

Personverntjenester

Målbilde for digitale innbyggertjenester

Publikasjonens tittel: Personverntjenester- Målbilde for digitale innbyggertjenester

Utgitt: xx

Publikasjonsnummer: IS-xxxx
[fås av Trykksaksteamet, tlf. 24 16 33 68]

ISBN-nr. xx-xxxx-xxx-x [fås av Trykksaksteamet]

Utgitt av: Direktoratet for e-helse

Kontakt: Avd. digitale innbyggertjenester

Postadresse: Pb 6737 St.Olavs plass, 0130 Oslo

Besøksadresse: Verkstedveien 1, 0277 Oslo

Tlf.: +47 21 49 50 70

Faks: 24 16 30 01

www.ehelse.no

Forfattere: Torunn Brandt, Hólmar Örn Finnsson, Siri P Johansen, Håvard Lande, Anne Beth Mannes, Harald Schmidt-Horix, Nina Linn Ulstein

Utformet på oppdrag fra: Nasjonal IKT

Versjonshistorikk

| Versjon | Dato påbegynt | Revidert av | Beskrivelse | Status |
|---------|---------------|--------------|---|----------------------------|
| 0.9 | 01.08.15 | | Rapport distribuert for kvalitetssikring av innhold | Under arbeid |
| 0.95 | 17.12.15 | | Rapport distribuert for ekstern kvalitetssikring av innhold | Under arbeid |
| 0.96 | 03.02.15 | Håvard Lande | Oppdatert sammendrag basert på innspill fra under QA | Under arbeid |
| 0.97 | 26.02.15 | Håvard Lande | Oppdater teknisk målbilde med avgrensninger | Presentert for godkjenning |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

SAMMENDRAG

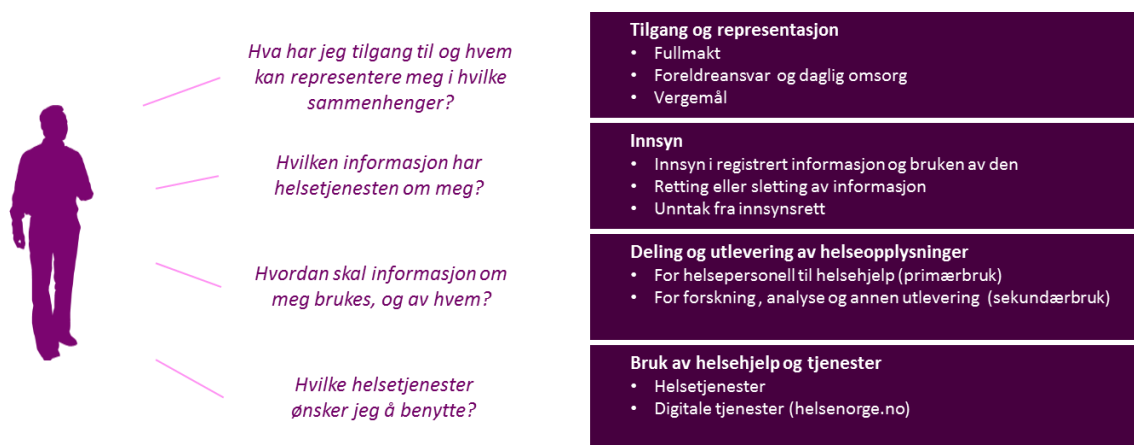
Personvern handler om innbyggers rett til et privatliv og rett til selvbestemmelse. Personvern målbildet beskriver nasjonale tjenester for å gi innbyggeren mulighet til å administrere sine personverninnstillinger og få mulighet for innsyn i sine helseopplysninger gjennom Helsenorge.no. Hovedmålet for tjenesten er å bidra til sikrere, enklere og mer effektiv håndtering av innbyggerens personvern innenfor helse- og omsorgssektoren.

Målbildet vil ha hovedfokus på digitale personverntjenester som kan tilbys gjennom helsenorger.no og i mindre grad ta for seg hvordan personvern håndteres internt i den enkelte helsevirksomhet.

Målbildet beskriver en personverntjeneste som vil

1. Fungere som en autorisasjonstjeneste for helsenorger.no
2. Tilgjengeliggjøre innbyggers personverninnstillinger for å kunne håndheve personvern gjennom etablert sikkerhetsinfrastruktur, og eksisterende løsninger for ivaretagelse av personvern og informasjonssikkerhet hos aktørene i sektoren.

I møte med helse- og omsorgssektoren avtegner det seg fire personvernområder, som illustrert i Figur 7.



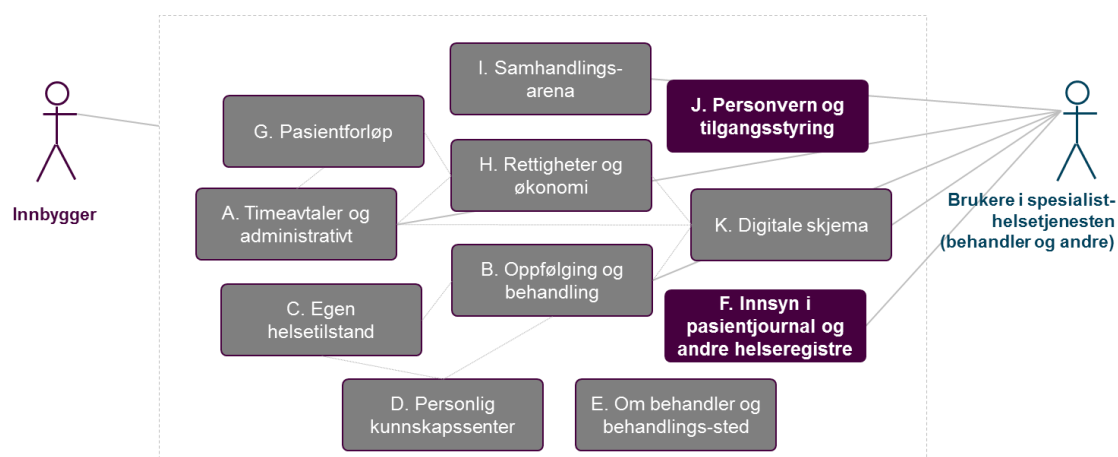
Figur 1: Personvernområder i helse- og omsorgssektoren.

Målbildet fokuserer på disse personvernområdene:

1. **Tilgang og representasjon:** Hva har jeg tilgang til og hvem kan representere meg i hvilke sammenhenger?
2. **Innsyn:** Hvilken informasjon har helsetjenesten om meg?
3. **Deling og utlevering av helseopplysninger:** Hvordan skal informasjon om meg brukes, og av hvem?
4. **Bruk av helsehjelp og tjenester:** Hvilke helsetjenester ønsker jeg å benytte?

FUNKSJONELT MÅLBILDE

Det funksjonelle målbildet for personverntjenester tar utgangspunkt i en beskrivelse av behovene som skal dekkes og vurderinger av funksjonalitet knyttet til dette. Behovene inngår som en integrert del av målbildet for *digitale innbyggertjenester for spesialisthelsetjenesten, DIS*.



Figur 2 Omfang av målbilde for digitale innbyggertjenester i spesialisthelsetjenesten, som utviklet i NIKT Tiltak 2001: Forprosjekt DIS.

Følgende behov er identifisert:

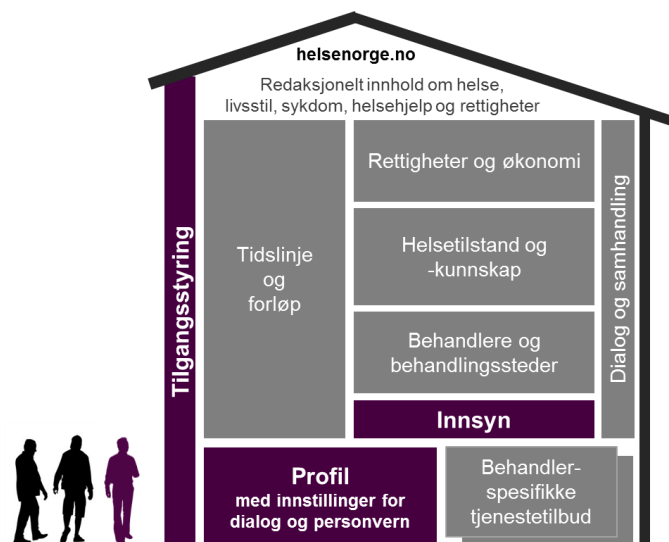
Personvern og tilgangsstyring

- Tilgangsstyring inkludert representasjon; foreldre, fullmektig
- Logg over bruk av digitale helsetjenester; historikk for personverninnstillinger
- Administrasjon av fullmakter
- Deling og utlevering av helseopplysninger
- Bruk av helsehjelp og -tjenester

Innsyn i pasientjournal og andre helserelevante registre

- Innsyn i pasientjournal
- Dialog vedrørende pasientjournal
- Brukslogg for pasientjournal
- Innsyn i helseregistre og biobanker; innhold og bruk
- Dialog vedrørende helseregistre og biobanker.

De identifiserte behovene understøttes av personverntjenester på den nasjonale helseportalen helsenorge.no, som er innbyggerens inngangsport til digital samhandling med helsetjenesten. Innbyggers personverninnstillinger vil også tilgjengeliggjøres for helsesektoren.



Figur 3: Funksjonelle komponenter realiserer innbyggers brukerflate på helsenorge.no

Helsenorge.no omfatter følgende funksjonelle løsningskomponenter knyttet til personverntjenester:

- Tilgangsstyring
- Profil med personverninnstillinger
- Innsyn

Målbildet beskriver hvordan innhold og funksjonalitet struktureres innenfor hver av disse løsningskomponentene.

Tilgangstyring:

Tilgangsstyring ivaretar innbyggers rett til å representere seg selv og andre. Dette skjer gjennom

- en personvelger i brukerflaten der innbygger kan se hvem hun/han kan representere og eventuelt velge å representere en annen
- en tjenestemodell der forutsetninger for tilgang er definert for hver enkelt tjeneste på helsenorge.no
- løpende evaluering av et regelsett for tjenestetilgang, som omfatter representasjon (foreldre, fullmektig) så vel som andre personverninnstillinger (samtykker, reservasjoner).

Profil med personverninnstillinger:

Gjennom Profilkomponenten gis innbygger anledning til å registrere sine egne innstillinger for personvern, samt overvåke bruken av dem. Dette omfatter

- fullmakter (representasjon)
 - tildelt direkte fra innbygger/fullmaktsgiver
 - tildelt på grunnlag av vergemål, fremtidsfullmakt eller andre forhold
- bruk av helsetjenester og ordninger (reservasjoner/samtykker)
 - digitale helsetjenester på helsenorge.no
 - andre programmer og ordninger
- deling av informasjon - utlevering og sperring av informasjon (samtykker/reservasjoner/sperringer)
 - primærbruk
 - sekundærbruk
- logg over bruk/historikk
 - bruk av helsenorge.no
 - endringer i personverninnstillinger.

Innsyn:

Innsynskomponenten understøtter innbyggers innsynsrett i helsetjenestens opplysninger om ham/henne i behandleres pasientjournaler så vel som i nasjonale registre, slik som kjernejournal, kvalitetsregistre og annet. Komponentene gir oversikt over hvilken dokumentasjon som finnes, og tilbyr innsyn i det enkelte registeret og bruken av det, i den grad underliggende systemer tilbyr dette. Dette vil inkludere funksjonalitet for

1. **Innsyn i innhold.** Sammenstiller en innholdsfortegnelse over innbyggers helseopplysninger, slik at innbygger kan søke, filtrere og hente fram enkeltelementer etter ønske.
2. **Innsyn i bruk.** Tilgjengeliggjør informasjon om bruken av helseopplysninger der behandlingsstedet/helsevirksomheten tilbyr dette.
3. **Dialogfunksjonalitet for retting, sletting og sperring.** Innbyggers behov knyttet til informasjon og veiledning, samt eventuelle meldinger om feilregistreringer, støttet

gjennom meldingsfunksjonalitet. Det samme gjelder anmodning om å sperre enkeltelementer i helseregisteret for helsepersonell.

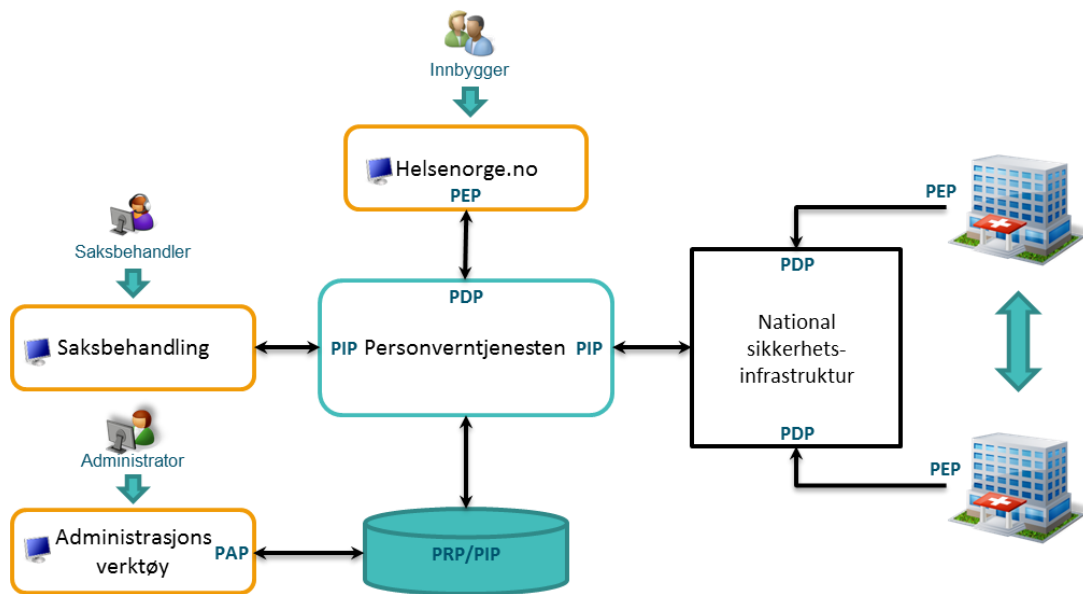
TEKNISK MÅLBILDE

Figur 4 viser arkitekturen for personverntjenesten uttrykt ved XACML definisjonene. Som det her fremgår vil helsenorge.no håndheve personvern på vegne av innbyggeren og derved fungere som et «Policy Enforcement Point» (PEP). For å kunne ta en beslutning om hvilke tjenester som skal være tilgjengelig for innbyggeren vil helsenorge.no forespør personverntjenesten som vil gjøre en evaluering av tilgang basert på innbyggerens personverninnstillinger (samtykker, reservasjoner og fullmakt). Personverntjenesten vil derved fungere som en autorisasjonstjeneste («Policy Decision Point» (PDP)) for helsenorge.no.

For resten av helsesektoren vil personverntjenesten tilgjengeliggjøre innbyggerens personverninnstillinger, men selve beslutningen om tilgang og håndhevelse av personvernet må sektoren selv håndtere. Personverntjenesten vil for sektoren derved fungere som en informasjonskilde for personverninnstillinger, definert som et «Policy Information Point» (PIP). Selve håndhevelsen av innbyggerens personvern på tvers av helsesektoren er en del av arbeidet som det jobbes med i prosjektet for Nasjonal sikkerhetsinfrastruktur (NSI). Personverntjenesten vil da for en fremtidig nasjonal sikkerhetsinfrastruktur bistå med et beslutningsunderlag for å kunne beslutte og håndheve autorisasjon på vegne av innbyggeren.

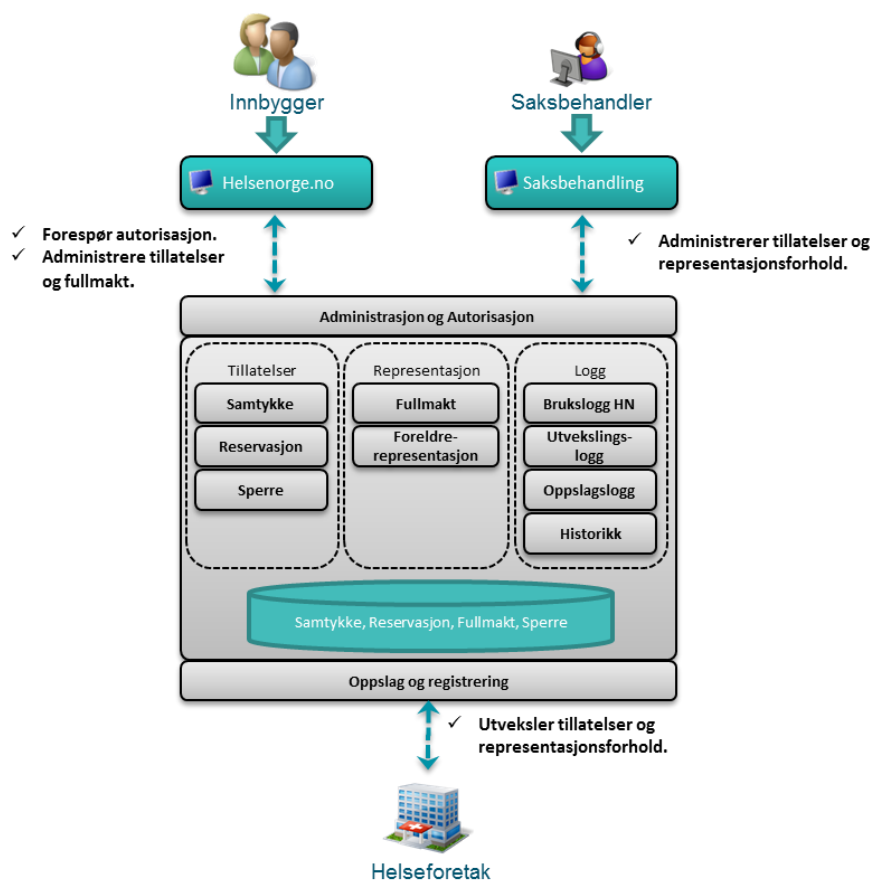
Arkitekturen for personverntjenesten baserer seg altså på veletablerte prinsipper fra XACML arkitekturen ved å:

- Skille selve tilgangsstyringen fra applikasjonen i en sentral autorisasjonskomponent for helsenorge.no
- Skille på PDP og PIP som muliggjør at kun beslutningsunderlaget tilgjengeliggjøres for en fremtidig nasjonal sikkerhetsinfrastruktur uten at selve autorisasjonsbeslutningen må gjøres i personverntjenesten.
- Ha et separat «Policy Administration Point» (PAP) for administrasjon av tilgangsregler.



