsorgstjeneste som ytes når tjenestemottaker og tjenesteyter befinner seg på ulike geografiske steder. Tjenesten ytes ved hjelp av digital kommunikasjon av data, lyd, bilde og video.
Trygghetsskapende teknologi (Trygghetsteknologi)	Teknologi som skal muliggjøre at mennesker kan føle trygghet og gis mulighet til å bo lengre hjemme. I dette inngår løsninger som gir mulighet for sosial deltagelse og motvirke ensomhet.
Sentral hub	Sentral hub er et IT-system som administrerer, lagrer og videreformidler signaler fra flere personlige huber. Dels er dette et støttesystem for håndtering og svar på de signaler som mottas (tradisjonelt alarmmottak), dels et system for beslutningsstøtte og individuell tilpasning av regler og terskelverdier, og dels har sentral hub funksjonen å sende signaler videre – f.eks. hjemmepleie, fastlege, spesialisthelsetjenesten, pårørende, private aktører mv. *Kilde: Referansearkitektur velferdsteknologi* (https://ehelse.no/velferdsteknologi/nasjonal-referansearkitektur)
Personlig hub	Personlig hub er en personlig eller lokal enhet som befinner seg i brukerens hjem eller som brukeren bærer eller har på seg. Oppgaven til en personlig hub er å samle inn data, kontrollere enheter i hjemmet og kommunisere med en sentral hub. Personlig hub tilsvarer Application Hosting Device (AHD) i Continua Design Guidelines. *Kilde: Referansearkitektur velferdsteknologi*
Dokument	Dokument er i VFT sammenhengen et objekt som inneholder informasjon om en gitt innbygger og som håndteres som en samlet enhet. *Kilde: Referansearkitektur velferdsteknologi*
Lagringstjeneste	Tjeneste for å lagre data. *Kilde: Referansearkitektur velferdsteknologi*
Registry (referanse)	Registry eller indeks er i denne sammenhengen en oversikt over hvilke dokumenter og bilder som finnes, hva de inneholder (metadata) og hvor informasjonen er lagret. *Kilde: Referansearkitektur velferdsteknologi*
Repository (lagring)	Repository eller datalager defineres i denne sammenhengen som det fysiske stedet hvor dokumenter eller bilder lagres etter opprettelse, og hentes når de skal anvendes. Et repository har en standardisert grenseflate som gjør det mulig å aksessere den

	lagrede informasjonen. *Kilde: Referansearkitektur velferdsteknologi*
Integrasjonstjeneste	Tjeneste som kobler sammen forskjellige typer tjenester.
Enhet / sensor	Enhet er i denne sammenhengen sensorer og utstyr som benyttes til målinger eller funksjoner hos bruker eller i brukerens hjem. Enhet i denne sammenhengen er en samlebetegnelse for det som kalles TAN-, PAN- og LAN-device i Continua Design Guidelines.
Målinger	Automatiske eller manuelle målinger, bestående av måleverdier og metadata om for eksempel metode/utførelse og utstyr.
Skjema	Forhåndsdefinert eller automatisk generert skjema med felter for å etterspørre informasjon.
Varsel	En melding til bruker av system om en hendelse basert på regler, for eksempel feilmeldinger, måleverdier utenfor normalområde.
Behandlingsplan	Målrettet, individuelt tilpasset behandling, og en vurdering om pasienten trenger oppfølging. *Kilde: https://sykepleien.no/forskning/2004/04/individuelle-planer-og-behandlingsplaner*
Egenbehandlingsplan	Behandlingsplan der pasienten selv følger opp behandlingen, for eksempel ved forverring av helsesituasjon.
Responssenter-løsning	IT-løsning som benyttes som verktøy for responstjenesten. Responssenterløsning er en teknisk løsning som brukes for å betjene et responssenter, og brukes for å vise at et responssenter både består av en løsning og en organisasjon med prosesser, ressurser og avtaler. *Kilde: Referansearkitektur velferdsteknologi*
Responssenter-personell	Responssenterpersonell er personene/organisasjonene som betjener responssenteret *Kilde: Referansearkitektur velferdsteknologi*
Responstjeneste (Responssenter-tjeneste)	Funksjon med ansvar for å overvåke og følge opp brukers situasjon, og iverksette nødvendige aksjoner ved behov. Responssentertjeneste er den tjenesten som responssenterpersonellet yter ved hjelp av en responssenterløsning og definerte arbeidsprosesser. *Kilde: Referansearkitektur velferdsteknologi* Responssentertjeneste er en tjeneste som tar imot, vurderer, dokumenterer og responderer på varsler fra velferdsteknologiske