Figur 4: Arkitektur for personverntjenesten uttrykket ved XACML definisjonene.

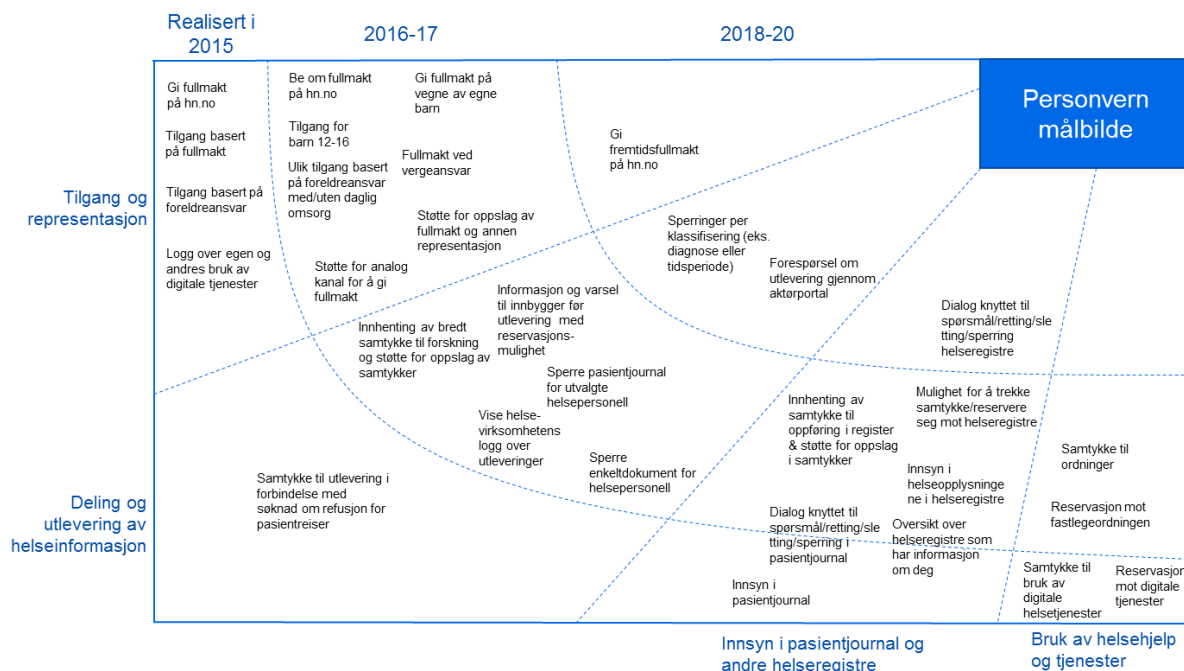
For å kunne realisere ønsket funksjonalitet er det utarbeidet en konseptuell målarkitektur for personverntjenesten. Denne er illustrert i Figur 5.



Figur 5: Konseptuell målarkitektur for personverntjenesten.

Personverntjenesten skal etableres som en ny, separat komponent som gir innbyggeren kontroll over deling av personopplysninger og representasjonsforhold gjennom helsenorge.no portalen. Tjenesten begrenses ikke kun til tjenester som eksponeres gjennom helsenorge.no, men anses som en felleskomponent for helse- og omsorgssektoren. Dette støttes ved å tilby oppslag- og registreringstjenester for å kunne tilgjengeliggjøre personvernfunksjonalitet til de ulike aktørene i sektoren. Arkitekturen legger derved til rette for i størst mulig grad å samle alle tillatelse og representasjonsforhold ett sted. Dette vil trolig ikke være mulig i alle tilfeller, men det er en strategi å etterstrebe en slik løsning på sikt.

Funksjonalitet for innsyn i pasientjournal, kjernejournal og helseregistre med tilhørende funksjonalitet som forespørsel om retting og sletting av helseopplysninger, i tillegg til sperring av enkeltelementer er valg å holde utenfor personverntjenesten. Dette realiseres som en separat tjeneste på helsenorge.no.



Figur 6: Veikart for personvernfunksjonalitet.

Figur 6 viser anbefalt veikart for realisering av personvernfunksjonalitet på helsenorge.no. Som det her vises, er grunnleggende funksjonalitet allerede levert som en del av leveranseløpet parallelt med målbiddearbeidet i 2015. Videre realisering av tjenestene i målbildet avhenger av prioriteringen i sektoren.

INNHold

| | |
|---|-----------|
| SAMMENDRAG | 3 |
| INNHold | 11 |
| 1 Omfang og Formål | 16 |
| 1.1 Omfang: personverntjenester innen helse og omsorg | 16 |
| 1.2 Formål | 18 |
| 1.3 Bakgrunn og avhengigheter | 19 |
| 1.4 Avgrensninger | 19 |
| 1.5 Begreper | 20 |
| 1.6 Interessenter | 22 |
| 2 Funksjonelt målilde | 24 |
| 2.1 Funksjonelt omfang | 24 |
| 2.2 Funksjonelle komponenter | 46 |
| 3 Teknisk målilde | 59 |
| 3.1 Prinsipper for målarkitektur | 60 |
| 3.2 Målarkitektur og arkitekturprinsipper | 61 |
| 3.3 Konseptuell løsning og tjenestekomponenter | 63 |
| 3.4 Beskrivelse av personverntjenester | 79 |
| Personverntjenester | 11 |

| | | |
|----------|---|------------|
| 3.5 | Personverninnstillinger og masterdatastrategi | 98 |
| 3.6 | Overordnede løsningskonsepter | 99 |
| 3.7 | Målarkitektur og avhengigheter | 101 |
| 3.8 | Sikkerhetsarkitektur og infrastruktur | 102 |
| 4 | Veikart for gjennomføring | 103 |
| 4.1 | Veikart | 103 |
| 4.2 | Evaluering av effektoppnåelse og kompleksitet | 109 |

VEDLEGG

| Vedlegg | Beskrivelse |
|--|--|
| Vedlegg 1 - Nåsituasjon | Nåsituasjon sett fra henholdsvis innbyggerens og aktørens side. Sistnevnte er delt inn helse- og omsorgstjenesten, helse- og omsorgsforvaltningen og eksterne aktører. |
| Vedlegg 2 - Rettslige rammebetingelser | Rettslige rammebetingelser for personverntjenester. |
| Vedlegg 3 - Teknologi og rammeverk | Ulike standarder, teknologier, og rammeverk for å håndtere personvern og tilgangsstyring. |
| Vedlegg 4 - Vekting av funksjonalitet | Evaluering av effektoppnåelse ved realisering av personvernfunksjonalitet. |

TABELLOVERSIKT

| | |
|--|----|
| Tabell 1 Relevante begreper for personvernstjenester | 20 |
| Tabell 2: Identifiserte behov for tilgangsstyring | 25 |
| Tabell 3: Juridiske krav for tilgangsstyring | 26 |
| Tabell 4: Funksjonalitet for tilgangsstyring | 27 |
| Tabell 5: Identifiserte innbyggerbehov for logg over bruk og historikk..... | 30 |
| Tabell 6: Juridiske krav for logg over bruk og historikk..... | 30 |
| Tabell 7: Funksjonalitet for logg over bruk og historikk..... | 30 |
| Tabell 8: Identifiserte innbyggerbehov for fullmakter | 31 |
| Tabell 9: Juridiske krav for fullmakter | 31 |
| Tabell 10: Funksjonalitet for fullmakter | 31 |
| Tabell 11: Identifiserte innbyggerbehov for deling av helseopplysninger | 34 |
| Tabell 12: Juridiske krav for deling av helseopplysninger | 34 |
| Tabell 13: Funksjonalitet for deling av helseopplysninger | 35 |
| Tabell 14: Identifiserte innbyggerbehov for helsehjelp og tjenester..... | 37 |
| Tabell 15: Juridiske krav for helsehjelp og tjenester..... | 38 |
| Tabell 16: Funksjonalitet for helsehjelp og tjenester..... | 38 |
| Tabell 17: Identifiserte innbyggerbehov for innsyn pasientjournal..... | 39 |
| Tabell 18: Juridiske krav for innsyn pasientjournal | 40 |
| Tabell 19: Funksjonalitet for innsyn pasientjournal | 40 |
| Tabell 20: Identifiserte innbyggerbehov for dialog pasientjournal..... | 41 |
| Tabell 21: Juridiske krav for dialog pasientjournal..... | 41 |
| Tabell 22: Funksjonalitet for dialog pasientjournal..... | 42 |
| Tabell 23: Identifiserte innbyggerbehov for brukslogg pasientjournal..... | 42 |
| Tabell 24: Juridiske krav for brukslogg pasientjournal..... | 43 |
| Tabell 25: Funksjonalitet for brukslogg pasientjournal..... | 43 |
| Tabell 26: Identifiserte innbyggerbehov for innsyn helseregistre og biobanker | 43 |
| Tabell 27: Juridiske krav for innsyn helseregistre og biobanker | 44 |
| Tabell 28: Funksjonalitet for innsyn helseregistre og biobanker | 44 |
| Tabell 29: Identifiserte innbyggerbehov for dialog helseregistre og biobanker..... | 45 |
| Tabell 30: Juridiske krav for dialog helseregistre og biobanker | 45 |
| Tabell 31: Funksjonalitet for dialog helseregistre og biobanker | 45 |
| Tabell 32: Beskrivelse av komponentene i målarkitektur for personverntjenester. | 64 |
| Tabell 33: Beskrivelse av de ulike komponentene for innsyn på helsenorge.no..... | 66 |
| Tabell 34: Ansvarsmatrise ved realisering av innsynstjenesten..... | 67 |
| Tabell 35: Beskrivelse av de ulike komponentene for aktørportal. | 69 |
| Tabell 36: Beskrivelse av de ulike komponentene for personverntjenesten..... | 71 |
| Tabell 37: Ansvarsmatrise ved realisering av personverntjenesten | 75 |
| Tabell 38: Hovedtyper for sperring. | 82 |
| Tabell 39: Ulike tilfeller av foreldrerepresentasjon. | 90 |

| | |
|--|-----|
| Tabell 40: Type representasjonsforhold i hendelsesloggen..... | 93 |
| Tabell 41: Oppslag og registreringstjenester for helsesektoren..... | 95 |
| Tabell 42: Personvernfunksjonalitet for tjenester eksponert gjennom helsenorge.no..... | 96 |
| Tabell 43: Oversikt over målarkitektur og avhengigheter. | 101 |
| Tabell 44: Beskrivelse av funksjonalitet i veikart for personvernfunksjonalitet. | 104 |

FIGUROVERSIKT

| | |
|---|----|
| Figur 1: Personvernområder i helse- og omsorgssektoren..... | 4 |
| Figur 2 Omfang av mål bilde for digitale innbyggertjenester i spesialisthelsetjenesten, som utviklet i NIKT Tiltak 2001: Forprosjekt DIS..... | 4 |
| Figur 3: Funksjonelle komponenter realiserer innbyggers brukerflate på helsenorge.no | 5 |
| Figur 4: Arkitektur for personverntjenesten uttrykket ved XACML definisjonene. | 8 |
| Figur 5: Konseptuell målarkitektur for personverntjenesten. | 9 |
| Figur 6: Veikart for personvernfunksjonalitet..... | 10 |
| Figur 7: Personvernområder i helse- og omsorgssektoren..... | 16 |
| Figur 8 Omfang av mål bilde for digitale innbyggertjenester i spesialisthelsetjenesten, som utviklet i NIKT Tiltak 2001: Forprosjekt DIS..... | 24 |
| Figur 9: Funksjonelle komponenter realiserer innbyggers brukerflate på helsenorge.no | 46 |
| Figur 10: Profilkomponenten på helsenorge.no, med fokus på personverninnstillinger | 49 |
| Figur 11: Bruk av innbyggers personverninnstillinger i og utenfor helsenorge.no..... | 54 |
| Figur 12: Innsynskomponenten på helsenorge.no..... | 55 |
| Figur 13: Plassering av personverntjenesten i DIS målbildet..... | 59 |
| Figur 14: Arkitektur for personverntjenesten uttrykket ved XACML definisjonene. | 61 |
| Figur 15: Konseptuell målarkitektur for personverntjenester. | 63 |
| Figur 16: Konseptuell arkitektur for innsyn på helsenorge.no..... | 66 |
| Figur 17: Konseptuell arkitektur for aktørportal..... | 69 |
| Figur 18: Konseptuell arkitektur for personverntjenesten. | 71 |
| Figur 19: Logisk informasjonsmodell for samtykke..... | 79 |
| Figur 20: Logisk informasjonsmodell for reservasjon. | 80 |
| Figur 21: Logisk informasjonsmodell for sperre..... | 82 |
| Figur 22: Illustrasjon av sperrefunksjonalitet..... | 83 |
| Figur 23: Logisk informasjonsmodell for innsynsbegrensning. | 84 |
| Figur 24: Konseptuell skisse for håndtering av innsynsbegrensning. | 85 |
| Figur 25: Logisk informasjonsmodell for fullmakt..... | 87 |
| Figur 26: Konseptuell skisse for håndtering av fullmakt. | 88 |
| Figur 27: Logisk informasjonsmodell for vergemål. | 89 |
| Figur 28: Logisk informasjonsmodell for foreldrerepresentasjon..... | 90 |
| Figur 29: Flytdiagram for evaluering av tilgang til tjenester ved foreldrerepresentasjon..... | 92 |
| Figur 30: Logisk informasjonsmodell for hendelseslogg..... | 93 |

| | |
|---|-----|
| Figur 31: Konseptuell løsning for personverntjenester ved eksponering gjennom Helsenorge plattformen. | 97 |
| Figur 32: Illustrasjon av forskjellen mellom sentralisert og distribuert løsning for tillatelser | 98 |
| Figur 33: Veikart for personvernfunksjonalitet | 103 |
| Figur 34: Evaluering av effektoppnåelse og kompleksitet for realisering..... | 109 |

1 OMFANG OG FORMÅL

1.1 Omfang: personverntjenester innen helse og omsorg

Personvern handler om retten til et privatliv og rett til selvbestemmelse. Personverntjenester innebærer tjenester som ivaretar disse rettighetene for innbyggeren. I møte med helse- og omsorgssektoren avtegner det seg fire personvernområder, som illustrert i Figur 7 og beskrevet nedenfor.



Figur 7: Personvernområder i helse- og omsorgssektoren

Tilgang og representasjon: Dette området omfatter innbyggerens egne tilganger, med de restriksjoner som blant annet gjelder for barn under 16 år. Videre har man representanter som opptrer på vegne av innbyggeren, som kan være fullmektige, foresatte og verger. I målbildet beskrives hvordan disse tilgangene styres på helsenorge.no, og hvordan representasjonsforhold kan tilgjengeliggjøres for andre aktører slik at tilgangsstyring kan ivaretas i hele sektoren.

Innsyn i egne helseopplysninger: En viktig forutsetning for å kunne utøve sin selvbestemmelsesrett tilknyttet helseopplysninger er at innbyggeren har innsyn i hvilke helseopplysninger som er lagret hvor, samt av hvem og til hvilket formål det brukes. I målbildet beskrives hvordan dette kan ivaretas gjennom helsenorge.no, både for pasientjournaler og helseregistre.

Deling og utlevering av helseopplysninger: I dag har man ikke god nok kontroll på hvordan innbyggerens helseopplysninger deles innad i sektoren, og til eksterne aktører. I målbildet fremheves derfor viktigheten av å gi innbyggeren en oversikt over hvordan helseopplysninger blir delt gjennom helsenorge.no. Videre har innbyggeren rettigheter knyttet til deling av

helseopplysninger. I forbindelse med helsehjelp, hvor helsepersonell ikke behøver å innhente samtykke, skal innbyggeren ha anledning til å motsette seg deling («sperre»). Til andre formål skal som regel samtykke innhentes fra innbygger. Mulige tilnærminger blir beskrevet i målbildet.

Bruk av helsehjelp og tjenester: Innbyggeren skal i stor grad selv bestemme over helsehjelp og andre tjenester som mottas fra helse- og omsorgstjenesten. I målbildet beskrives i hovedsak hvordan samtykker og reserverasjoner tilknyttet digitale tjenester og ordninger kan håndteres.

1.2 Formål

Det overordnede formålet som ligger til grunn for utviklingen av digitale personverntjenester er:

Sikrere, enklere og mer effektiv håndtering av innbyggerens personvern innenfor helse- og omsorgssektoren

Formålets tre deler beskrives mer utfyllende under, og ligger til grunn for prioritering av tjenester som beskrives i «4 - Veikart for gjennomføring».

Sikrere håndtering av innbyggerens personvern

Informasjonssikkerhet er et grunnleggende element innen personvern, og tjenester som utvikles må ta sikte på å styrke personvernet til innbyggeren. Her er det viktig å unngå fare for misbruk, ved at uvedkommende får tilgang til innbyggerens helseopplysninger eller opptrer på innbyggerens vegne.

Eksempel: I dag logger Anne seg på med Kåres bruker for å bestille time til fastlegen (misbruk). I framtiden kan Kåre gi Anne en fullmakt, slik at Anne logger seg på med egen bruker. Dette er en sikrere håndtering av Kåres personvern, som selv kan bestemme hva Anne skal og ikke skal kunne gjøre.

Enklere håndtering av personvern for innbyggeren

Tjenestene som utvikles må være oversiktlige og enkle å bruke, uavhengig av alder og forståelse.

Eksempel: I dag må Kari spørre etter oppføringer i helseregistre hos mange ulike aktører for å danne seg et bilde av lagring av hennes helseopplysninger, og for eventuelt å reservere seg mot dette. I framtiden kan hun gå inn på helsenorge.no for å se denne oversikten og gjøre reserveringer. Dette gir Kari kontroll over egne helseopplysninger og sparer henne for mye tid.

Mer effektiv håndtering av personvern for helse- og omsorgssektoren

Fra det offentliges perspektiv er det viktig at tjenestene som utvikles reduserer arbeidsmengden, slik at unødvendig tidsbruk på saksbehandling isteden kan gå til andre aktiviteter som er mer verdiskapende for behandling av pasienter. Tjenestene skal også tilrettelegge for kunnskapsutvikling i sektoren/forskning ved å gjøre prosesser for innhenting/administrasjon av samtykker enklere.

Eksempel: I dag sender Bjørn inn en forespørsel per post om å sperre innsyn i sin psykiatriske behandling til tre behandlingssteder, som så tastes inn manuelt av personell. I framtiden kan

Bjørn gå inn på helsenorge.no og sette sperren selv. Dette sparer personellet på behandlingsstedene for arbeid.

1.3 Bakgrunn og avhengigheter

Målbildet for personverntjenester bygger videre på målbildet for digitale innbyggertjenester¹, der innbyggeren skal møte én helsetjeneste på nett og hvor helsenorge.no skal være innbyggerens inngangsport til digitale helse- og omsorgstjenester.

Målbildet tar hensyn til at fremtidens IKT-løsninger i helse kan ha en annen utforming enn i dag. HelseDirektoratet utreder nå alternativer for hvordan man kan realisere de overordnede målene for IKT i Stortingsmelding «Én innbygger – én journal»². En forstudierapport med anbefalt konseptalternativ presenteres høsten 2015.

Den delen av målbildet som omhandler representasjon, kan knyttes til en potensiell fremtidig nasjonal løsning for mer overordnede fullmakter. Program for Styring og koordinering av tjenester i e-forvaltning (Skate) har utredet muligheten for en nasjonal felles digital løsning for håndtering av fullmakter og andre representasjonsforhold på tvers av offentlig sektor³. Den foreløpige konklusjonen fra foranalysen «Fullmakter for innbyggere» er at eventuelle nasjonale fullmakter vil være på et overordnet nivå. Det vil derfor uansett være behov for håndtering av mer detaljerte fullmakter innenfor hver sektor.

1.4 Avgrensninger

Målbildet beskriver løsninger som kommer i tillegg til etablert sikkerhetsinfrastruktur og eksisterende rutiner å ivareta innbyggers personvern og informasjonssikkerhet hos aktørene i sektoren. Målbildet omfatter ikke:

- **Sikkerhetsinfrastrukturen i sektoren:** Sikkerhetsinfrastrukturen beskrives i «Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren (NSI)»⁴. Det antas at løsninger i målbilde personverntjenester vil inngå som del av NSI ved at den vil tilby en nasjonal kanal som gir innbygger mulighet til å administrere og lagre sine personverninnstillinger.

¹ http://www.nasjonalikt.no/no/dokumenter/prosjekter_og_tiltak/sluttrapporter/2001_-_digitale_innbyggertjenester_i_spesialisthelsetjenesten_dis/

² <https://ehelse.no/n-innbygger-n-journal>

³ http://www.difi.no/sites/difino/files/20150624_skate-mote_sak_12-15_-_foranalyse_fullmakter_og_annen_representasjon_for_innbyggere_-_vedlegg_1_rapport_pr_juni_2015.pdf

⁴ <https://ehelse.no/nasjonale-prosjekter/nasjonal-sikkerhetsinfrastruktur-for-helse-og-omsorgssektoren-nsi>

Personverntjenesten vil da fungere som en informasjonskilde for NSI for å kunne ivareta innbyggerens personvern. Dette er nærmere beskrevet under kapittel 3.2.

- **Eksisterende rutiner og prosesser for personvern:** Målbildet beskriver nasjonal funksjonalitet som kommer i *tillegg* til eksisterende rutiner og prosesser for å ivareta innbyggerens personvern i sektoren.
- **Sektorens håndtering av informasjonssikkerhet:** Målbildet legger til grunn kravene definert i Norm for informasjonssikkerhet. Enkeltaktørers, og sektorens håndtering av informasjonssikkerhet inngår ikke i målbildet.

1.5 Begreper

I Tabell 1 oppføres begreper som er relevante for personverntjenester, og som vil bli brukt videre i dokumentet. Der forklaringen står oppført som sitat, er den hentet ordrett fra kilden. For flere begreper kan man bruke henholdsvis Normen og Volven.

Tabell 1 Relevante begreper for personverntjenester

| Begrep | Forklaring |
|---------------------------------|--|
| Aktør | Alle organisasjoner, uavhengig om de yter helsehjelp eller ikke. |
| Behandling av helseopplysninger | «Enhver bruk av helseopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter» (Helseregisterloven § 2) |
| Daglig omsorg | Et ansvarsforhold for foreldre som har foreldreansvar for barnet og som barnet bor fast med. Skal ta avgjørelser for barnet som gjelder vesentlige sider av omsorgen av barnet, uten at andre med foreldreansvar kan motsette seg det. (Barneloven § 37) |
| Foreldreansvar | Et ansvarsforhold der foreldre har rett og plikt til å ta avgjørelser på vegne av sine barn, enten på det personlige området i kraft av foreldreansvaret eller på det økonomiske området i kraft av å være verge. Innenfor helsenorge.no begrenses retten til innsynsrett, mens handlingsrett legges til foreldre med daglig omsorg. (Barneloven § 30, Vergemålsloven § 17) |
| Fullmakt | En avtale om at fullmektig kan handle på vegne av fullmaktsgiver, og eventuell opphevelse av taushetsplikt tilknyttet helseopplysninger. (Avtaleloven § 10) |
| Helseopplysninger | I målbildet benyttes et utvidet fullmaktsbegrep, der andre enn innbygger selv kan tildele fullmakt på vegne av innbygger. Sensitive personopplysninger om helseforhold, som er taushetsbelagt (Helseregisterloven § 2) |
| Helseregister | I målbildet brukt om alle helseregistre som ikke er pasient-journaler. For øvrig gjelder følgende definisjon: «register, fortegnelser, mv. der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen» (Helseregisterloven § 2) |

| Begrep | Forklaring |
|---|--|
| | I målbildet faller sentrale helseregistre, nasjonale og lokale kvalitetsregister, forskningsregistre og helseopplysninger tilknyttet biobanker faller innunder denne betegnelsen. |
| Helsevirksomhet | En offentlig eller privat behandlingsrettet virksomhet hvor helsepersonell yter helsehjelp til innbyggeren. Begrepet «behandlingssted» brukes noen steder synonymt. |
| Innsyn | Med innsyn menes i denne rapporten innbyggerens rett til innsyn i egne helseopplysninger i henhold til Pasient- og brukerrettighetsloven kapittel 5. <i>(Pasient- og brukerrettighetsloven kap. 5)</i> |
| Kjernejournal | En nasjonal journal som «som sammenstiller vesentlige helseopplysninger om den registrerte og gjør opplysningene tilgjengelige for helsepersonell som trenger dem for å yte forsvarlig helsehjelp.» <i>(Kjernejournalforskriften § 1)</i> |
| Nærmeste pårørende | Nærmeste pårørende er den innbyggeren oppgir som pårørende. Der pårørende ikke er pekt ut, er rekkefølgen: <ul style="list-style-type: none"> - Ektefelle/partner/samboer - Barn over 18 år - Foreldre eller andre med foreldreansvar - Søsken over 18 år - Besteforeldre - Andre familiemedlemmer som står pasienten nær - Verge/fremtidsfullmektig på det personlige området Pårørende er ikke en representant, og kan ikke handle på vegne av innbyggeren uten en fullmakt. Pårørende kan imidlertid ha rett på informasjon om pasientens helsetilstand og helsehjelp som ytes. <i>(Pasient- og brukerrettighetsloven § 1-3, § 3-3)</i> |
| Pasientjournal | I målbildet brukt om behandlingsrettede helseregistre, utenom Kjernejournal. For øvrig gjelder følgende definisjon: «Pasientjournal- og informasjonssystem eller annet register, fortegnelse eller lignende, der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner» <i>(Pasientjournalloven § 2)</i> |
| Personopplysninger | «Opplysninger og vurderinger som kan knyttes til en enkeltperson» <i>(Personopplysningsloven § 2)</i> |
| Representant | Brukes i dette målbildet som en samlebetegnelse for innbyggere som representerer en annen innbygger, og inkluderer representasjon med grunnlag i fullmakt (fullmektig) og representasjon med grunnlag i foreldreansvar (med/uten) daglig omsorg (foresatt). |
| Reservasjon mot behandling av opplysninger | En handling der innbyggeren motsetter seg behandling av sine helseopplysninger i helseregistre <i>(Helseregisterloven § 10)</i> |
| Reservasjon mot helsehjelp og andre tjenester | En handling der innbyggeren motsetter seg helsehjelp eller andre tjenester |
| Rettslig handleevne | Evnen til å foreta rettslige handlinger, for eksempel inngå avtaler eller på annet vis påta seg ansvar. |

| Begrep | Forklaring |
|---|--|
| Samtykke til behandling av opplysninger | «En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av helseopplysninger om seg selv» (Personopplysningsloven § 2, Helseregisterloven § 2) |
| Samtykke til helsehjelp | En uttrykkelig eller stilltiende erklæring fra pasienten om at han eller hun godtar helsehjelpen. (Pasient- og brukerrettighetsloven § 4-2) |
| Samtykkekompetanse | «En persons skikkethet til selv å gi samtykke til behandlings- eller omsorgstiltak» (Volven, Administrativ terminologi for pleie- og omsorgstjenesten) «Rettslig handleevne og i den konkrete situasjon rett person til å vurdere og ta stilling til et spørsmål.» (Volven, Definisjonskatalog for helsestasjons- og skolehelsetjenesten) |
| Sensitive personopplysninger | «Opplysninger om a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, c) helseforhold, d) seksuelle forhold, e) medlemskap i fagforeninger» (Personopplysningsloven § 2) |
| Sperring | En handling der innbyggeren motsetter seg helsepersonells innsyn i eller utlevering av egne helseopplysninger til annen helsevirksomhet. (Helsepersonelloven § 25, § 45) |
| Tilgang | Med tilgang menes at helsepersonell gis adgang til direkte elektronisk å hente frem helseopplysninger om pasienter. (Forskrift om tilgang til helseopplysninger mellom virksomheter § 2, andre ledd) |
| Tilgangskontroll | Utføre autorisasjon. |
| Tilgangsstyring | Administrere autorisasjoner som kan benyttes for tilgangskontroll. |
| Utlevering | Med utlevering menes at helsepersonell, eller andre, får opplysninger om pasient formidlet muntlig, skriftlig eller på andre måter innenfor rammene for taushetsplikten når de ikke har mulighet til tilgang til slike opplysninger direkte. |
| Vedtak om omsorgsovertakelse | Et vedtak der foreldrenes daglige omsorg overtas av barnevernstjenesten (Barnevernloven § 4-12) |
| Vedtak om vergemål | Et vedtak som oppnevner verge som kan handle på vegne av personen med verge innenfor for personlige og/eller økonomiske forhold, med eventuell opphevelse av taushetsplikt tilknyttet helseopplysninger. (Vergemålsloven § 25, § 31) |

1.6 Interessenter

Målbildet er basert på intervjuer og samtaler med en rekke interessenter i og utenfor helsesektoren. Disse interessentene kan deles i fire hovedgrupper som vil bli kort presentert i dette kapittelet. For utfyllende informasjon om nåsituasjon for hver interessent, se vedlegg 1 – Nåsituasjon.

1.6.1 Innbygger

Innbyggeren er den primære interessenten i utforming av personverntjenester. Innbyggeren kan fylle mange ulike roller, som pasient i helse- og omsorgstjenesten, som bruker av helse- og omsorgsforvaltningen, som barn, som hjelpetrequende, som representant for annen innbygger mv. Dermed vil omfang av helseopplysninger som deles og behov for representasjon og tilgang variere.

1.6.2 Helse- og omsorgstjenesten

Helse- og omsorgstjenesten omfatter offentlige og private helsevirksomheter som yter helsehjelp eller omsorg til innbyggeren. Innen spesialisthelsetjenesten er dette sykehusene og tilknyttede spesialister. Den kommunale helse- og omsorgstjenesten omfatter allmennhelse-tjenesten, sykehjem og hjemmesykepleie. I tillegg kommer apotekene. Felles for alle helsevirksomheter er at de behandler innbyggerens helseopplysninger med det formål å yte helsehjelp.

1.6.3 Helse- og omsorgsforvaltningen

Helse- og omsorgsforvaltningen omfatter enheter som ikke er direkte involvert i å yte helsehjelp og omsorg. Helseøkonomi og pasientskadesaker er to områder som er særlig relevant i dette målbildet, hvor helseopplysninger fra helse- og omsorgstjenesten deles med forvaltningen. Det kan også være relevant for innbyggeren å la seg representere i disse tjenestene.

1.6.4 Eksterne aktører

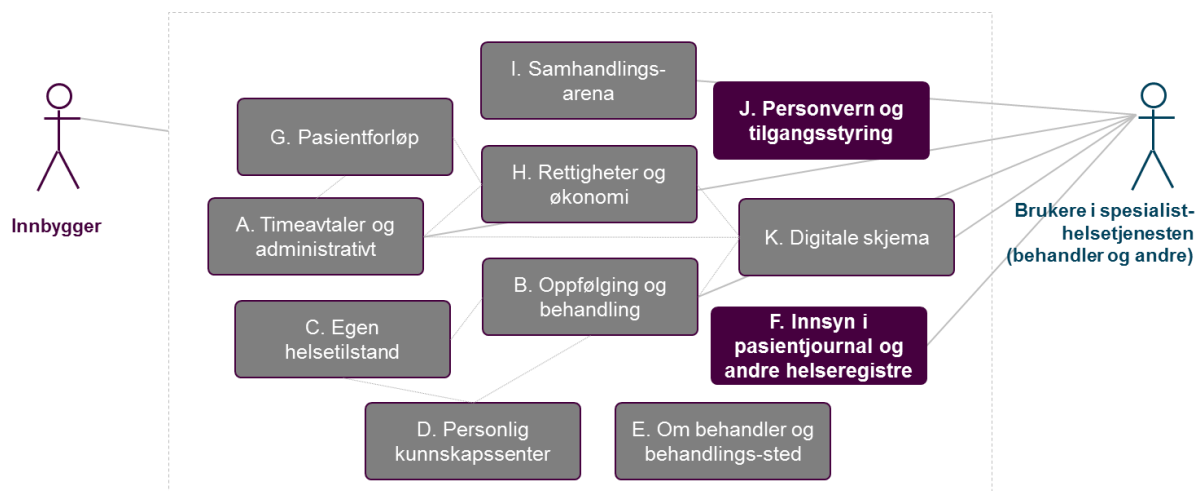
I og utenfor helse- og omsorgssektoren er det flere som har interesse av innbyggerens helseopplysninger. Dette gjelder blant annet for forskning og forsikring, som man særlig har sett på i dette målbildet. I likhet med forvaltningen deles her helseopplysninger fra innbyggerens møte med helse- og omsorgstjenesten.

2 FUNKSJONELT MÅLBILDE

I dette kapitlet beskrives personverntjenester som dekker behov og krav identifisert i nåsituasjon og rettslige rammer, se vedlegg 1 og 2. Først beskrives målbildets funksjonelle omfang i form av hvilke behov som dekkes og vurderinger av funksjonalitet knyttet til dette. Deretter gis en beskrivelse av løsningen som realiserer behovene, gjennom et sett med funksjonelle komponenter.

2.1 Funksjonelt omfang

Innbyggers personverntjenester inngår i det funksjonelle målbildet for *innbyggertjenester for spesialisthelsetjenesten*; se tjenestemålene F. Innsyn og J. Personvern og tilgangsstyring.



Figur 8 Omfang av målbilde for digitale innbyggertjenester i spesialisthelsetjenesten, som utviklet i NIKT Tiltak 2001: Forprosjekt DIS.

I påfølgende avsnitt beskrives behovene som er identifisert innenfor personvernområdet. Følgende behov er identifisert:

J. Personvern og tilgangsstyring

- J1. Tilgangsstyring
- J2. Logg over bruk; historikk
- J3. Fullmakter

J4. Deling og utlevering av helseopplysninger

J5. Bruk av helsehjelp og -tjenester

F. Innsyn i pasientjournal og andre helserelevante registre

F1. Innsyn i pasientjournal

F2. Dialog vedrørende pasientjournal

F3. Brukslogg for pasientjournal

F4. Innsyn i helseregistre og biobanker; innhold og bruk

F5. Dialog vedrørende helseregistre og biobanker.

For å tilrettelegge for et smidig utviklingsløp er behovene formulert som overordnede brukerhistorier (epos). Hvert epos er beskrevet mer detaljert i tre tabeller:

1. **Identifiserte behov** som faller innunder eposet, og hvorvidt det skal støttes av digitale innbyggertjenester gjennom helsenorge.no. Flere behov kan avdekkes når epos og brukerhistorier skal realiseres, innbyggerperspektivet er prioritert i behovsanalysen.
2. **Juridiske krav** som faller innunder eposet, oppsummert.
3. **Innspill til funksjonalitet** som behøves for å svare på behovene, med en mer detaljert behovsbeskrivelse. Dette kan bli justert i det videre løpet, når epos og brukerhistorier skal realiseres.

Kolonnen «Støttet i målbildet» indikerer om de løsningene som anbefales vil understøtte det identifiserte behovet. Dersom behovet ikke støttes, «Nei», må man benytte de eksisterende arbeidsprosesser man har i dag.

2.1.1 J Personvern og tilgangsstyring

2.1.1.1 J.1 Tilgangsstyring

Som innbygger får jeg eller andre med tilgang på vegne av meg (foreldre og andre med fullmakt) etter innlogging på helsenorge.no tilgang til de tjenestene jeg kan benytte relatert til min helse, slik at jeg gjennom en sikker nettløsning kan benytte digitale helsetjenester, samt administrere og holde oversikt over min kontakt med helsetjenesten.