	løsninger som tjenestemottakeren benytter. Utførende tjeneste er en tjeneste som bistår tjenestemottakeren når responssentertjenesten mener det er behov for bistand der hvor tjenestemottakeren befinner seg.
Velferdsteknologisk responssenter	Velferdsteknologisk responssenter er det første kontaktpunktet for brukeren inn i den velferdsteknologiske tjenesten, i en driftsfase. Det er responssenteret som mottar informasjonen fra enheter og personlige hub'er ute hos brukeren, som kommuniserer direkte med brukeren og beslutter videre aksjoner. Et responssenter kan inneholde en sentral hub for å motta og behandle signaler fra enheter og brukere, men vil i tillegg omfatte organisasjonen som må til for å håndtere oppfølgingen av brukerne. *Kilde: Referansearkitektur velferdsteknologi*
Skytjeneste (Cloud computing)	Samlebetegnelse på alt fra dataprosessering, datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. *Kilde: Datatilsynet* *https://www.datatilsynet.no/regelverk-og-skjema/veiledere/skytjenester---cloud-computing/hva-er-nettskytjenester/*
Tilgangsstyring	Sikre at helse- og personopplysninger kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere (ESS: og system) autentiseres på en betryggende måte og at tilganger tildeles administreres, kontrolleres og fjernes. *Kilde: Norm for informasjonssikkerhet - Faktaark nr 14 Tilgangsstyring*
Autentisering	Kontrollere en person eller et systems identitet. *Med "autentisering" menes i Normen prosessen som gjennomføres for å bekrefte en påstått identitet.*
Autorisering	Å tildele en person eller et system tilgang og rettigheter til informasjon eller andre systemer.
Trygghetsalarm	En VFT-tjeneste basert på teknologiløsninger for å utløse alarm og opprette toveis taleforbindelse med responssenterfunksjonen.
Digitalt tilsyn	En VFT-tjeneste basert på kamerateknologi, med overføring av bilde og eventuelt lyd. Digitalt tilsyn kan benyttes til å utføre avtalt, planlagt tilsyn – f.eks. i form av nattlig sjekk, som erstatning for fysisk tilsyn. Noen løsninger kan også fange opp uønskede hendelser, f.eks. fall, og gi varsel om dette til en responssenterfunksjon.
Smarthus	Automatisk styring av funksjoner i et hjem, som lys, temperatur,

(Smarthjem)	alarmer, ventilasjon, sensorer etc. Er gjerne koblet sammen i et felles system og styrt av regler.
E-lås	Elektronisk lås, som VFT-tjeneste er dette en teknologisk løsning som installeres hos brukere av hjemmetjenester eller i kommunale institusjoner.
Medisin- dispenser (Elektronisk)	En VFT-tjeneste basert på teknologiløsninger som automatisk varsler bruker om at det er tid for å ta medisin, utleverer medisinen samt varsler hvis bruker ikke har fått utlevert medisin i tide.
Geolokalisering	En VFT-tjeneste for å følge opp personer med kognitiv svikt, basert på teknologiløsninger for satellittbasert lokalisering og geofencing. Geofencing er å definere områder hvor det anses som trygt / OK at brukeren beveger seg på egen hånd. Ved bevegelse utenfor definert område, eller andre typer avvik, varsles responssenterfunksjonen.
SCAIP	SCAIP er en svensk standard brukt til overføring av alarmer og oppsett av taleanrop for stasjonære, digitale trygghetsalarmer. *Kilde: Referansearkitektur velferdsteknologi*
HL7	HL7 er en standardiseringsorganisasjon som lager standarder som er mye brukt i helsevesenet. Det finnes flere versjoner av standarden som har vesentlige forskjeller. De viktigste er HL7 v2.x, HL7 v3, CDA og FHIR som er under utarbeidelse. *Kilde: Referansearkitektur velferdsteknologi*
FHIR	FHIR er en ny standard som er under utarbeidelse innen HL7 (release 3 STU publisert mars 2017), for strukturert utveksling av helsedata mellom systemer og applikasjoner. FHIR er basert på teknologier som er enkle å utvikle web-applikasjoner på, som REST og JSON. *Kilde: Referansearkitektur velferdsteknologi*

Vedlegg B Internasjonale referansemodeller innen tilgangsstyring

Det finnes mange ulike internasjonale standarder for håndtering av påstandsbasert sikkerhet. De viktigste er:

- OAuth 2.0
- OpenId Connect
- User-managed Access
- XACML
- SAML
- WS-Federation

Disse er nærmere beskrevet under:

OAuth

OAuth er en svært utbredt standard for delegert tilgangskontroll som brukes av mange ledende internettjenester. Standarden brukes blant annet for å gi klienter tilgang til APIer i henhold til brukerens ønsker, og på vegne av brukeren. Den vanlige flyten i OAuth er:

1. Brukeren ønsker å benytte en applikasjon (klient) som trenger tilgang til visse ressurser som eies av brukeren.
2. Tjenesten som lagrer ressursene (ressursserver) avviser tilgangen i mangel på en tilgangsbillett, og henviser klienten til en autorisasjonsserver som kan gi tilgang.
3. Bruker får opp et brukergrensesnitt der hun autentiserer seg, for eksempel ved bruk av brukernavn og passord (vanligvis en webside)
4. Bruker får opp en side som spør om hun vil gi klienten tilgang til sine data. Bruker sier ja, og modifiserer eventuelt hvilke data klienten skal få tilgang til.
5. Klienten får en tilgangsbillett som den kan bruke med en gang eller ved en senere anledning til å få tak i brukerens data. Tilgangen gjøres på vegne av brukeren, i henhold til de tilgangene brukeren selv har bestemt at klienten skal få.

I OAuth er det en rekke konsepter som er standardisert, men det er stor fleksibilitet i implementering av standarden[8]:

Tilgangsbillett (access token): en tilgangsnøkkel som kan brukes for å få tilgang til en ressurs som er lagret på en ressursserver. En slik tilgangsbillett kan være en referanseverdi som ikke betyr noe i seg selv eller også inneholde signert informasjon om tilganger (JSON Web Token - JWT)

Scope: et sett med parametere som sier hvilken tilgang en klient har til ressurser.

Entitet: kan for eksempel være et menneske, maskin eller en tjeneste

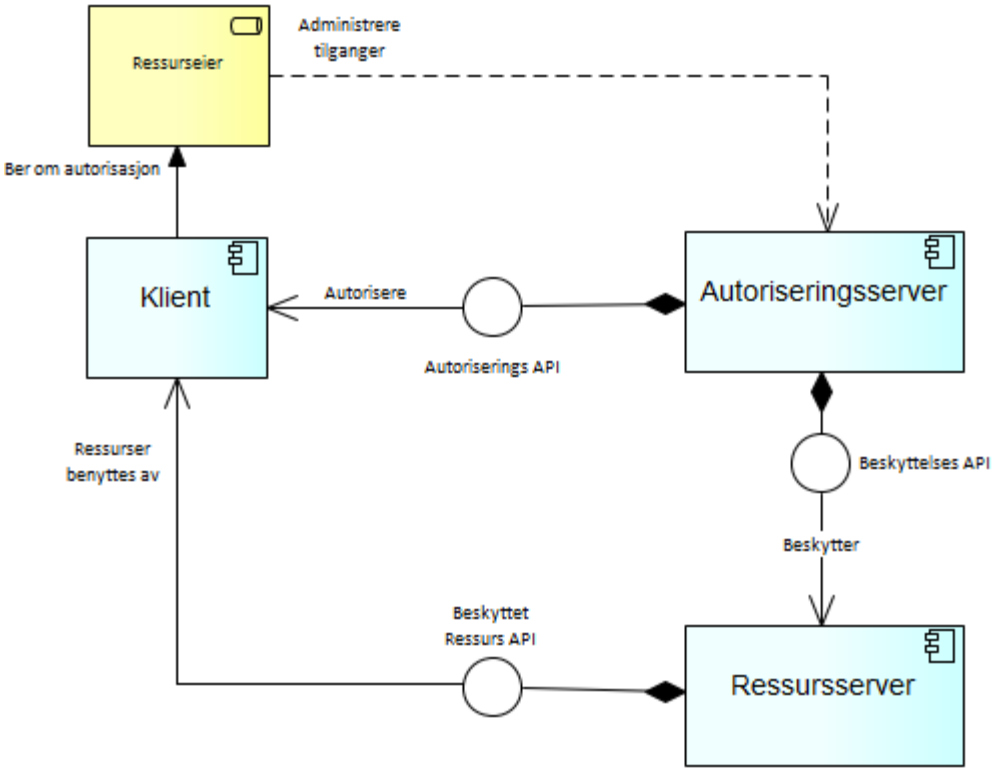
[8] The OAuth 2.0 Authorization Framework https://tools.ietf.org/html/rfc6749

Ressurseier: en entitet som kan gi tilgang til en beskyttet ressurs. En ressurseier kan være er en person, og er da vanligvis sluttbrukeren i OAuth-regimet.

Ressurstjener: tjeneren som lagrer de beskyttede ressursene og som er i stand til å akseptere og svare på forespørsler på beskyttede ressurser ved hjelp av medfølgende tilgangsbillett.

Klient: en applikasjon som foretar forespørsel etter beskyttede ressurser på vegne av ressurseier og med ressurseiers samtykke. Betegnelsen "klient" innebærer ikke noen krav til implementasjonsdetaljer.

Autoriseringstjener: Tjener som utsteder tilgangsbilletter etter å ha gjennomført en vellykket autentisering av ressurseier samt mottatt ressurseiers samtykke.