Tabell 2: Identifiserte behov for tilgangsstyring

| Identifisert innbyggerbehov | Støttet i målbildet? |
|--|----------------------|
| Få tilgang til egne tjenester på helsenorge.no | Ja |
| Få tilgang til tjenester på helsenorge.no som fullmektig | Ja |

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|----------------------|
| Få tilgang til tjenester på helsenorge.no som forelder | Ja |
| Få tilgang til tjenester på helsenorge.no som verge (dekkes gjennom at verge må gis fullmakt) | Ja |
| Som barn 12-16 år få rett til å bruke utvalgte tjenester (forutsetter at forelder har samtykket til det, samt etablering av eID tilgjengelig for aldersgruppen) | Ja |
| Få tilgang til tjenester på helsenorge.no som pårørende uten fullmakt | Nei |
| Få tilgang til tjenester på helsenorge.no gjennom skifteattest ved dødsfall | Nei |
| Som innbygger, utnevne en representant (advokat el.) som kan få innsyn i helseopplysninger som du selv har blitt nektet innsyn i | Nei |

Tabell 3: Juridiske krav for tilgangsstyring

| Juridisk krav | Lov/forskrift |
|--|---|
| Foreldre med foreldreansvar skal ta avgjørelser for barnet i personlige forhold | Barneloven § 30 |
| Vergen skal ta avgjørelser for barnet i økonomiske forhold | Vergemålsloven § 17 |
| Vergen for mindreårige er den/de med foreldreansvar, evt. oppnevnt verge | Vergemålsloven § 16 |
| Vergen skal også ta avgjørelser for barnet i personlige forhold dersom ingen har foreldreansvar for barnet. Dette gjelder også hvis begge foreldre er umyndige. | Vergemålsloven § 17 |
| Foreldre skal legge vekt på hva barnet mener i økende grad fram til det fyller 18 år og legge stor vekt fra barnet er fylt 12 år. For helse gjelder at foreldre samtykker til helsehjelp fram til barnet er 16 år, når barnet som regel får samtykkekompetanse og kan bestemme selv. | Barneloven § 31 Barneloven § 33 Pasient- og brukerrettighetsloven § 4-3 |
| Én av foreldrene skal samtykke dersom det er en del av daglig omsorg, begge om det er av mer inngripende karakter. Forelder barnet bor fast med skal ta avgjørelser som gjelder vesentlige deler av omsorg (barnehage, bosted, større avgjørelser i dagliglivet) | Pasient- og brukerrettighetsloven § 4-4 Vergemålsloven § 18 Barneloven § 37 |
| Barnevernstjenesten overtar omsorgen etter vedtak, noe som medfører at foreldre mister det meste av sine rettigheter selv om de fortsatt har foreldreansvar | Barnevernloven § 4-18 |
| Fosterforeldre eller institusjon utøver daglig omsorg og tar avgjørelser ut fra barnevernstjenestens bestemmelser | Barnevernloven § 4-18 |
| Vergen oppnevnes innenfor for økonomiske og/eller personlige forhold, men ikke gjøres mer omfattende enn nødvendig | Vergemålsloven § 21 |
| Person med verge kan fratas rettslig handleevne i økonomiske og/eller personlige forhold, slik han/hun ikke lenger får representere seg selv | Vergemålsloven § 22-24 |

| Juridisk krav | Lov/forskrift |
|---|--|
| Ved flere verger innenfor samme område må verger handle i felleskap. Man kan her tenke seg samme fordeling som for foreldre (se ovenfor). Ved uenighet avgjør fylkesmannen. | Vergemålsloven § 28 Vergemålsloven § 18 |
| Vergen kan ikke foreta en rettslig handling dersom den som er satt under vergemål motsetter seg det (så lenge innbygger ikke er fratatt rettslig handleevne og forstår hva disposisjonen innebærer) | Vergemålsloven § 33 |
| Innbygger har rett til å la seg representere ved fullmektig i alle trinn av saksbehandlingen | Forvaltningsloven § 12 |

Tabell 4: Funksjonalitet for tilgangsstyring

| Funksjonalitet | Beskrivelse |
|--------------------------|--|
| Tilgang for innbygger | <p>Ved innlogging vises alle tjenester som innbygger har tilgang til og som har noe å vise innbyggeren.</p> <p>I utgangspunktet har innbygger tilgang til alle tjenester, men unntak vil gjelde for barn under 16 år og innbyggere som er fratatt rettslig handleevne. Dette er beskrevet nedenfor.</p> <p>Ved evaluering av tjenestetilgang må det også tas høyde for innbyggerens personlige personverninnstillinger i form av samtykke til og reservasjon mot tjenester på helsenorge.no. Selv om en innbygger juridisk sett har tilgang til en tjeneste, skal den eksempelvis ikke være tilgjengelig dersom innbyggeren har valgt å reservere seg mot å ha tjenesten tilgjengelig på internett.</p> |
| Tilgang for representant | <p>Tilsvarende som for innbygger vises tjenester som representant (foresatt eller fullmektig) har tilgang til og som har noe å vise.</p> <p>Tilgang for representanter går fram av omfanget i representasjonsforholdet.</p> <ul style="list-style-type: none"> • For fullmektig fremgår det av fullmakten som er gitt. • For foreldre er omfanget beskrevet etter tabellen. <p>En fullmektig skal som utgangspunkt alltid ha de samme begrensingene i forhold til personverninnstillinger som innbyggeren fullmektig representerer. Eksempelvis betyr dette at dersom innbyggeren selv har reservert seg mot å ha en tjeneste på internett vil den heller ikke være tilgjengelig for fullmektig.</p> |
| Valg av person | <p>Når innbygger er innlogget på Min Helse på helsenorge.no, må det være mulig å velge en annen innbygger som han/hun kan representere.</p> <p>Som et prinsipp for løsningen skal all representasjon foregå ved at innlogget bruker velger å bytte til en annen bruker gjennom personvelgeren på hovedsiden. Det skal da tydelig fremgå at innlogget bruker handler på vegne av en annen innbygger.</p> |

| Funksjonalitet | Beskrivelse |
|---|--|
| | All representasjon skal logges i den representerte brukerens logg over bruk på helsenorge.no. For mer informasjon om loggfunksjonalitet, se «J.2 Logg over bruk og historikk». |
| Tilgjengeliggjøre informasjon om representasjonsforhold | Aktører utenfor helsenorge.no må få mulighet til å gjøre oppslag mot et sentralt datagrunnlag driftet av helsenorge.no. Dette gjelder særlig for fullmakter, men kan også være en kilde for foreldreansvar og daglig omsorg. |

J.1.A Tilgangsstyring ved fratatt rettslig handleevne

Ved fratatt rettslig handleevne vil man fortsatt ha rett til innsyn, men har ikke lov til å utføre handlinger på helsenorge.no. Her kan det være aktuelt å skille mellom det personlige og økonomiske området. Dersom man kun er fratatt rettslig handleevne på det økonomiske området vil det fortsatt være aktuelt å utføre handlinger for de fleste tjenester på helsenorge.no. Fratakelse på det økonomiske og/eller personlige området står i Folkeregisteret.

J.1.B Tilgangsstyring for barn

Tilgangsstyring for barn regulerer innbyggers tilgang til egne opplysninger og tjenester på helsenorge.no fram til 18 års alder.

Barn 0-11 år skal ikke ha tilgang til noen av tjenestene på helsenorge.no, hverken for innsyn eller handling.

Barn 12-16 år skal i utgangspunktet ikke ha tilgang til noen av tjenestene på helsenorge.no, hverken for innsyn eller handling. Unntaket er når foreldre har gitt barnet tilgang ved samtykke.

Barn 16-18 år har i utgangspunktet rett til innsyn og handling på helsenorge.no. Unntaket gjelder blant annet helseøkonomi, hvor myndighetsalder på 18 år blir relevant, eksempelvis for pasientreiser og pasientskadesaker.

J.1.C Tilgangsstyring for foreldre

Tilgangsstyring for foreldre skiller mellom foreldreansvar⁵ og daglig omsorg.

Foreldreansvar: Den eller de som har foreldreansvaret for barnet. Ved omsorgs-overtakelser vil foreldre som regel fortsatt ha foreldreansvaret. Hvem som har foreldreansvar er

⁵ Forutsetter at foreldre ikke selv er mindreårige. Dersom dette er tilfellet tilfaller foreldreansvaret den som har foreldreansvar eller vergeansvar for barnemoren.

registrert i folkeregistret. Det er per i dag ikke informasjon om omsorgsovertakelser i Folkeregisteret.

Daglig omsorg: Den eller de som har foreldreansvaret for barnet og barnet bor fast hos.

I utgangspunktet skal man ha full tilgang til å handle på vegne av barn ved foreldreansvar, men det finnes likevel handlinger som gjelder større avgjørelser om dagliglivet og som krever daglig omsorg. Dette vil eksempelvis være tjenesten for bytte av fastlege.

Hvilke foresatte som har daglig omsorg er ikke direkte registrert i folkeregisteret. Derfor vil det kun være mulig å evaluere daglig omsorg ved å se på om barnet har samme folkeregisteret adresse som den foresatte. I tilfeller der barnet bor fast hos begge foreldrene, vil kun forelder med lik folkeregistrert adresse som barnet få tilgang tilsvarende daglig omsorg. Det er anslått at dette vil utelukke 70 000 foreldre som har daglig omsorg. En mulig løsning vil være å la foresatte med daglig omsorg for barnet opprette en fullmakt til en samboer med samme folkeregistrerte adresse, eller annen foresatt med foreldreansvar.

J.1.D Tilgangsstyring ved omsorgsovertakelser og adressesperring

Barnevernstjenesten trenger ikke tilgang til barnets tjenester på helsenorge.no. Ved behov for innsyn i forbindelse med saksbehandling henvender barnevernstjenesten seg til helsevirksomheter i likhet med andre aktører. For å utføre handlinger kan barnevernstjenesten gi fosterfamilie eller barnevernsinstitusjon fullmakt til å utføre handlinger. Fosterfamilie og barnevernsinstitusjoner skal imidlertid ikke få tilgang til barnets tjenester på helsenorge.no. Dette fordi man må være forsiktig med tanke på innsyn, særlig før omsorgsovertakelsen. Det er videre ingen god måte å identifisere forholdet mellom fosterforeldre og barnet. De må derfor bruke andre kanaler for å representere barnet.

I tilfeller der barn bor med adressesperre kode 7 (fortrolig) eller kode 6 (strengt fortrolig), er det viktig at opplysninger som tilkjenner innbyggerens bosted ikke gjøres tilgjengelig for uvedkommende. Når kode 6 eller 7 er registrert på innbyggeren, må man derfor sørge for at helseopplysninger ikke er tilgjengelig for noen andre enn innbyggeren selv. Der det gjelder et barn vil det sikre at uvedkommende foreldre ikke får tilgang til barnets opplysninger, for eksempel dersom det skulle være en forsinkelse mellom adressesperring og fratakelse av foreldreansvar.

2.1.1.2 J.2 Logg over bruk og historikk

Som innbygger kan jeg hente fram en logg over når jeg eller andre med tilgang på vegne av meg har logget inn og benyttet tjenester på helsenorge.no og når mine personverninnstillinger er endret, slik at jeg får oversikt over bruk av mine digitale innbyggertjenester.

Tabell 5: Identifiserte innbyggerbehov for logg over bruk og historikk

| Identifisert innbyggerbehov | Støttet i målbildet? |
|--|----------------------|
| Se oversikt over logg over eget bruk | Ja |
| Se oversikt over logg over bruk på mine vegne | Ja |
| Tilgang til tidligere personverninnstillinger, som basis for egen/andres bruk av tjenester | Ja |

Tabell 6: Juridiske krav for logg over bruk og historikk

| Juridisk krav | Lov/forskrift |
|---|---------------|
| Ingen identifiserte juridiske krav. Derimot skal vanlig logg over helsepersonells tilgang alltid angi tidspunkt og hvilke opplysninger de ble gitt tilgang til. | |

Tabell 7: Funksjonalitet for logg over bruk og historikk

| Funksjonalitet | Beskrivelse |
|--|---|
| Registrere innlogginger og bruk av tjenester av innbygger | Overordnet logg som viser tjenester hvilke tjenester på helsenorge.no som er benyttet av innbygger selv. |
| Registrere innlogginger og bruk av tjenester på vegne av innbygger | Overordnet logg som viser tjenester på helsenorge.no som er benyttet på vegne av innbygger |
| Registrere endringer i innbyggers profil | Aktivitetslogg/historikk som gir kunnskap om hvilke personverninnstillinger som til enhver tid var gjeldende. For eksempel tidligere fullmakter og reservasjoner. |
| Oppslagslogg for representasjon utenfor hn.no | En logg over eksterne oppslag i personverntjenesten, med en obligatorisk forklarende tekst som forklarer bakgrunnen for oppslaget. |

2.1.1.3 J.3 Fullmakter

Som innbygger kan jeg gi andre fullmakt til å opptre på mine vegne, og jeg kan be om eller motta fullmakt fra andre, slik at pårørende og andre kan støtte meg ved bruk av digitale innbyggertjenester og andre helsetjenester.

Tabell 8: Identifiserte innbyggerbehov for fullmakter

| Identifisert innbyggerbehov | Støttet i målbildet? |
|--|----------------------|
| Opprette, endre og trekke tilbake fullmakt eller fremtidsfullmakt | Ja |
| Som representant avslå opprettet fullmakt | Ja |
| Som representant be om fullmakt eller fremtidsfullmakt | Ja |
| Akseptere eller avslå forespurt fullmakt | Ja |
| Se gjeldende og historiske representasjonsforhold. Se fremtidsfullmakter. | Ja |
| Gi andre innbyggere fullmakt til å bruke tjenester på vegne av barnet | Ja |
| Få tildelt fullmakt på bakgrunn av vergeansvar | Ja |
| Få tildelt fullmakt på bakgrunn av vedtak knyttet til pasient- og brukerrettighetsloven. | Ja |
| Gi fullmakt til helsepersonell til å bruke tjenester på vegne av seg selv | Nei |
| Administrere fullmakt gjennom en alternativ, analog/papirbasert kanal | Ja |

Tabell 9: Juridiske krav for fullmakter

| Juridisk krav | Lov/forskrift |
|---|---|
| Det skapes rett og plikt for fullmaktsgiveren umiddelbart når fullmektigen har gjort en rettshandel i fullmaktsgiverens navn og innenfor fullmaktens grenser. | Avtaleloven § 10 |
| Innbygger har rett til å la seg representere ved fullmektig i alle trinn av saksbehandlingen | Forvaltningsloven § 12 |
| Innbygger kan opprette en fremtidsfullmakt for det personlige og/eller økonomiske området som stadfestes når et tilfelle inntreffer (sinnslidelse, svekket helbred) | Vergemålsloven § 78, 80, 83, 84 |
| Innbygger må være myndig (over 18 år og ikke fratatt rettslig handleevne) for å opprette fullmakt, og fullmakt kan ikke opprettes ved tvang | Avtaleloven kapittel 3, Vergemålsloven § 8, 9 |
| Fullmektig må være myndig (over 18 år og ikke fratatt rettslig handleevne) | Vergemålsloven § 8, 9 |

Tabell 10: Funksjonalitet for fullmakter

| Funksjonalitet | Beskrivelse |
|---------------------------------|--|
| Oversikt over fullmakter som er | Oversikt over aktive, fremtidige, historiske og forespurte fullmakter som er mottatt fra andre innbyggere gir innbyggeren en oversikt over hvem han/hun kan representere. Fullmaktsgiver, omfang, tidsperiode og hvorvidt fullmakt er aktiv må |

| Funksjonalitet | Beskrivelse |
|--|---|
| mottatt | <p>fremgå.</p> <p>Den kan vurderes om man skal inkludere andre representasjonsforhold i oversikten, eventuelt at innbyggeren blir gjort oppmerksom på at andre representasjonsforhold foreligger. Innbygger vil uansett se dette ved valg av innbygger, se J.1 Tilgangsstyring</p> |
| Oversikt over fullmakter som er gitt eller forespurt | <p>Oversikt over aktive, fremtidige, historiske og forespurte fullmakter som er gitt andre innbyggere gir innbyggeren en oversikt over hvem som kan representere han/hun. Fullmaktsgiver, omfang, tidsperiode og hvorvidt fullmakt er aktiv må fremgå.</p> <p>Den kan vurderes om man skal inkludere andre representasjonsforhold i oversikten, eventuelt at innbyggeren blir gjort oppmerksom på at andre representasjonsforhold foreligger.</p> |
| Opprette ny fullmakt | <p>Innbygger kan opprette en ny fullmakt, ved å spesifisere fullmektig, omfang og tidsperiode. Fullmakt er gyldig fra den opprettes. Fullmektig får et varsel om at fullmakt er opprettet.</p> <p>I utgangspunktet må fullmaktsgiver og fullmektig være myndige.</p> |
| Be om fullmakt | <p>Innbygger kan be om en fullmakt med seg selv som fullmektig, ved å spesifisere fullmaktsgiver, omfang og tidsperiode. Fullmaktsgiver får et varsel. Fullmakt er ikke aktiv før innbyggeren har akseptert fullmakten.</p> |
| Endre fullmakt | <p>Både fullmaktsgiver og fullmektig kan endre fullmakten. Der fullmaktsgiver endrer fullmakten blir endringen aktiv med en gang, der fullmektig endrer fullmakten blir det et forslag fullmaktsgiver må akseptere.</p> <p>Hver gang fullmakten endres opphører den forrige fullmakten og en ny fullmakt opprettes. Sluttdato for den gamle fullmakten blir startdato for den nye fullmakten.</p> <p>Ved endringer blir fullmektig varslet.</p> |
| Trekke tilbake fullmakt | <p>Fullmaktsgiver kan trekke tilbake fullmakten, slik at den ikke lenger er aktiv.</p> <p>Dersom en fullmakt trekkes tilbake, blir fullmektig varslet.</p> |
| Akseptere eller avslå forespurt fullmakt | <p>Ved foreslåtte fullmakter, kan fullmaktsgiver velge om han/hun vil akseptere eller avslå fullmakten.</p> |
| Forespørre endring | <p>Fullmektig kan forespørre en endring til fullmakten som er mottatt. I så fall må fullmaktsgiver akseptere endringen.</p> |
| Avslå mottatt fullmakt | <p>Fullmektig kan avslå en fullmakt han/hun har mottatt, slik at den ikke lenger er aktiv. Dersom en fullmakt avslås, blir fullmaktsgiver varslet.</p> |
| Analog registrering av fullmakt | <p>Et fullmaktsskjema som speiler den elektroniske fullmakten på helsenorge.no kan skrives ut, fylles ut, signeres og sendes inn til HELFO per brevpost. Gjennom et saksbehandlingsgrensesnitt kan fullmakten registreres, slik at fullmektig får tilgang til å representere fullmaktsgiver på helsenorge.no.</p> |

| Funksjonalitet | Beskrivelse |
|---|--|
| Opprette fullmaktsforhold basert på vergeansvar | Ved vergeansvar vil helseopplysningene vergen skal ha tilgang til i utgangspunktet være veldig begrenset og må i stor del defineres av fylkesmannen for det enkelte tilfellet. Denne funksjonaliteten tilbys derfor gjennom en analog kanal der omfanget defineres av fylkesmannen basert på vedtaket. |
| Oppslag av fullmakter og andre representasjonsforhold | Helsenorge.no må gjøre personverntjenesten tilgjengelig for oppslag fra andre aktører, slik at disse har oppdatert informasjon om gjeldende representasjonsforhold. En utfordring her vil være at noe av oppslaget kan omfatte taushetsbelagte personopplysninger, slik det blant annet er med foreldreansvar. I prinsippet vil aktøren behøve en lovhjemmel for å hente slik informasjon uten å be innbyggeren om et samtykke. Her kan det være en forskjell om aktøren er en offentlig helsevirksomhet, privat helsevirksomhet eller en aktør som ikke yter helsehjelp. |

J.3.A Fullmaktens innhold

En fullmakt må inneholde følgende fire deler:

- Fullmektig
- Fullmaktsgiver
- Tidsperiode
- Omfang

Fullmektig må være myndig, det vil si over 18 år og ikke fratatt rettslig handleevne.