Figur 17 Referansearkitektur OAuth

Det som kjennetegner OAuth er en delegert autoriseringsflyt der ressurseier (bruker) gir sin autorisasjon til en klient gjennom formidling av en tilgangsbillett:

- Ressurstjener og autoriseringstjener er adskilte byggeklosser, som gir mulighet for gjenbruk av autoriseringstjener på tvers av flere ressurstjenere.
- Autoriseringstjener har et standardisert grensesnitt som klienten bruker for å be om og få tildelt en tilgangsbillett.
- Autoriseringstjener har et standardisert grensesnitt som ressurstjener bruker for å verifisere tilgangsbilletten. Dette grensesnittet er avhengig av type tilgangsbillett.
- Bruker og ressurseier er i hovedsak samme entitet, og er aktivt med i å bekrefte tilgangsbilletten som tildeles klienten.

- Klienten bruker tilgangsbilletten for å få tilgang til ressurser på ressurstjeneren, på vegne av ressurseier.
- Bruker og ressurseier gir klienten tilgang til sine data ved å gi et betinget og direkte samtykke i autorisasjonsøyeblikket.
- Ressurseier gir typisk kun tilgang til applikasjoner som de benytter selv eller applikasjoner som benytter ressurser på vegne av brukerne selv.
- Ressurseier delegerer “scope”-begrensende tilgang, som for eksempel skiller på lese og skriverettigheter, eller hvilke ressurser det gis tilgang til.
- En klient kjennes igjen basert på tilgangsbilletten og har vanligvis ikke egen autentisering.
- En klient kan få tilgang etter at brukeren selv er gått offline avhengig av rettighetene som ligger i tilgangsbilletten og dens levetid.
- En ressurseier kan typisk tilbakekalle tilgang ved å logge seg inn på autoriseringstjener og tilbakekalle billetter for gitte klienter.

Fordeler med bruk av OAuth som mekanisme for datadeling er:

- OAuth er svært vanlig å bruke både for interaktive internetttjenester og tilgang til API på internett
- OAuth har et fleksibelt og hensiktsmessig skille mellom ressurstjener og autoriseringstjener

Ulempene med bruk av OAuth er:

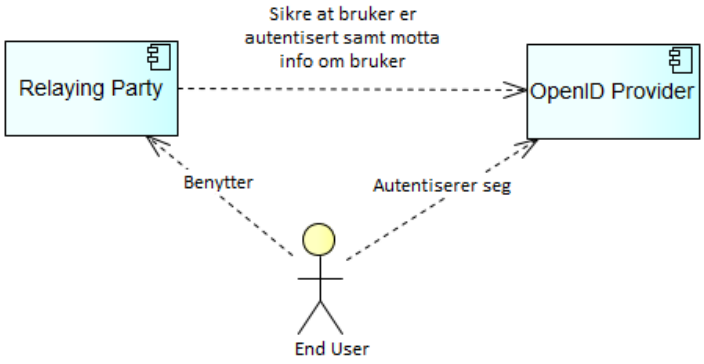
- Klientautentiseringen er implisitt i selve tilgangsbilletten og hvis noen får tilgang til denne billetten vil de også få tilgang til ressursene.
- Det er ingen klare standarder for administrering av tilganger, og dette skjer vanligvis gjennom et proprietært brukergrensesnitt på web.
- OAuth er en delegert autorisasjonsprotokoll og inkluderer ikke i seg selv en autentiseringsprotokoll. Gjennom bruk av OpenID Connect kan OAuth brukes til delegert autentisering, som gir et hensiktsmessig skille mellom autentisering, autorisering og ressursserver.
- OAuth er en svært fleksibel standard og faktiske implementasjoner spriker. Det er derfor behov for profilering og detaljering utover generell OAuth, noe som gjøres for eksempel som del av OpenID Connect og UMA

OpenID Connect

OpenId Connect er en OAuth-basert protokoll for delegert autentisering. Brukeren autentiserer seg mot en autentiseringstjener, og får tildelt en identitetsbillett som brukeren bruker til å identifisere seg mot en annen tjeneste. Teknologien gjør det mulig å skille autentisering ut fra resten av tjenesten slik at autentisering enklere kan gjenbrukes på tvers av flere tjenester. OpenID Connect sier ikke noe om akkurat hvordan brukeren autentiserer seg, men beskriver hvordan denne identiteten deles med andre tjenester på en verifiserbar måte. Løsninger kan bruke brukernavn og passord, smart-kort eller andre tofaktor autentiseringsløsninger.

OpenID Connect innfører mange begreper som verdiøker OAuth med autentisering. Noen av de viktigste er:

- **Påkrevet informasjon (claims):** informasjonselementer som en part ønsker å få fra en annen
- **Identitetsbillett (Identity token):** et strukturert dataelement som inneholder informasjon om brukerens identitet, signert av en autentiseringstjener.
- **RP (Relying party)**: en OAuth klient som krever sluttbruker autentifisering fra en OpenID tjenestetilbyder. (Identitetsforespørrer?)
- **OpenID tjenestetilbyder (OpenID provider):** en OAuth-kompatibel autorisasjonstjener som kan autentisere sluttbrukeren og utstede en signert identitetsbillett til en RP, med påkrevet informasjon som RP ba om.
- **Påloggingsdetaljer (credentials):** data som presenteres fra brukeren til et system som bevis på brukerens identitet. I OpenID connect utveksles påloggingsdetaljer med en OpenID tjenestetilbyder for å få utstedt en identitetsbillett.



Figur 18 OpenID connect

Hovedflyten i OpenID Connect er som følger. Det er antatt at en RP stoler på en OpenID tjenestetilbyder og har delegert sin autentiseringstjeneste til denne:

1. Sluttbrukeren ønsker å identifisere seg mot en RP, men ønsker ikke å gi sine påloggingsdetaljer direkte til RP.
2. RP videresender brukeren til OpenID tjenestetilbyderen.
3. Brukeren gir sine påloggingsdetaljer til OpenID tjenestetilbyder og tilbyderen verifiserer brukerens identitet.
4. OpenID tjenestetilbyderen utsteder en identitetsbillett som videreformidles til RP enten via brukeren eller direkte mellom RP og OpenID tjenestetilbyder.
5. Sluttbrukeren får tilgang til tjenesten hos RP basert på identiteten som OpenID tjenestetilbyderen har verifisert.

Hovedfordelene med OpenID Connect er:

- En delegert autentiseringstjeneste som er bygget på OAuth og som strammer inn nødvendige deler av OAuth-spesifikasjonen for å oppnå interoperabilitet mellom løsninger.

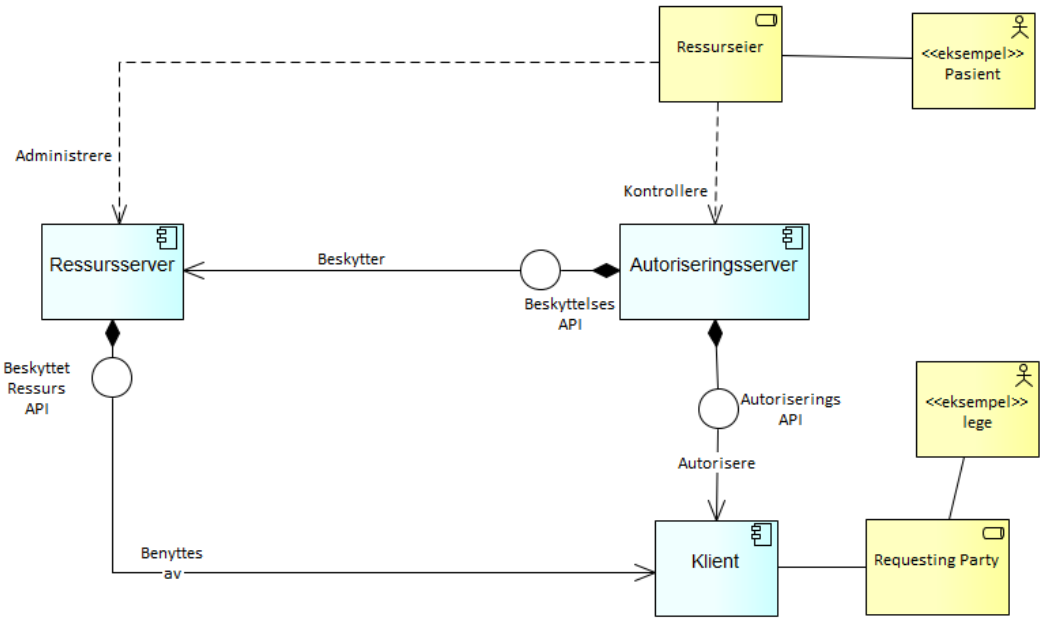
- Tjenesten gir føderert Single-sign-on (SSO) og utveksling av fakta om identiteten ved login (RP trenger ikke å kjenne til dette før login).
- Brukerne kan minimere passord sikkerhetsrisiko ved å bruke samme identitet hos mange tjenestetilbydere som støtter OpenID og har tillitt til din OpenID provider.
- Brukerne kan kontrollere hva som skal deles av fakta om sin identitet (f.eks personopplysninger) fra OpenID provider til RP.