Innbygger som fullmaktsgiver må være myndig, det vil si over 18 år og ikke fratatt rettslig handleevne.

Tidsperioden for fullmakten er definert ved en startdato og en sluttdato. Startdatoen kan være dagens dato eller en fremtidig dato, mens sluttdato kan være en fremtidig dato eller ubegrenset i tid. En fullmakt vil også avsluttes når en av partene trekker den tilbake, de ikke lenger oppfyller kravene beskrevet ovenfor, eller dør.

En fullmakt kan også utløses ved en betinget hendelse, slik som sinnslidelse eller alvorlig svekket helsetilstand, det vil si at man oppretter en fremtidsfullmakt. I et slikt tilfelle vil det gjennomføres saksbehandling med krav til dokumentasjon fremtidsfullmakten aktiveres.

Omfanget av en fullmakt kan avgrenses til spesifikke tjenester eller handlinger.

2.1.1.4 J.4 Deling og utlevering av helseopplysninger

Som innbygger kan jeg styre hvordan mine helseopplysninger deles/utleveres både for å yte meg helsehjelp (primærbruk) og for andre formål slik som forskning og analyse

(sekundærbruk), slik at andre kan yte tjenester og utvikle ny kunnskap samtidig som jeg har kontroll på bruken av mine helseopplysninger.

Tabell 11: Identifiserte innbyggerbehov for deling av helseopplysninger

| Identifisert innbyggerbehov | Støttet i målbildet? |
|--|----------------------|
| Samtykke til lagring og bruk av helseopplysninger i helseregistre | Ja |
| Reservere seg mot lagring og bruk av helseopplysninger i helseregistre (konsekvens av reservasjon: opplysninger lagres ikke, evt. slettes) | Ja |
| Lokale kvalitetsregistre og forskningsregistre | Nei |
| Samtykke til utlevering av helseopplysninger | Ja |
| Reservere seg mot utlevering av personlige helseopplysninger til forskningsprosjekt ved bredt samtykke | Ja |
| Sperre for helsepersonell (konsekvens av sperring: opplysninger lagres, men det gis ikke innsynsmulighet) | Ja |
| Sperre utvalgt innhold | Ja |
| Sperre dokumenttype (dato eller diagnose) | Ja |
| Se samtykker, reservasjoner og sperringer | Ja |
| Administrere samtykker, reservasjoner og sperringer tilknyttet deling av helseopplysninger gjennom en analog kanal | Ja |

Tabell 12: Juridiske krav for deling av helseopplysninger

| Juridisk krav | Lov/forskrift |
|--|---|
| Innbygger har rett til innsyn i egne helseopplysninger, inkludert hvem som har hatt tilgang eller fått utlevert helseopplysninger. | Helsepersonelloven § 41 Helseregisterloven § 24 Kjernejournalforskriften § 6 Pasientjournalloven § 17 Pasient- og brukerrettighetsloven § 5-1 Personopplysningsloven § 18 Forskrift om tilgang til helseopplysninger mellom virksomheter § 10 |
| Behandling av helseopplysninger krever 1) lovhjemmel, 2) samtykke eller 3) at nødvendighetskriterier er oppfylt. | Helsepersonelloven §§ 39 Pasientjournalloven § 6 Pasient- og brukerrettighetsloven § 5-3 Personopplysningsloven § 9 |

| Juridisk krav | Lov/forskrift |
|---|---|
| Helsepersonell har tilgang til nødvendige og relevante helseopplysninger i forbindelse med ytelse av helsehjelp, uten krav om samtykke fra innbyggeren. Dette inkluderer utlevering av helseopplysninger til helsepersonell ved andre helsevirksomheter (statlige eller kommunale), eller kommunen. | Helsepersonelloven § 25 Helsepersonelloven § 45 |
| Innbygger kan motsette seg ("sperre") at helsepersonell får tilgang til helseopplysninger eller at helseopplysninger utleveres i forbindelse med helsehjelp | Pasientjournalloven § 17 Pasient- og brukerrettighetsloven § 5-3 Helsepersonelloven § 45 Helsepersonelloven § 25 |
| Sperring av helsepersonells tilgang kan overstyres dersom tungtveiende grunner taler for det, der det er nødvendig for å avverge fare for innbyggerens liv eller alvorlige helseskader ("blålys" situasjoner) Dette gjelder kun innenfor den enkelte virksomhet og ikke på tvers av virksomhetsgrenser. | Pasient- og brukerrettighetsloven § 5-3 Kjernejournalforskriften § 7 |
| Innbygger må samtykke til behandling av helseopplysninger i helseregister, dersom ikke hjemlet i lov ⁶ | Helseregisterloven § 6 og § 9 Kjernejournalforskriften § 3 |
| Innbygger kan (gitt register/opplysninger) motsette seg behandling av helseopplysninger hjemlet i lov* | Helseregisterloven § 10 |
| Innbygger må samtykke til deltakelse i medisinsk og helsefaglig forskning. Samtykket må være informert, frivillig og dokumenterbart. | Helseforskningsloven § 13 |
| Innbygger kan gi et bredt samtykke til definerte forskningsmål som brukes til flere forskningsprosjekter. Deltakere har krav om jevnlig informasjon. | Helseforskningsloven § 14 |
| Statens helsetilsyn og Fylkesmannen kan få utlevert helseopplysninger uten hinder av taushetsplikten i tilsynssaker. | Helsepersonelloven § 30 |
| Barnevernstjenesten kan få utlevert helseopplysninger uten hinder av taushetsplikten når det foreligger mistanke om omsorgssvikt. | Helsepersonelloven § 33 |

Tabell 13: Funksjonalitet for deling av helseopplysninger

| Funksjonalitet | Beskrivelse |
|----------------|--|
| Forespørsler | Mottak av forespørsler om utleveringer fra pasientjournal og andre helseregistre. Forespørsel må vise hvem som har forespurt helseopplysninger, til hvilket formål og hvilke helseopplysninger som skal leveres ut. Der det er mulig skal innbyggeren få se hvilke opplysninger som skal bli utlevert. |
| Dialog | Innbygger kan forhøre seg med helsevirksomhet eller databehandlingsansvarlig for helseregister om utleveringen, eventuelt |

⁶ Se forskrifter hjemlet i helseregisterloven: <https://lovdata.no/referanse/hjemmel?dokID=NL/lov/2014-06-20-43>

| Funksjonalitet | Beskrivelse |
|---|--|
| | forespørre endringer på hva som leveres ut. |
| Samtykke og reservasjon | <p>Innbyggeren kan</p> <ul style="list-style-type: none"> a) Samtykke, dersom virksomhet som skal utlevere helseopplysninger har bedt om det b) Reservere seg, innenfor en bestemt tidsperiode, der innbyggeren har gitt et tidligere samtykke, men fortsatt skal ha mulighet til å reservere seg i enkelttilfeller c) Reservere seg mot helseregistre der innbyggeren er oppført som følge av lovhjemmel men har reservasjonsmulighet. |
| Logg | <p>En logg gir innbyggeren oversikt over hvilke helseopplysninger som er utlevert eller gitt tilgang til fra sin opprinnelige kilde i pasientjournal og andre helseregistre til aktører innen helsetjenesten, helseforvaltningen, forskning og eksternt.</p> <p>For gitt tilgang eller gjennomført utlevering skal grunnlaget spesifiseres, dvs. hvilket samtykke eller lovhjemmel som lå til grunn. Der det er tilgjengelig får innbyggeren se hvilke opplysninger som ble utlevert eller gitt tilgang til.</p> |
| Oversikt over brede samtykker til forskning | En liste over eksisterende, forespurte og avviste brede samtykker som åpner for flere utleveringer til forskningsprosjekter innenfor et avgrenset område. |
| Bredt samtykke | Innbygger kan gi eller trekke tilbake bredt samtykke til forskning. |
| Oversikt over sperringer | En oversikt over gjeldende og historiske sperringer som innbyggeren har gjort. |
| Sperre på helsepersonell | <p>Innbyggeren kan sperre sine helseopplysninger for utvalgt helsepersonell og samarbeidende personell. Innbygger må være over 16 år. Innbygger blir informert om konsekvensene av en slik sperring.</p> <p>Helsevirksomheter må ivareta at navngitt helsepersonell ikke får tilgang til helseopplysningene.</p> <p>Innbygger bør kun få anledning til å sperre for personell der man kan være sikker på at sperringen vil ivaretas. Dersom personen har tilgang i ulike journalsystemer bør i prinsippet alle disse tilgangene ta høyde for sperringen.</p> |
| Sperre på klassifisering | <p>Innbygger kan sperre sine helseopplysninger basert på en bestemt klassifisering, eksempelvis:</p> <ul style="list-style-type: none"> a) Tidsperiode, sperre alt som er tidligere enn en gitt dato, eller innenfor et gitt datointervall b) Diagnose, sperre alt som har med en bestemt diagnose å gjøre (eks. hovedgrupper i ICD-10) <p>Innbygger blir informert om konsekvensene av en slik sperring.</p> <p>Helsevirksomheter må ivareta at helsepersonell ikke får tilgang til disse</p> |

| Funksjonalitet | Beskrivelse |
|----------------|--|
| | helseopplysningene. Unntaksbestemmelser gjelder som før. |

2.1.1.5 J.5 Bruk av helsehjelp og -tjenester

Som innbygger får jeg informasjon om helsetjenester, både digitale og andre, og jeg kan registrere mine samtykker til/reservasjoner mot å delta, slik at min valgfrihet blir reell og jeg får oversikt over valgene jeg tar.

Funksjonalitet:

- Informasjon om tjenester
- Samtykker og reservasjoner for digitale innbyggertjenester
- Samtykker og reservasjoner for programmer og ordninger

Tabell 14: Identifiserte innbyggerbehov for helsehjelp og tjenester

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|--------------------------|
| Samtykke til helsehjelp ved oppmøte | Nei |
| Samtykke til digital helsehjelp (bruk av tjenester som e-konsultasjon mv) | Ja |
| Samtykke til helsehjelp på vegne av barn for gjennomføring av behandling (Eksempelvis en kritisk operasjon eller tilsvarende) | Nei |
| Samtykke til eller reservere seg mot digitale innbyggertjenester | Ja |
| Begrense eget digitalt innsyn | Ja |
| Reservere seg mot fastlegeordningen | Ja |
| Reservere seg mot biologisk forskning | Ja |
| Reservere seg mot automatisk oppføring i egenandelsregisteret (frikortordningen) | Ja |
| Reservere seg mot vaksinasjonsprogrammet | Ja |
| Samtykke til eller reservere seg mot organdonasjon | Mulig, avgjøres eksternt |
| Se gjeldende, mulige og historiske samtykker og reservasjoner | Ja |
| Se og administrere samtykker og reservasjoner for bruk av ikke-digitale helsetjenester | Ja |

Tabell 15: Juridiske krav for helsehjelp og tjenester

| Juridisk krav | Lov/forskrift |
|---|--|
| Innbygger må samtykke til helsehjelp | Pasient- og brukerrettighetsloven § 4-1 |
| Innbygger kan reservere seg mot å bli tilknyttet fastlegeordningen. | Forskrift om pasient- og brukerrettigheter i fastlegeordningen § 2 (merknad) |
| Innbygger kan reservere seg mot forskning på biologisk materiale | Helseforskningsloven § 28 |
| Innbygger må samtykke til donasjon av organer, celler og vev | Transplantasjonsloven § 6 |

Tabell 16: Funksjonalitet for helsehjelp og tjenester

| Funksjonalitet | Beskrivelse |
|---|--|
| Samtykke og reservasjon for digitale tjenester | Innbygger gi/trekke tilbake samtykker for digitale tjenester på helsenorge.no. Et Eksempel er samtykke til å ta i bruk digitale dialogtjenester med personlig helsearkiv. Innbygger kan reservere seg mot å ha tilgang til utvalgte digitale tjenester på helsenorge.no. Dette vil være aktuelt for tjenester som eksponerer mye helseopplysninger, for eksempel innsyn i pasientjournal. Dersom innbyggeren reserverer seg mot tilgang til en digital tjeneste på helsenorge.no, må reservasjonen oppheves gjennom en annen kanal. 800HELSE kan kontaktes for dette. |
| Samtykke og reservasjon programmer og ordninger | Innbygger kan samtykke til eller reservere seg mot ulike andre tjenester. Eksempel er reservasjon mot fastlegeordningen og mot å ha en kjernejournal. |
| Analog registrering av samtykker og reservasjoner | Innbygger kan gi eller oppheve samtykker og reservasjoner gjennom en såkalt analog kanal. 800HELSE kan være kontaktpunkt med informasjon om dokumentasjonskrav osv. reservasjoner |

2.1.2 F Innsyn i journal og helseregistre

2.1.2.1 F.1 Innsyn i pasientjournal

Som innbygger har jeg tilgang til en oversikt over hva mine pasientjournaler inneholder og kan åpne de enkelte dokumenter/seksjoner, slik at jeg har fullt innsyn i journalpliktig informasjon som er lagret om meg hos mine behandlere og kan tilegne meg kunnskap og kontroll i mitt forløp.

Tabell 17: Identifiserte innbyggerbehov for innsyn pasientjournal

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|----------------------|
| Få oversikt over hvilke pasientjournaler som har helseopplysninger | Ja |
| Få innsyn i innhold i pasientjournal | Ja |
| For ungdom mellom 12 og 16 år å kunne gjennom digital kanal anmode behandler om å begrense foreldres innsyn | Nei |
| For helsepersonell å nekte innbyggeren innsyn i hele eller deler av pasientjournalen | Nei |

Tabell 18: Juridiske krav for innsyn pasientjournal

| Juridisk krav | Lov/forskrift |
|---|---|
| Innbygger har rett til innsyn i egne helseopplysninger | Helsepersonelloven § 41 Helseregisterloven § 24 Kjernejournalforskriften § 6 Pasientjournalloven § 17 Pasient- og brukerrettighetsloven § 5-1 Personopplysningsloven § 18 Forskrift om tilgang til helseopplysninger mellom virksomheter § 10 |
| Helsepersonell kan nekte innbyggeren tilgang til egen journal | Pasient- og brukerrettighetsloven § 5-1 |

Tabell 19: Funksjonalitet for innsyn pasientjournal

| Funksjonalitet | Beskrivelse |
|--|---|
| Oversikt over behandlingssteder/ journaler | En oversikt over behandlingssteder innbyggeren har vært hos gjør innbyggeren oppmerksom på hvor egne helseopplysninger er lagret i helse- og omsorgstjenesten. Der elektronisk innsyn og dialog ikke foreligger, må innbygger selv ta kontakt med behandlingsstedet for å få innsyn i journal, rette opplysninger, forespørre sperring og se en logg over helsepersonell som har vært inne på journalen. |
| Oversikt over dokumenter/seksjoner med utvalgt nøkkelinformasjon | En samlet visning av journalene med dokumenter/seksjoner hos ulike behandlere vises for innbyggeren. Innbyggeren kan sortere på ulike parametere, slik som dato, type behandling og sted. Innbygger kan også filtrere ut/søke etter. Innbygger kan få en forklaring på ulike dokumenttyper og seksjoner med strukturert innhold. |
| Dokument-/innholdsvisning | Innbygger kan åpne innhold som ligger i journal, både dokumenter og strukturerte opplysninger. Innbygger får ikke innsyn i dokumenter/seksjoner der han/hun er nektet innsyn av helsepersonell. |

2.1.2.2 F.2 Dialog vedrørende pasientjournal

Som innbygger kan jeg kontakte behandlingsstedet for å få informasjon og veiledning knyttet til min pasientjournal, melde fra om feilregistreringer og/eller be om at utvalgt informasjon blir sperret for helsepersonell, slik at jeg kan opparbeide meg kunnskap om mitt forløp og bidra til at journalinnholdet er korrekt og benyttes som jeg ønsker.

Tabell 20: Identifiserte innbyggerbehov for dialog pasientjournal

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|----------------------|
| Be om forklaring av journalinnhold | Ja |
| Be om retting av helseopplysninger | Ja |
| Be om sletting av helseopplysninger | Ja |
| Be om sperring av helseopplysninger i den enkelte journal for helsepersonell og samarbeidende personell | Ja |
| For innbygger mellom 12 og 16 år, be om å få begrense foreldreinnsyn | Nei |

Tabell 21: Juridiske krav for dialog pasientjournal

| Juridisk krav | Lov/forskrift |
|---|--|
| Innbygger kan be om forklaring av faguttrykk og lignende i journal | Pasient- og brukerrettighetsloven § 5-1 |
| Innbygger kan be om retting av helseopplysninger. | Personopplysningsloven § 27 flg. Helsepersonelloven § 42 Pasient- og brukerrettighetsloven § 5-2 Kjernejournalforskriften § 6 |
| Innbygger kan be om sletting av helseopplysninger, når «1. opplysningene er feilaktige eller misvisende og føles belastende for den de gjelder eller 2. opplysningene åpenbart ikke er nødvendige for å gi pasienten helsehjelp.» | Personopplysningsloven § 28 flg. Helsepersonelloven § 43, 44 Pasient- og brukerrettighetsloven § 5-2 Kjernejournalforskriften § 6 |
| Innbygger kan motsette seg ("sperre") at helsepersonell får tilgang til helseopplysninger eller at helseopplysninger utleveres i forbindelse med helsehjelp | Pasientjournalloven § 17 Pasient- og brukerrettighetsloven § 5-3 Helsepersonelloven § 45 Helsepersonelloven § 25 |

| Juridisk krav | Lov/forskrift |
|---|---|
| Sperring av helsepersonells tilgang kan overstyres dersom tungtveiende grunner taler for det, der det er nødvendig for å avverge fare for innbyggerens liv eller alvorlige helseskader ("blålys" situasjoner) | Pasient- og brukerrettighetsloven § 5-3 Kjernejournalforskriften § 7 |

Tabell 22: Funksjonalitet for dialog pasientjournal

| Funksjonalitet | Beskrivelse |
|---------------------|--|
| Dialog | Innbyggeren kan sende meldinger til behandlingssted/journalarkiv tilknyttet et journaldokument, for å: Få innholdet forklart Rette eller slette opplysninger Sperre tilgang for helsepersonell og samarbeidende personell. |
| Elementsperring | Sperring foretas først når behandlingssted setter sperring. Informasjon om at innhold er sperret, og hvem det er sperret for, vises sammen med innholdet. Innbygger kan i forespørsel om sperring også be om at lignende eller hele journalen hos behandler sperres. Dette skjer i samråd med behandler. |
| Retting og sletting | Retting eller sletting foretas først når og dersom behandlingssted gjennomfører endringen. Ved endring vil innsynet endres tilsvarende. |
| Kontaktinformasjon | Innbyggeren får kontaktinformasjon til behandlingssted/journalarkiv der digital dialog ikke er mulig, slik at han/hun kan gjennomføre dialog utenom den digitale kanalen. |

2.1.2.3 F.3 Brukslogg for pasientjournal

Som innbygger kan jeg se hvem som har benyttet min pasientjournal, totalt og på dokument/seksjonsnivå, slik at jeg kan forsikre meg om at behandler har satt seg inn i min situasjon og at uvedkommende ikke har snoket.

Tabell 23: Identifiserte innbyggerbehov for brukslogg pasientjournal

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|----------------------|
| Få se hvilket helsepersonell eller samarbeidende personell som har hatt innsyn i journalen | Ja |
| Få se hvilket helsepersonell eller samarbeidende personell som har opprettet, endret og/eller lest det enkelte dokument/den enkelte seksjon i journalen | Ja |

Tabell 24: Juridiske krav for brukslogg pasientjournal

| Juridisk krav | Lov/forskrift |
|---|---|
| Innbygger har rett til innsyn i hvem som har hatt tilgang eller fått utlevert helseopplysninger | Personopplysningsloven § 18 flg. Pasient- og brukerrettighetsloven § 5-1 Pasientjournalloven § 18 Helsepersonelloven § 41 Kjernejournalforskriften § 6 Forskrift om tilgang til helseopplysninger mellom virksomheter § 10 |

Tabell 25: Funksjonalitet for brukslogg pasientjournal

| Funksjonalitet | Beskrivelse |
|---|---|
| Logg over helsepersonells bruk | En logg viser helsepersonell og samarbeidende personell som har vært inne på innbyggerens journal, og hvilke aktiviteter som er gjennomført. Informasjon om bruker må blant annet inneholde navn, rolle, avdeling. Innbyggeren kan søke og filtrere på ulike parametere, slik som dato og navn. |
| Logg over egen eller representanters bruk | En logg som viser når innbygger selv eller representanter har vært inne på innbyggerens journal. Innbyggeren kan søke og filtrere på ulike parametere, slik som dato og navn. |

2.1.2.4 F.4 Innsyn helseregistre og biobanker; innhold og bruk

Som innbygger kan jeg finne fram til helseopplysninger som er registrert om meg i personidentifiserte helseregistre og biobanker, samt bruken av den, slik at min innsynsrett er ivaretatt og jeg kan verifisere om opplysningene er korrekte.

Tabell 26: Identifiserte innbyggerbehov for innsyn helseregistre og biobanker

| Identifisert innbyggerbehov | Støttet i målbildet? |
|--|----------------------|
| Få oversikt over helseregistre og biobanker man står oppført i | Ja |
| Få oversikt over innholdet i helseregistre og biobanker man står oppført i | Ja |
| Få oversikt over bruken av egne helseopplysninger i helseregister eller biobank. | |

Tabell 27: Juridiske krav for innsyn helseregistre og biobanker

| Juridisk krav | Lov/forskrift |
|--|--|
| Innbygger har rett til innsyn i egne helseopplysninger | Personopplysningsloven § 18 flg. Helseregisterloven § 24 Helseforskningsloven § 40 |

Tabell 28: Funksjonalitet for innsyn helseregistre og biobanker

| Funksjonalitet | Beskrivelse |
|------------------------------|--|
| Oversikt over helseregistre | <p>En oversikt over helseregistre innbyggeren står oppført i, gjør innbyggeren oppmerksom på andre helseopplysninger som er lagret i helse- og omsorgssektoren. Den må kunne vise oversikt over sentrale helseregistre og nasjonale kvalitetsregistre som ikke er aidentifisert, eventuelt redegjøre for mulige helseregistre som ikke er innebefattet i oversikten. Oversikten bør videre vise helseregistre innbyggeren har reservert seg mot å stå oppført i, eller der innbyggeren har trukket samtykket sitt. Innbyggeren kan søke og filtrere.</p> <p>Per helseregister bør det framgå om:</p> <ul style="list-style-type: none"> a) Innbyggeren har samtykket til å stå oppført (som implisitt betyr at samtykke kan trekkes) b) Innbyggeren kan reservere seg mot å stå oppført c) Oppføring er lovhjemlet, dvs. uten mulighet for å reservere seg <p>Der elektronisk innsyn og dialog ikke foreligger, må innbygger selv ta kontakt med databehandlingsansvarlig, for eksempel for å få innsyn eller rette feilaktige opplysninger. Dette fordrer kontaktinformasjon for manuelt innsyn der digitalt innsyn mangler.</p> |
| Innholdsvisning per register | Der elektronisk innsyn er tilgjengeliggjort, kan innbyggeren få innsyn i egne helseopplysninger. |
| Innsynslogg | En logg som viser hvem som har vært inne på innbyggerens opplysninger i helseregistre. Dette inkluderer utleveringer fra helseregisteret, som også er omhandlet i «J.4 Deling og utlevering av helseopplysninger». |

2.1.2.5 F.5 Dialog vedrørende helseregistre og biobanker

Som innbygger kan jeg motta informasjon og forespørsler, og jeg kan kontakte registreier for å få informasjon, melde fra om feilregistreringer og/eller be om at utvalgt informasjon blir slettet eller sperret, slik at jeg kan bidra til at registerinnholdet er korrekt og benyttes som jeg ønsker.

Tabell 29: Identifiserte innbyggerbehov for dialog helseregistre og biobanker

| Identifisert innbyggerbehov | Støttet i målbildet? |
|---|----------------------|
| Forespørre retting av helseopplysninger | Ja |
| Forespørre sletting eller sperring av helseopplysninger | Ja |

Tabell 30: Juridiske krav for dialog helseregistre og biobanker

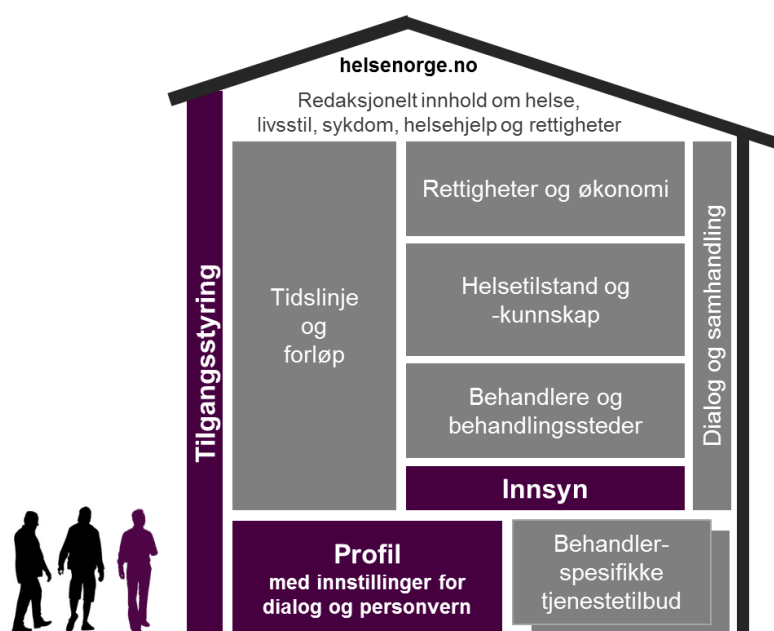
| Juridisk krav | Lov/forskrift |
|--|---|
| Innbygger kan be om sletting eller sperring av helseopplysninger | Personopplysningsloven § 28 flg. Helseregisterloven § 25 |

Tabell 31: Funksjonalitet for dialog helseregistre og biobanker

| Funksjonalitet | Beskrivelse |
|----------------|---|
| Dialog | Innbyggeren kan sende meldinger til databehandlingsansvarlig, dersom det er spørsmål, forespørsel om innsyn, retting, sletting, sperring m.m. |

2.2 Funksjonelle komponenter

Helsenorge.no er innbyggerens inngangsport til digital samhandling med helsetjenesten. Funksjonelle komponenter representerer en logisk «rominndeling» på helsenorge.no og sammenstiller digitale tjenester mot aktørene i helsetjenesten i en felles brukerflate.



Figur 9: Funksjonelle komponenter realiserer innbyggers brukerflate på helsenorge.no

Innbyggeren møter personverntjenester i de «rommene» som tilbyr innhold og funksjonalitet knyttet til henholdsvis *Innsyn* og *Profil med personverninnstillinger*. Innbyggerens rett til å representere seg selv og andre ivaretas gjennom *Tilgangsstyring*.

Nedenfor gis en overordnet beskrivelse av målbildet for disse tre komponentene, i form av hvordan de er bygget opp og realiserer det funksjonelle omfanget som ble identifisert for innbyggers personverntjenester i forrige kapittel. De funksjonelle komponentene understøttes av tekniske løsninger som beskrives i det tekniske målbildet; se kapittel 3.

2.2.1 Tilgangsstyring

Tilgangsstyring ivaretar innbyggers rett til å representere seg selv og andre. Dette skjer gjennom

- en personvelger i brukerflaten der innbygger kan se hvem hun/han kan representere og eventuelt velge å representere en annen
- en tjenestemodell der forutsetninger for tilgang er definert for hver enkelt tjeneste på helsenorge.no

- løpende evaluering av et regelsett for tjenestetilgang, som omfatter representasjon (foreldre, fullmektig) så vel som andre personverninnstillinger (samtykker, reservasjoner).

Tilgangsstyringskomponenten utnytter datagrunnlag som etableres i komponenten *Profil*: fullmakter, reservasjoner og samtykker.

2.2.1.1 Personvelger i brukerflaten

Et hovedprinsipp på helsenorge.no er at innbyggeren ser helseopplysninger og benytter tjenester for én person om gangen. Innbyggere som kan representere andre, kan velge å *bytte* til en annen person. Det vil da tydelig fremgå at innbyggeren handler på vegne av den andre.

Alle innbyggere som logger inn på helsenorge.no, vil i utgangspunktet representere seg selv. Det vil si at de ser sine egne helseopplysninger og benytter tjenester på egne vegne. Innbyggere som har mulighet til å representere andre, vil ha tilgang til en personvelger. Her kan innbygger velge i en liste over øvrige personer som innbyggeren kan representere, sammen med informasjon om hvilket grunnlag representasjonen bygger på: foreldreansvar eller fullmakt (inkl. spesialtyper som fullmakt ved vergerepresentasjon).

Bytte av person må bekreftes av innbyggeren før det trer i kraft. Personbytte medfører alltid at innbyggeren tas tilbake til Min helse forside og derfra kan velge hvilke tjenester som han/hun vil benytte.

2.2.1.2 Tjenestemodell inkl. forutsetning for tilgang

Det juridiske grunnlaget for å tilby digitale helsetjenester er sammensatt, og tjenestene inkludert bakenforliggende systemløsninger har varierende modenhet. For å styre tilgang til tjenestene på helsenorge.no ved representasjon og for ulike aldersgrupper etableres en tjenestemodell som definerer forutsetninger for tilgang. Innholdet i tjenestemodellen inngår i grunnlaget for å evaluere hvorvidt den enkelte innbygger skal ha tilgang til hver enkelt tjeneste.

For hver enkelt tjeneste defineres følgende egenskaper:

- Krever autentisering; alternativt er tjenesten åpent tilgjengelig
- Tilgjengelig for innbyggere med sperret adresse, dvs. kode 6 og 7 i Folkeregisteret
- Tilgjengelig for ungdom 12-16 år forutsatt foreldresamtykke
- Tilgjengelig ved foreldreansvar, hhv. under og over 12 år (representasjon)
- Tilgjengelig ved daglig omsorg; i praksis foreldreansvar og felles folkeregistrert adresse (representasjon)
- Tilgjengelig via fullmakt (representasjon)

Det forventes at flere tjenester etter hvert vil kunne gjøres tilgjengelig ved representasjon. En forutsetning for å gi foresatte tilgang til en tjeneste på vegne av barn på 12-16 år, er at tjenesten ivaretar kravet om at foresattes innsynsrett skal kunne begrenses dersom behandler godtar barnets ønske om dette. For eksempel kan en ungdom be sin behandler sørge for at foresatte ikke får innsyn i hennes p-pillebruk eller abort. Tjenestemodellen understøtter en slik utvikling ved at det er enkelt å endre tjenestenes egenskaper i modellen.

Enkelte tjenester har tilleggskrav knyttet til seg, for eksempel «forutsetter samtykke til dialogtjenester med personlig helsearkiv», eller «forutsetter aktiv kjernejournal». Det er behov for en grenseoppgang for hva som skal ivaretas gjennom tjenestemodellen og hva som skal håndteres av den enkelte tjeneste.

For å ivareta alle aspekter kan enkelte tjenester modelleres som hoved- og undertjenester, der kun hovedtjenesten gjøres tilgjengelig via primærnavigasjon (for eksempel som «flis» på Min helse forside).

2.2.1.3 Evaluering av regelsett for tjenestetilgang

Tjenestene på helsenorge.no er tilgjengelig for innbygger via

- innganger på Min helse forside (p.t. «fliser»)
- dyplinker og søk
- bokmerker/nettadresser.

Ved uttegning av Min helse forside evalueres regelsettet for tjenestetilgang, slik at siden viser kun de tjenestene som er tilgjengelig for innbyggeren. Samme regelsett evalueres og legges til grunn dersom innbygger velger alternative navigasjonsveier.

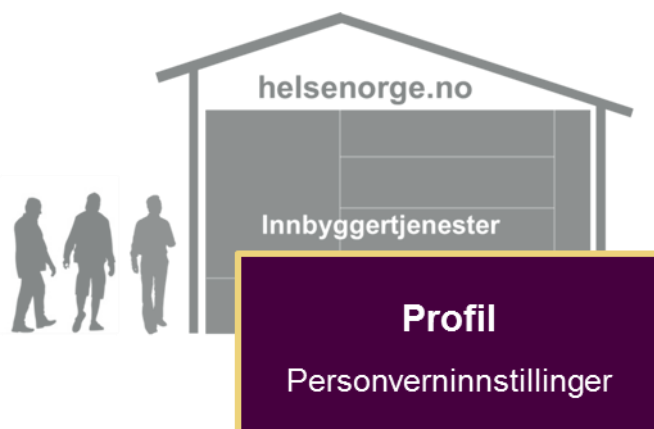
Ved manglende tilgang gis melding om dette i brukerflaten. Der innbygger opererer via fullmakt kan han/hun forespørre fullmaktsgiver om å få tildelt en videre fullmakt – dersom dette er mulig i henhold til tjenestemodellen.

Regelsettet ivaretar

- representasjonsforhold: hvorvidt innlogget innbygger representerer seg selv, har foreldreansvar eller fullmakt.
- generelle forutsetninger for tilgang til den enkelte tjeneste (tjenestemodellen)
- innbyggers (evt. den som representeres) eventuelle reservasjoner/samtykker som er relevante for den enkelte tjeneste.

Evaluering av regelsettet for den enkelte innbygger gjøres basert på tjenestemodellen og på datagrunnlag som etableres i innbyggers *Profil*, samt informasjon i Folkeregisteret.

2.2.2 Profil med personverninnstillinger



Figur 10: Profilkomponenten på helsenorge.no, med fokus på personverninnstillinger

Gjennom Profilkomponenten gis innbygger anledning til å registrere sine egne innstillinger for personvern, samt overvåke bruken av dem. Dette omfatter

- fullmakter (representasjon)
- bruk av helsetjenester og ordninger (reservasjoner/samtykker)
- deling av informasjon - utlevering og sperring av informasjon (samtykker/reservasjoner/sperringer)
- logg over bruk/historikk.

Datagrunnlag som etableres gjennom Profilkomponenten benyttes også i komponenten *Tilgangsstyring*. Datagrunnlag knyttet til fullmakter, reservasjoner/samtykker og sperringer tilgjengeliggjøres dessuten for eksterne aktører, slik at disse kan ta hensyn til innbyggers personverninnstillinger i sine løsninger.

2.2.2.1 Fullmakter

Profilkomponenten omfatter funksjonalitet for å administrere fullmakter, slik at innbyggeren kan representeres av andre der dette er hensiktsmessig. Fullmaktsadministrasjon kan gjøres av innbyggeren selv via brukergrensesnittet på helsenorge.no, eller via et saksbehandlergrensesnitt basert på skriftlig dokumentasjon fra innbyggeren eller andre.

Vi har to typer fullmakt, avhengig av grunnlaget for tildeling:

- Fullmakt tildeles direkte fra innbygger/fullmaktsgiver, i tilfeller der denne er myndig (over 18 år) og samtykkekompetent. Fullmaktsgiver kan selv trekke tilbake en slik fullmakt. **AVKLARINGSBEHOV: Det vurderes om 16-8 åringer til å gi foreldre innsyn. Usikkert om det at man må være 18 til å gi fullmakt er et krav, ettersom det er uklart om det å gi noen rett til innsyn anses som fullmakt. Dette er under avklaring.**

- Fullmakt tildeles på grunnlag av vergemål, fremtidsfullmakt eller andre forhold, i tilfeller der andre enn innbygger/fullmaktsgiver er ansvarlig for å vurdere grunnlag for og omfang av fullmakten som registreres. En slik fullmakt kan ikke uten videre trekkes tilbake av innbyggeren selv. Den som benytter fullmakten skal ikke nødvendigvis ha innsyn i grunnlaget for opprettelse av fullmakten.