User Managed Access

User Managed Access (UMA) er en videreutvikling av OAuth som innfører et klarere skille mellom brukerne som eier ressursene og klienten som bruker ressursene. Klienten som trenger tilgang til ressursene blir autentisert individuelt og er ikke lenger bare avhengig av å benytte en tilgangsbillett. Mekanismen gjør det mulig for en bruker å gi andre brukere eller systemer tilgang til sine sensitive opplysninger på en kontrollert måte. UMA kunne for eksempel brukes av en innbygger til å gi en lege kontrollert tilgang til spesifikke helseopplysninger er lagret i et personlig helsearkiv. Tilganger som gis gjennom UMA kan tidsbegrenses og tilbakekalles om nødvendig.

UMA-protokollen definerer en metode:

1. For en sluttbruker (resource owner)
    a. å introdusere en ressurs til en autorisasjonsserver,
    b. å definere et sett med regler og retningslinjer som styrer tilgangen til denne ressursen. Tilgangen kan også gis reaktivt basert på forespørsler fra en anmodende part, men implementasjonen av dette er utenfor spesifikasjonen.
2. For en anmodende part (requesting party)
    a. å be om tilgang til en ressurs, og få tilgang i henhold til retningslinjene som er konfigurert av ressurseier.



Figur 19 UMA referansemodell

Følgende begreper og komponenter er viktige i UMA:

- **Ressurseier:** Typisk en sluttbruker, men kan også være en virksomhet eller annen juridisk entitet som har ansvaret og eierskap for visse ressurser. I helse kan denne rollen sammenlignes med databehandlingsansvarlig. I noen tilfeller vil ressurseier være pasienten selv og i andre tilfeller kan dette være en organisasjon.
- **Ressurstjener:** en tjeneste som lagrer ressurser på vegne av en ressurseier.
- **Forespørrende part (Requesting party):** en sluttbruker eller virksomhet som bruker en klient til å få tilgang til en beskyttet ressurs.
- **Klient:** en applikasjon som gjør en forespørsel om å få tilgang til en beskyttet ressurs.
- **Retningslinjer (policy):** Konfigurasjonsparametre for en autorisasjonstjener som påvirker tilgang til ressurser.
- **Autoriseringstjener:** en tjeneste som utsteder tilgangsbilletter som kan brukes for å verifisere at man skal ha tilgang til en beskyttet ressurs.
- **Autoriserings API:** et grensesnitt for å be om og få utstedt en tilgangsbillett.
- **Beskyttet ressurs API:** et grensesnitt som brukes til å hente ut eller modifisere beskyttede ressurser i henhold til en tilgangsbillett.
- **Beskyttelses API**: et grensesnitt som brukes av en ressursserver til å blant annet verifisere tilgangsbillett.

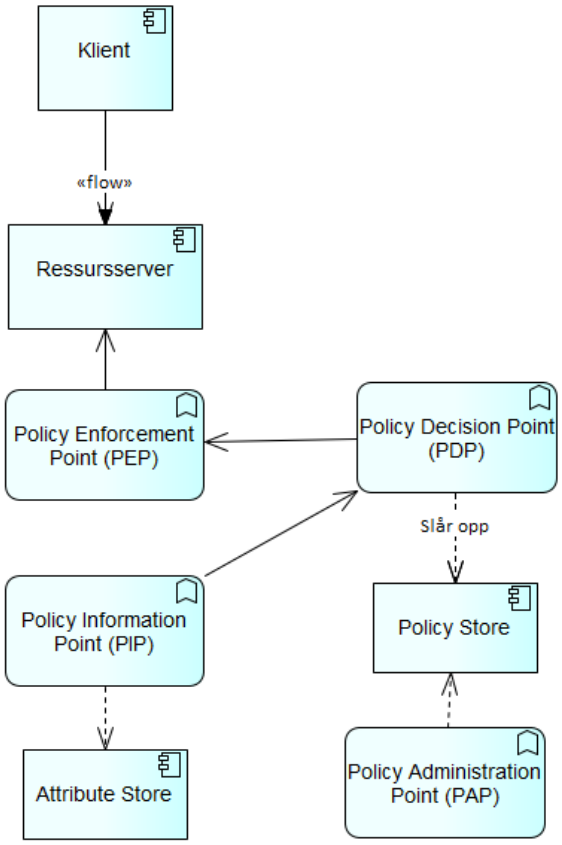
UMA er en utvidelse av OAuth som adresserer behovet for å skille mellom ressurseier og forespørrende part. I UMA kan forespørrende part autentisere seg separat og få tilgang i henhold til tilgangsregler som ressurseieren har satt opp på autoriseringsserveren. UMA representerer med dette en viktig utvidelse av OAuth som gjør den mer andvendbar til bruk i datadeling innen helse.