Under fullmakter får innbygger oversikt over fullmakter som er tildelt andre, og fullmakter som er mottatt fra andre. En fullmakt omfatter informasjon om

- fullmaktsgiver og fullmektig
- eventuell tidsbegrensning; gyldighet
- omfang
- grunnlag for tildeling; detaljer vises ikke nødvendigvis til fullmektig.

I første omgang tilbys fullmakt for digitale helsetjenester på helsenorge.no. Dette kan utvides til også å gjelde områder som er relevante for helsetjenesten generelt.

For tjenestene på helsenorge.no er det aktuelt å tildele fullmakt til alle tjenester, eller alle tjenester innen et område/utvalgte områder, som til enhver tid tilbys via fullmakt. Dette fordi det skal være enkelt å få hjelp, og enkelt for pårørende å bistå den som trenger det. Ved å tillate at fullmaktene har dynamisk innhold, dvs. at omfanget vokser når nye tjenester utvikles, vil det ikke være behov for å endre den enkelte fullmakt i takt med tilbudet av digitale tjenester.

Aktuelle fullmaktsområder kan være

- timer/forløp/helsekontakter og tilknyttet informasjon
- helsehjelp og -opplysninger
- innsyn i pasientjournal og andre helseregistre
- økonomi og rettigheter
- profil og personverninnstillinger

Informasjon om hva et fullmaktsområde til enhver tid omfatter vil være lett tilgjengelig, slik at de som ønsker og har kapasitet til en tettere kontroll kan gi en tidsbegrenset fullmakt og justere løpende,

Den som har tildelt en fullmakt, kan når som helst trekke den tilbake. Den som har mottatt en fullmakt, kan når som helst si den fra seg. Fullmaktsfunksjonalitet vil understøttes av komponenten *Dialog*, ved at det sendes meldinger mellom fullmaktsgiver og fullmektig når fullmakt tildeles, trekkes tilbake og sies fra seg. Det er også aktuelt å tilby mulighet for å be om en fullmakt, med støtte for at fullmaktsgiver enkelt kan godkjenne et ferdig oppsett.

2.2.2.2 *Bruk av helsetjenester og ordninger*

Profilkomponenten tilrettelegger for at innbygger selv kan ta stilling til hvilke helsetjenester han/hun ønsker å benytte. Reservasjoner og samtykker kan registreres av innbyggeren selv via brukergrensesnittet på helsenorge.no, eller via et saksbehandlergrensesnitt basert på skriftlig dokumentasjon fra innbyggeren.

Muligheten omfatter i første omgang digitale tjenester på helsenorge.no, men kan utvides til å omfatte andre programmer og ordninger, slik som for eksempel fastlegeordningen, kjernejournal, automatisk innhenting av egenandeler (automatisk frikort) og barnevaksinasjonsprogrammet.

For de digitale tjenestene på helsenorge.no organiseres innstillingene slik:

- Ved innlogging bes innbygger om å samtykke til **bruksvilkår for Min helse**. Dette er en forutsetning for å benytte tjenester der innhold og funksjonalitet tilpasset innbyggeren selv, dvs. tjenestene som er tilgjengelig kun etter innlogging. - Uten dette samtykket er det ikke mulig å forbli innlogget på Min helse.
- Innlogget bruker kan velge å samtykke til å ta i bruk **dialogtjenester med personlig helsearkiv**. Dette er en forutsetning for å benytte tjenester som medfører lagring av opplysninger på helsenorge.no. Samtykket er påkrevet fordi det kreves samtykke til å motta helsehjelp digitalt, og fordi det inntil videre ikke finnes annet rettslig grunnlag for å lagre innbyggers opplysninger på helsenorge.no. - Uten dette samtykket er det likevel mulig å benytte rene oppslagstjenester, slik som oversikt over resepter og innsyn i kjernejournal. Dialogtjenester som medfører lagring av opplysninger, vil likevel være tilgjengelig i brukerflaten. Hvis innbyggeren prøver å benytte dem, gis anledning til å gi samtykke.
- **Reservasjon mot utvalgte digitale tjenester:** Innbygger kan velge å reservere seg mot å ha tilgang til enkelttjenester på helsenorge.no. Det gjelder fortrinnsvis tjenester som eksponerer mye sensitiv helseinformasjon, slik som innsyn i kjernejournal og innsyn i pasientjournal. Bakgrunnen for dette er at enkelte vil frykte misbruk og sikkerhetsbrudd når slike tjenester er tilgjengelig via Internett, selv om tjenestene krever høyeste nivå autentisering og alle regler for sikker behandling av personopplysninger følges. - Ved reservasjon mot en enkelttjeneste vil tjenesten ikke være synlig i brukerflaten. Reservasjonen kan heller ikke oppheves på helsenorge.no, men i en alternativ kanal, som ved å kontakte brukerstøtte/800HELSE.

2.2.2.3 Deling av informasjon - sperring og utlevering

Profilkomponenten gir innbyggeren mulighet til å regulere helsetjenestens bruk og utlevering av hans/hennes helseopplysninger, og den gir innsyn i de utleveringer som er foretatt.

Helsepersonell i ulike avdelinger og virksomheter kan i forbindelse med ytelse av helsehjelp dele helseopplysninger, uten å innhente samtykke fra innbyggeren. Innbygger skal imidlertid ha anledning til å motsette seg slik deling ved å sperre for helsepersonells tilgang eller at helseopplysninger utleveres i forbindelse med helsehjelp.

For utlevering til andre formål skal som regel samtykke innhentes fra innbygger, eller innbygger kan ha mulighet for å reservere seg. Innen forskning kan innbygger gi et såkalt bredt samtykke til utlevering og bruk av egne data, forutsatt at han/hun mottar informasjon om planlagte forskningsprosjekter med mulighet for å reservere seg mot et eller flere av disse.

Sperre mot deling av helseopplysninger i forbindelse med helsehjelp (primærbruk)

I profilkomponenten vil innbygger kunne registrere generelle regler for sperring av helseopplysninger for helsepersonell, som deretter tilgjengeliggjøres for helsetjenestens systemløsninger. Sperring kan registreres på følgende nivåer:

- **Sperre alle opplysninger for utvalgt helsepersonell:** Innbygger kan registrere én eller flere personer som ikke skal ha tilgang til hans/hennes helseopplysninger. En person kan identifiseres ved ID-nummer i helsepersonellregisteret (HPR-nummer), der alt helsepersonell med autorisasjon eller lisens er oppført.
- **Sperre utvalgte opplysninger for alt helsepersonell:** Innbygger kan registrere kategorier av helseopplysninger som skal sperres for helsepersonell. Kategori kan angis ved eksempelvis tidsperiode (eldre enn 1990), tema (legemiddelinformasjon) eller diagnose (epilepsi); alternativer må vurderes nærmere.

AVKLARINGSBEHOV: Det må vurderes nærmere hvorvidt en sperring skal kunne forseres i kritiske situasjoner, eller om den skal fungere som en reell blokkering – eventuelt om man skal nyansere på type sperring.

Et bredt samspill mellom innbyggers og helsepersonells systemer er en forutsetning for at sperring registrert i profilkomponenten skal ha tilsiktet effekt. Dette ligger noe fram i tid. Derfor er funksjonalitet knyttet til sperring av konkrete innholdselementer per register også lagt til *Innsynskomponenten*.

Utlevering av helseopplysninger – samtykke/reservasjon (sekundærbruk)

I profilkomponenten vil innbygger kunne registrere samtykker til og reservasjoner mot utlevering av egne helseopplysninger fra pasientjournaler og andre helseregistre til forvaltningen, forskning/registre og andre aktører. Profilkomponenten vil gjennom dette bygge opp en oversikt over utleveringer basert på samtykke. Denne vil kunne suppleres med informasjon fra helsetjenesten om utleveringer foretatt uten behov for samtykke (ved reservasjonsrett eller annet lovgrunnlag), og dermed gi innbygger samlet innsyn i utleveringer av sine helseopplysninger.

Følgende funksjonalitet og innhold vil være tilgjengelig:

- **Motta og behandle forespørsler** om samtykke til utlevering, alternativt informasjon om forestående utlevering med reservasjonsrett. Dette gjelder engangsforespørsler så vel som informasjon knyttet til bredt samtykke til forskning. Innbygger kan behandle forespørselen ved å gi samtykke eller avstå fra dette, og tilsvarende ved reservasjon.
- **Oversikt over samtykker og reservasjoner** med mulighet til å reversere disse.
- **Utleveringslogg** med oversikt over hvilken informasjon som er utlevert, til hvem, basert på hvilket grunnlag.

Samspill mellom innbyggers og helsepersonells systemløsninger vil være en forutsetning for å realisere funksjonalitet knyttet til utlevering av helseopplysninger i profilkomponenten. Her inngår også komponenten *Dialog*, som håndterer meldingsflyten mellom innbygger og aktørene i helsetjenesten knyttet til informasjon og forespørsler.

2.2.2.4 Logg over bruk/historikk

Gjennom Profilkomponenten gis innbygger også anledning til å overvåke bruken av sine egne innstillinger for personvern. Dette omfatter

- **Logg over bruk av helsenorge.no:** Overordnet oversikt over innbyggers egen bruk av digitale tjenester på helsenorge.no, dvs. informasjon om innlogginger og hvilke tjenester som er benyttet til hvilken tid, men ingen detaljer. Tilsvarende for andres bruk, dersom andre har grunnlag for å representere innbyggeren gjennom fullmakt eller foreldreansvar.
- **Historikk/logg over endringer i personverninnstillinger:** Mer detaljert oversikt over endringer i fullmakter og innstillinger for bruk av helsetjenester, samt innstillinger for deling og utlevering av helseopplysninger.

- **Logg over ekstern bruk av personverninnstillinger:** Det er aktuelt på sikt å inkludere en oversikt over eksterne forespørsler mot personverninnstillingene, slik at innbygger får innsyn i bruken av sine innstillinger hos aktører i sektoren.

2.2.2.5 Endringer av innbyggers personverninnstillinger i analog kanal

I tillegg til at innbygger selv kan vedlikeholde sine personverninnstillinger via brukerflaten på helsenorge.no, tilrettelegges det for at innbyggers *Profil med personverninnstillinger* skal være tilgjengelig via et saksbehandlergrensesnitt, såkalt «analog kanal». Dermed kan innbyggere som ikke bruker helsenorge.no, likevel få registrert fullmakter og samtykker/reservasjoner/sperringer relatert til deres bruk av helsetjenesten og deling av helseopplysninger.



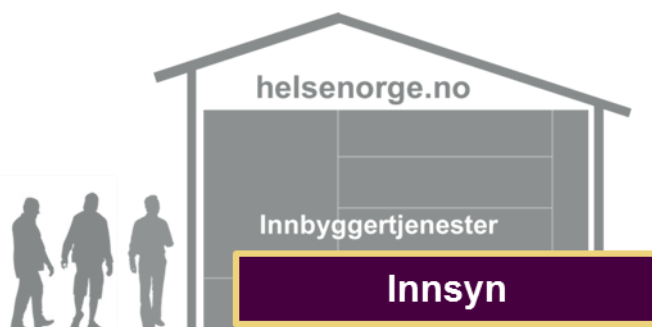
Figur 11: Bruk av innbyggers personverninnstillinger i og utenfor helsenorge.no

2.2.2.6 Bruk av innbyggers personverninnstillinger utenfor helsenorge.no

Innbyggers personverninnstillinger omfatter fullmakter, reservasjoner/samtykker og sperringer knyttet til digitale innbyggertjenester så vel som til øvrige helsetjenester og ordninger. Datagrunnlaget tilgjengeliggjøres for eksterne aktører, slik at disse kan hensynta innbyggers personverninnstillinger i sine systemløsninger. Dette vil ha stor betydning for ivaretagelse av innbyggers rettigheter knyttet til personvern.

Videre kan eksterne aktører via komponentene *Dialog* og *Profil med personverninnstillinger* forespørre innbygger om samtykke til utlevering av opplysninger og/eller informere om utleveringer som vil finne sted med mindre innbygger reserverer seg, samt rapportere om andre utleveringer som er foretatt.

2.2.3 Innsyn



Figur 12: Innsynskomponenten på helsenorge.no

Innsynskomponenten understøtter innbyggers innsynsrett i helsetjenestens opplysninger om ham/henne i behandleres pasientjournaler så vel som i nasjonale registre, slik som kjernejournal, kvalitetsregistre og annet. Komponentene gir oversikt over hvilken dokumentasjon som finnes, og tilbyr innsyn i det enkelte registeret og bruken av det, i den grad underliggende systemer tilbyr dette.

Komponenten består av følgende hoveddeler:

- Pasientjournal: alle pasientjournaler innbygger har i helsetjenesten
- Kjernejournal
- Andre helseregistre

Innsynskomponenten er helt avhengig av funksjonalitet i helsetjenestens systemløsninger, og kan derfor ikke realiseres utelukkende ved å utvikle personverntjenester på helsenorge.no. Det er imidlertid en sterk sammenheng med komponenten *Profil med personverninnstillinger* som omfatter samtykker til/reservasjon mot utlevering av helseopplysninger, informasjon om utleveringer, samt generelle regler for sperring av helseopplysninger for helsepersonell. Personverninnstillinger registrert i *Profil* tilgjengeliggjøres for helsetjenestens systemløsninger slik at disse kan hensynta innbyggers personvern ved spørsmål om deling og utlevering av opplysninger.

Innsynskomponenten samspiller også med komponenten *Behandlere og behandlingssteder* ved at behandler/behandlingssted – på type- eller individnivå – gir en naturlig inngang og filterdimensjon i pasientjournalen. Videre samspiller den med komponenten *Dialog* ved at vesentlig funksjonalitet knyttet til innsyn og selvbestemmelse løses ved å sende og motta meldinger til/fra registreier, framfor direkte i innsynstjenestene.

2.2.3.1 Pasientjournal

Innsyn i pasientjournal - innhold

Innsynskomponenten sammenstiller en innholdsfortegnelse over innbyggers journal-dokumentasjon, slik at innbygger kan søke, filtrere og hente fram enkeltelementer etter ønske. Målbildet er at dette gjøres på tvers av alle pasientjournalene innbygger har i helsetjenesten, slik at informasjon kan presenteres kronologisk, per behandler, per dokumenttype etc. avhengig av innbyggers behov.

Den totale pasientjournalen kan presenteres helhetlig, eller forhåndsfiltrert etter bestemte dimensjoner. En naturlig inngang og filterdimensjon er behandler/behandlingssted – på type- eller individnivå – som støttes av komponenten *Behandlere og behandlingssteder*.

I praksis vil det ta lang tid før alle pasientjournaler kan gjøres tilgjengelig gjennom en sammenstilt innholdsfortegnelse, slik at brukerflaten også vil tilby innsyn per faktiske pasientjournal. Innsynskomponenten vil uansett tilgjengeliggjøre innholdet i innbyggers pasientjournaler, inntil videre gjennom flere mekanismer:

- Sammenstilt innholdsfortegnelse
- Oppslag på en enkelt behandler/et behandlingssted
- Dialog eller skjema for å forespørre om papirbasert innsyn.

Innsyn i pasientjournal – bruk

Innsynskomponenten tilgjengeliggjør informasjon om bruk av pasientjournal der behandlingsstedet tilbyr dette. Foreløpig omfatter tilgangsløggene kun helsepersonells bruk, men på sikt kan også innbyggers eget innsyn fremkomme. Innsyn i bruk av pasientjournal vil skje gjennom følgende mekanismer:

- Mulighet for å hente fram tilgangsløgg per dokument i sammenstilt innholdsfortegnelse
- Oppslag på tilgangsløgg for én pasientjournal, fortrinnsvis med mulighet for søk og filtrering på tidsperiode, person etc.

Relatert funksjonalitet: Innbygger får informasjon om utlevering til andre aktører samt eventuelle forespørsler om dette i brukerflaten knyttet til sin *Profil*. Dette håndteres i komponenten *Profil med personverninnstillinger*.

Dialog om pasientjournal - spørsmål, retting, sperring

Innbyggers behov knyttet til informasjon og veiledning, samt eventuelle meldinger om feilregistreringer, støttes gjennom meldingsfunksjonalitet. Det samme gjelder anmodning om å sperre enkeltelementer i pasientjournalen for helsepersonell.

Når ny melding opprettes, ivaretar innsynskomponenten

- eventuell kobling mot et spesifikt journalelement
- kobling mot rett mottaker/jornaleier (for eksempel journalarkiv)

Forøvrig håndteres meldingsfunksjonalitet i komponenten *Dialog*.

Relatert funksjonalitet: Innbygger definerer generelle regler for sperring av helseopplysninger for helsepersonell i brukerflaten knyttet til sin *Profil*. Dette håndteres i komponenten *Profil med personverninnstillinger*.

2.2.3.2 Kjernejournal

Innsynskomponenten tilbyr innsyn i innbyggers kjernejournal, slik helsepersonell ser den. Dette omfatter opplysninger som er fysisk lagret i kjernejournal, så vel som opplysninger som ved oppslag hentes fra andre registre.

Oppslag på kjernejournalens logg over bruk er også tilgjengelig. Denne omfatter helsepersonell så vel som innbygger selv. Her tilbyr kjernejournal utvidet funksjonalitet i forhold til målbildet og øvrige helseregistre: I tillegg til oppslag i logg er det mulig å be om SMS- eller e-postvarsler ved helsepersonells bruk.

Innbygger har også mulighet via innsynstjenesten til direkte å registrere begrensninger i helsepersonells tilgang; dette for hele eller deler av kjernejournalen.

Kjernejournalen skiller seg fra andre helseregistre ved at innbygger selv kan registrere opplysninger direkte i sin kjernejournal. P.t. er det innsynstjenesten som tilbyr slik funksjonalitet. Det må imidlertid vurderes om egenregistrering skal løftes fram som et mer framtrødende element i brukerflaten på Min helse.

Relatert funksjonalitet: Reservasjoner mot kjernejournal, samt evt. opprettelse av kjernejournal, håndteres iht. målbildet i komponenten *Profil med personverninnstillinger*, sammen med øvrige reservasjoner mot henholdsvis digitale helsetjenester og programmer/ordninger. Denne funksjonaliteten ble opprinnelig lagt i innsynstjenesten, siden personverntjenester og profil ikke eksisterte den gang.

2.2.3.3 Andre helseregistre

Innsynskomponenten gir oversikt over helseregistre der opplysninger om innbyggeren er - eller kan være - registrert, sammen med mulighet for innsyn i innhold og bruk. Dette realiseres gjennom følgende mekanismer:

- Oppslag på et enkelt register

- Dialog eller skjema for å forespørre om papirbasert innsyn.