Fokus i UMA er på én ressurseier som setter opp regler og håndterer forespørsler om tilgang til ressurseierens ressurser, per forespørrende part. I virksomhetsbruk kan det være virksomheter som er ressurseier (databehandlingsansvarlig) for data som tilhører forskjellige pasienter og generiske retningslinjer som ligger til grunn for tilgangsbeslutningen, heller enn beslutningen til en faktisk person. I slike virksomhetstilfeller vil UMAs fokus på en faktisk person som svarer på tilgangsforespørsler ikke dekke alle brukstilfeller, og det vil være behov for at retningslinjer kan settes opp generelt for å automatisk svare på tilgangsforespørsler.

XACML

XACML[9] ble introdusert i 2003. Den definerer en konfigurerbar tilgangskontroll basert på XML som har blitt gjort til en standard av OASIS's tekniske komite. XACML validerer attributter som brukeren sender inn, og kombinerer dem med informasjon den har tilgang til. Autoriseringstjeneren kan slik ta avgjørelsen om brukeren har lov å se ressursene. XACML tar ikke ansvar for autentiseringen, men den er bare opptatt om brukerne har autorisasjon til å se ressursene

[9] http://xacmlinfo.org/2011/10/30/xacml-reference-architecture/



Figur 20 XACML referansearkitektur (http://xacmlinfo.org/2011/10/30/xacml-reference-architecture/)

XACML består av ulike komponenter:

- Policy Enforcement Point (PEP) er komponenten som utfører tilgangskontroll ved å spørre PDP om en autorisasjonsavgjørelse og deretter effektuerer tilgangsbeslutningen gjort av PDP.
- Policy Decision Point (PDP) mottar tilgangsforespørsler fra PEP-er og evaluerer aktuelle policyer og sender tilbake tilgangsbeslutninger.
- Policy Information Point (PIP) har kontroll over attributtene og hvordan slå de opp. Når PDP mangler informasjon om attributter for å fullføre evaluering av en policy, spør den en eller flere PIP-er som så henter de frem. Det er normalt at PDP'er cacher mottatt informasjon.
- Policy Administration Point (PAP) brukes til å administrere policyene som skal brukes i systemet.
- Policy Store inneholder alle policyene som blir administrert fra PAP og hvor PDP henter aktuell policy fra. Noen ganger benyttes også begrepet/komponenten Policy Retrieval Point (PRP) som et API mot Policy Store.

- Attributt Store: Her lagres attributtene om en bruker. Kan for eksempel være en LDAP eller AD osv.

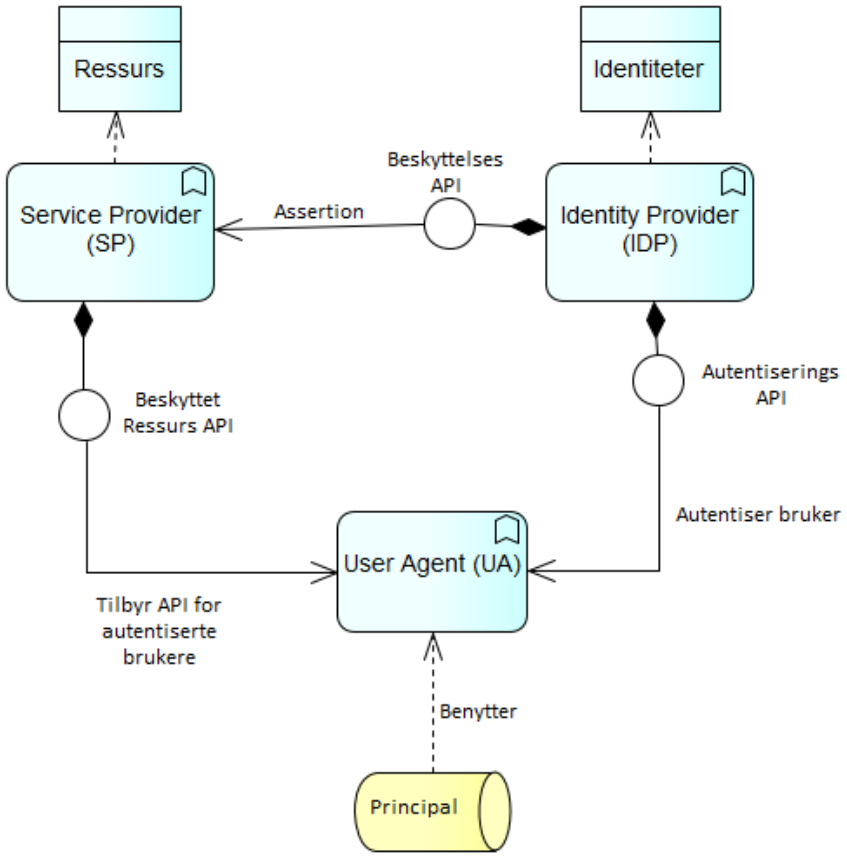
SAML

Security Assertion Markup Language er en XML standard som tillater sikre webtjenere å utveksle brukerautentiserings- og autoriseringsinformasjon. I standarden benyttes to roller, Identitetstilbyder (IDP) og tjenestetilbyder (SP). Standarden definerer en SAML assertion format som inneholder ulike attributter (påstander) og disse pakkes inn i en SAML token. Standarden har en stor utbredelse innen sikring av web-baserte tjenester og benyttes blant annet av ID-porten.

Den mest benyttede profilen av SAML er "Web Browser Single Sign-On SSO".

SAML standarden består av 3 roller:

Principal - som spør om tilgang til en tjeneste hos Service Provider
Service Provider (SP) - Har tillit til Identity Provider og etterspør bekreftelse på en identitet for Principal fra identity Provider kalt Assertion. Basert på Assertion så kan Service Provider ta en tilgangsbeslutning.
Identity Provider (IDP) - Autentiserer Principal samt utsteder Asertions til Service Provider når den mottar gyldig påstand fra Service Provider.



Figur 21 Referansemodell SAML

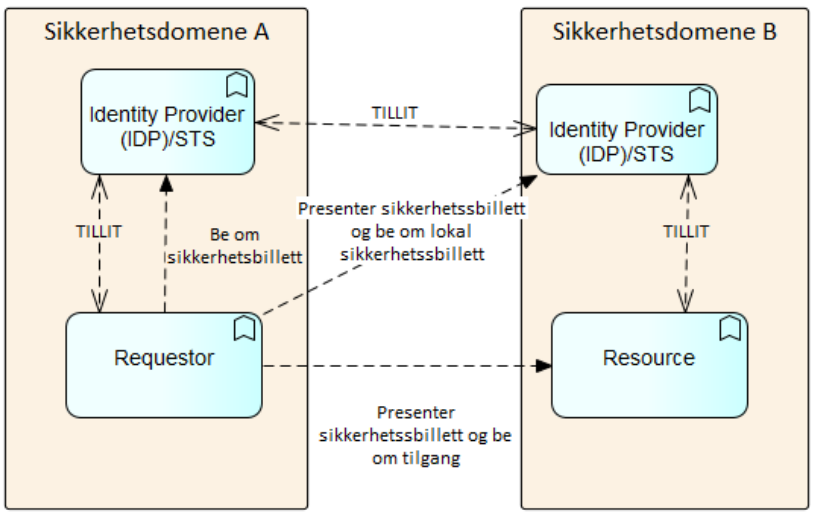
SAML er godt utbredt og er en etablert standard. Utfordringen med SAML er at det er kun Web Browser Single Sign-On SSO - profilen som er utbredt og har da kun støtte for nettleser baserte "User Agents" samt at den er XML-basert. Kommunikasjon mellom SP og IDP foregår på en sikker måte, ofte kalt en "bakkanal". ID-porten ble opprinnelig basert på SAML.

WS-Federation

WS-Federation er en standard for å føderere identiteter på tvers av sikkerhetsdomener. Føderasjon av identiteter er basert på at ulike systemer tilhører ulike sikkerhetsdomener som kan ha ulike sikkerhetsmekanismer og regler. WS-Federation bygger på WS-Security som beskriver en standardisert syntax og semantisk representasjon av sikkerhetsinformasjon, WS-SecurityPolicy og WS-Trust som beskriver et standardisert grensesnitt for en sikkerhetsbillett tjeneste (STS). WS-Federation standardiserer hvordan man kan oppnå å dele sikkerhetsressurser på tvers.

Referansemodellen er vist i figuren under. Requestor er klienten som ønsker tilgang til en Resource. En Resource er typisk enten en web server eller webservice. I Standarden så skiller man på aktive og passive Requestorer. Aktiv Requestor kan f.eks være en webservice-klient som forstår WS-Security og WS-Trust og selv håndterer dialog med STS og IDP, mens et eksempel på en passiv Requestor er en nettleser hvor WS* meldinger blir kodet inn som HTTP meldinger og som indirekte overføres mellom IDP og STS.

IDP i Sikkerhetsdomene A er identitets provider for Requester og har ansvaret for å autentisere bruker som benytter Requestor og utstede et sikkerhetsbillett. For å få tilgang til en Resource i et annet sikkerhetsdomene, må Requestor bytte sin billett til en billett som Resource aksepterer. Dette gjør den ved å presentere billetten sin til IDP i sikkerhetsdomene B. Denne har en tillit til IDP i sikkerhetsdomene A og utsteder ny sikkerhetsbillett til Requestor som den da kan benytte for å få tilgang til Resource.



Figur 22 Referansemodell WS-Federation

I motsetning til SAML kan WS-Federation benyttes av webservice-klienter som benytter webservices i andre sikkerhetsdomener. WS-Federation er en XML basert standard. WS-Federation er agnostisk til hvilken type sikkerhetsbilletter som benyttes i motsetning til SAML som krever SAML assertion baserte billetter.