Anmodning fra innbygger om retting eller sletting i registeret, samt anmodning om å sperre enkeltelementer i registeret for helsepersonell, støttes gjennom meldinger/dialog.

Når ny melding opprettes, ivaretar innsynskomponenten

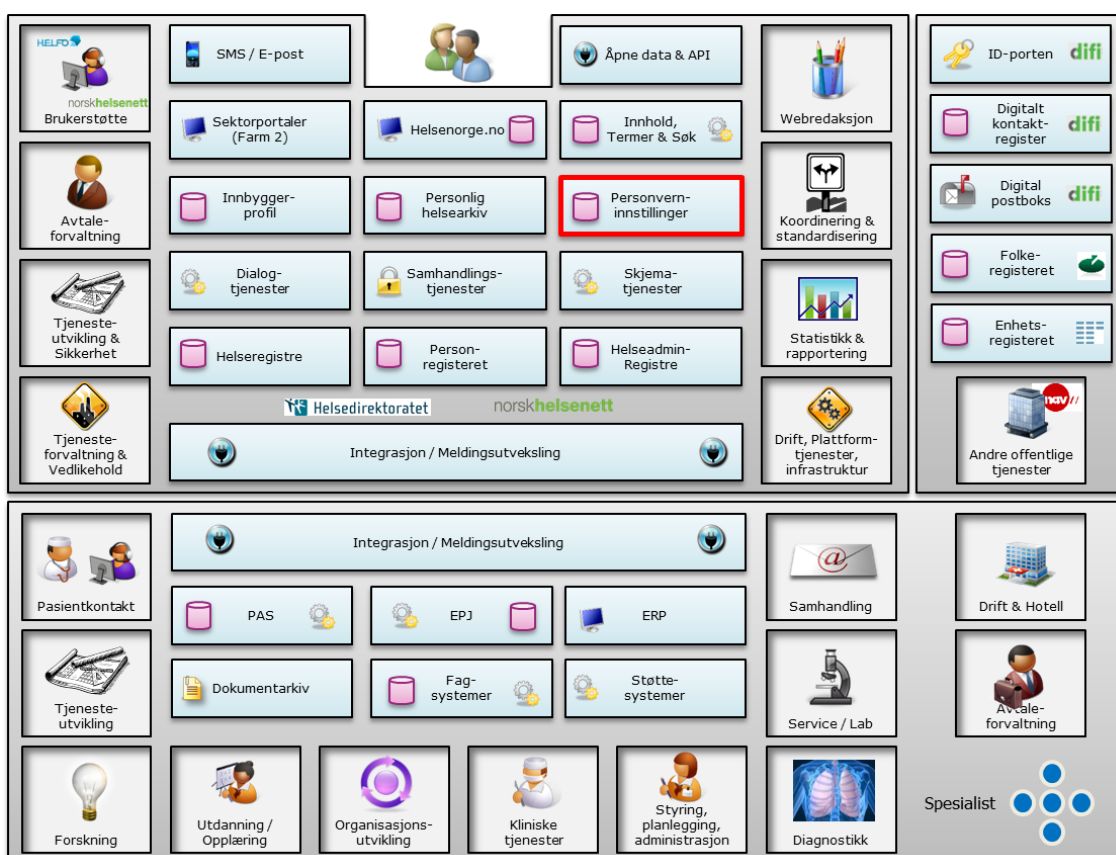
- eventuell kobling mot et spesifikt journalelement
- kobling mot rett mottaker/registerereier.

Forøvrig håndteres meldingsfunksjonalitet i komponenten *Dialog*.

Relatert funksjonalitet: Innbygger definerer generelle regler for sperring av helseopplysninger for helsepersonell i brukerflaten knyttet til sin *Profil*. Her får innbygger også informasjon om utlevering til andre aktører samt eventuelle forespørsler om dette, og her håndteres eventuelle reserverasjoner knyttet til bredt samtykke. Alt dette håndteres i komponenten *Profil med personverninnstillinger*.

3 TEKNISK MÅLBILDE

Personverntjenesten vil realiseres gjennom arkitekturkomponenten Personverninnstillinger fra DIS målbildet (markert med rødt omriss);



Figur 13: Plassering av personverntjenesten i DIS målbildet.

Teknisk målarkitektur for realisering av denne komponenten vil bli beskrevet nærmere i dette kapittelet.

3.1 Prinsipper for målarkitektur

Overordnede prinsipper for løsningen

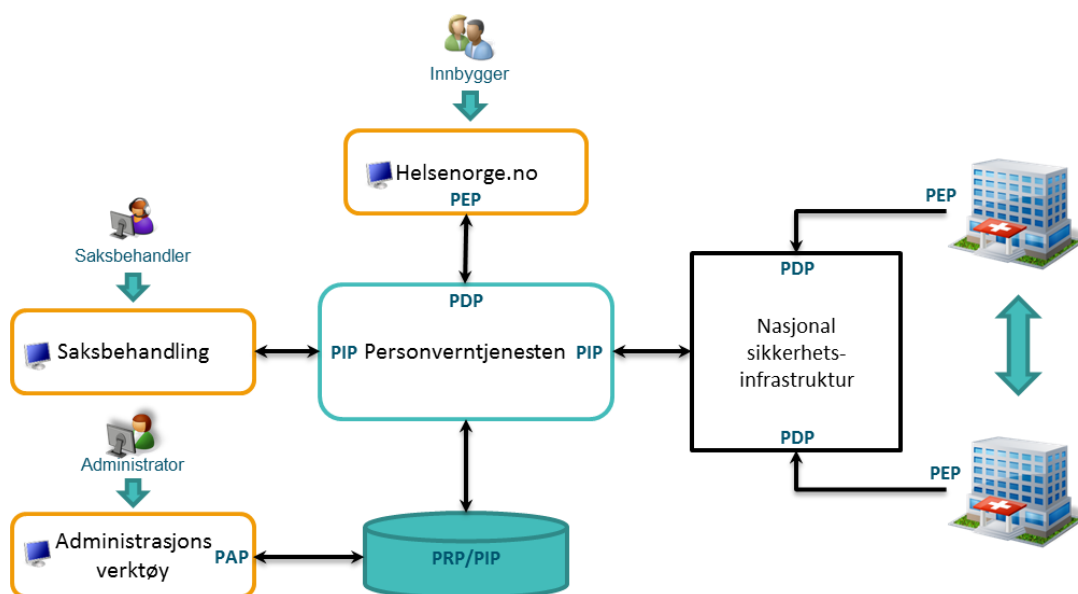
- Løsningen skal være i tråd med DIFI sine arkitekturprinsipper.
- Brukervennlighet – Personverninnstillingene skal presenteres på en forståelig og allmennspråklig måte, men samtidig gi muligheten for innsyn i detaljerte lover og gjeldende regelverk dersom brukeren ønsker dette.
- Løsningen skal baseres på føringer gitt i Norm for informasjonssikkerhet⁷. Sentrale områder som trekkes frem i normen vil være at løsningen underbygger kravene til konfidensialitet, integritet og tilgjengelighet.
- Tjenesteorientering og gjenbruk – Løsningen skal legge til rette for en tjenesteorientert arkitektur. Løsningen skal ha en ryddig tjenestesegmentering. Tjenestene skal ha en ryddig funksjonsinndeling, et klart definert formål og legge til rette for gjenbruk på tvers av sektoren.
- Tverrsektoriell – Løsningen skal så langt det er hensiktsmessig legge til rette for en tverrsektoriell løsning.
- Skalerbarhet – Løsningen skal være skalerbar både i forhold til brukermasse og funksjonalitet. Ny funksjonalitet skal enkelt kunne legges til samtidig som løsningen skal kunne utvides til å tas i bruk av en større del av helsesektoren.
- Sentralisert tilgangsstyring – Løsningen skal i størst mulig grad ha sentralisert tilgangsstyring.
- Gjenbruk av data - Løsningen skal basere seg på prinsippet om gjenbruk av data fra færrest mulige databaser, slik at man unngår inkonsistens og behov for synkronisering.
- Innsyn i fremfor utlevering – Løsningen skal legge til rette for at aktørene får innsyn i, fremfor utlevering av innbyggerens helseopplysninger. Dette vil sikre bedre kontroll på helseopplysninger og et bedre personvern for innbyggeren.
- Åpenhet fremfor skjerming – Løsningen må i størst mulig grad legge til rette for at innbyggeren kan få innsyn og kontroll over sine personopplysninger og helsetjenester.

⁷ <https://ehelse.no/Documents/Normen/Norm%20for%20informasjonssikkerhet%205.1%20%20utgave.pdf>

3.2 Målkitektur og arkitekturprinsipper

Figur 14 viser overordnet arkitektur for personverntjenesten uttrykt ved XACML definisjonene (For mer informasjon om XACML, se vedlegg 3). Som det her fremgår vil personverntjenesten være en autorisasjonstjeneste («Policy Decision Point» (PDP)) for helsenorge.no. Derimot for resten av helsesektoren vil personverntjenesten bare fungere som et «Policy Information Point» (PIP) som basert på innbyggerens personverninnstillinger vil kunne bistå med et beslutningsunderlag til en felles nasjonal autorisasjonstjeneste (PDP). Arkitekturen for personverntjenesten baserer seg altså på veletablerte prinsipper fra XACML arkitekturen ved å:

- Skille selve tilgangsstyringen fra applikasjonen i en sentral autorisasjonskomponent for helsenorge.no
- Skille på PDP og PIP som muliggjør at kun beslutningsunderlaget tilgjengeliggjøres for en fremtidig nasjonal sikkerhetsinfrastruktur uten at selve autorisasjonsbeslutningen må gjøres i personverntjenesten.
- Ha et separat «Policy Administration Point» (PAP) for administrasjon av tilgangsregler.



Figur 14: Arkitektur for personverntjenesten uttrykt ved XACML definisjonene.

3.2.1 Ansvarsdeling og tilgjengeliggjøring av personvernfunksjonalitet

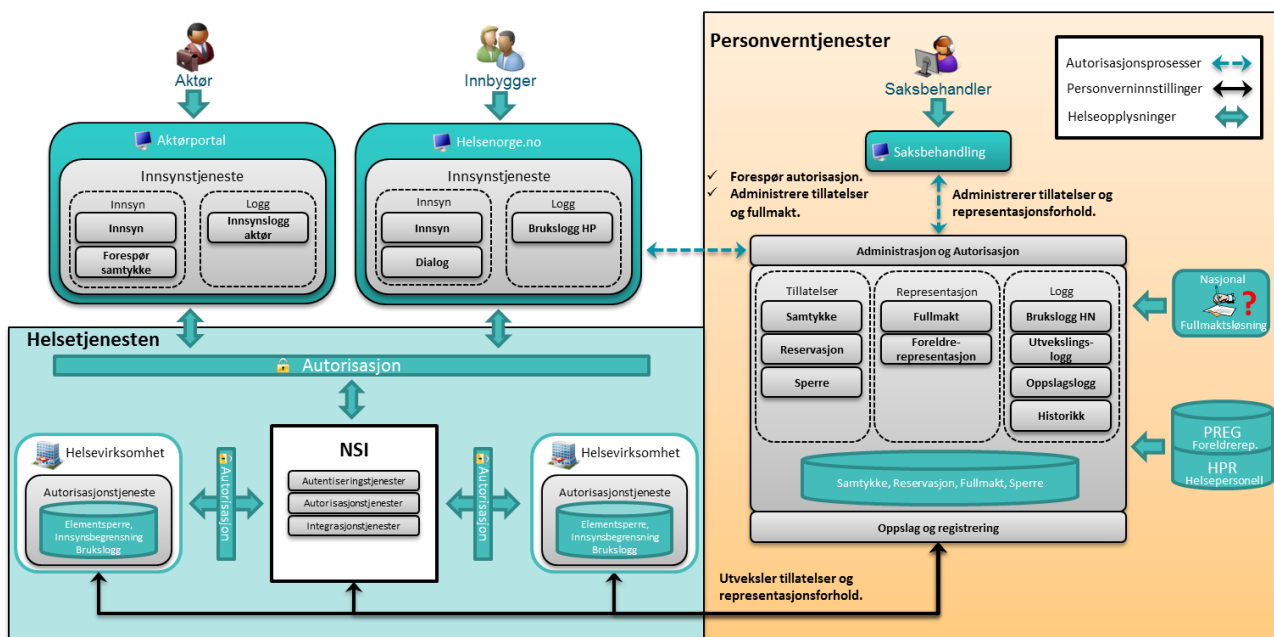
For å ha en klar ansvarsdeling og føring for tilgjengeliggjøring av personvernfunksjonalitet for helse- og omsorgssektoren foreslås det å tilby

1. En event basert kø-løsning der aktørene i helse- og omsorgssektoren kan abonnere på endringer i innbyggernes personverninnstillinger.
2. En synkron oppslag- og registreringstjeneste der aktørene kan registrere forespørsel for innhenting av reservasjon/samtykke fra en innbygger. I tillegg til synkront å kunne slå opp innbyggerens personverninnstillinger ved behov.

Fordelen med en slik løsning er at det er en klar ansvarsdeling mellom personverntjenesten og aktørene i sektoren. Personverntjenesten vil være ansvarlig for å sikre at alle endringer i innbyggerens personverninnstillinger vil bli tilgjengeliggjort som en event på køen, mens det er opp til aktøren hvordan dette skal forvaltes i det enkelte system. Eksempelvis kan aktørene selv velge om de ønsker å vedlikeholde en separat kopi av innbyggerens personverninnstillinger i sine systemer, eller bare benytte et synkront oppslag for å slå opp personverninnstillinger ved behov.




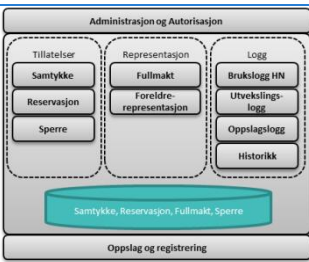



3.3 Konseptuell løsning og tjenestekomponenter

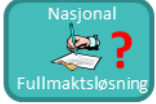





Figur 15 viser en konseptuell målarkitektur for personverntjenester, og Tabell 32 gir en tilhørende beskrivelse av de ulike komponentene. Her får innbyggeren kontroll over sine personopplysninger og helsetjenester ved å sette ulike tillatelser, i tillegg til å la seg representere, eller representere andre gjennom fullmakt eller foreldrerepresentasjon. Som illustrert i figuren er personverntjenester en separat komponent som muliggjør kontroll over deling av personopplysninger og representasjonsforhold ved å tilby oppslagslagstjenester for aktører i helsesektoren. Arkitekturen legger derved til rette for i størst mulig grad å samle alle tillatelser og representasjonsforhold ett sted. Dette vil trolig ikke være mulig i alle tilfeller, men det er en strategi å etterstrebe en slik løsning på sikt. For deler av personvernfunksjonaliteten er det derimot vurdert som ikke hensiktsmessig å legge i personverntjenesten, men heller realisere som en del av innsynstjenesten på helsenorge.no. Dette er også illustrert i figuren ved at tjenestene ligger i helsenorge.no komponenten. Nærmere detaljer om grunnlaget for dette vil bli gitt under kapittel 3.4. En mer detaljert beskrivelse av de ulike hovedkomponentene vil gitt i dette kapitlet.



Figur 15: Konseptuell målarkitektur for personverntjenester.

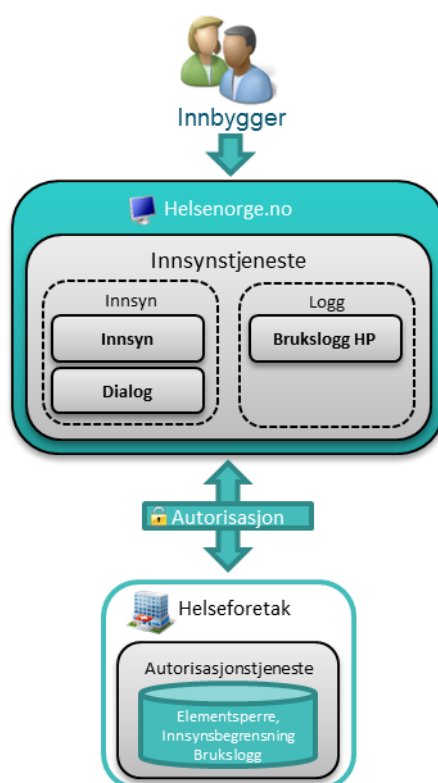
Tabell 32: Beskrivelse av komponentene i målarkitektur for personverntjenester.

| Komponent | Beskrivelse |
|---|---|
|  | <p>Helsenorge.no. Nasjonal portal for digitale helsetjenester på nett.</p> |
|  | <p>Aktørportal. Digital kanal for å tilby tjenester til aktører som har behov for helseopplysninger. Realisering av selve aktørportalen vil ikke bli tatt inn som en del av målbildet for helsenorge.no da fokuset her i hovedsak dreier seg om innbyggertjenester. Derimot vil det tilrettelegges ved oppslag-/registreringstjenester slik at en slik portal kan realisere i samarbeid med aktører i sektoren på sikt.</p> |
|  | <p>Saksbehandlerløsning for administrasjon av personverntjenester. Dette vil eksempelvis kunne være en utvidelse av HELFO sin eksisterende saksbehandlerløsning eSaks.</p> |
|  | <p>Nasjonal personverntjeneste for helse- og omsorgssektoren.</p> |
|  | <p>Helsevirksomhet som tilbyr helsetjenester til innbyggeren. Dette kan være helsevirksomheter både innenfor primær- og spesialisthelsetjenesten som eksempelvis fastlege, sykehus, pleiehjem etc. Virksomheten vil kunne ha flere ulike systemer som har behov for oppslag mot personverntjenesten. Dette kan eksempelvis være EPJ eller fagsystemer for helseforvaltningen.</p> |
|  | <p>Autorisasjonsgrense som krever oppslag mot personverntjenesten for å vurdere tillatelse/tilgang for utlevering av helseopplysninger.</p> |
|  | <p>Nasjonal sikkerhetsinfrastruktur. Felles nasjonal løsning for å håndterer autentisering og autorisasjon på tvers av helsesektoren. Denne komponenten finnes ikke i dag, men pågående prosjekt for Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren ser på muligheten for å etablere en slik løsning.</p> |

| Komponent | Beskrivelse |
|---|---|
|  | <p>Nasjonal fullmaktsløsning. Denne løsningen eksisterer ikke i dag, og det er ennå ikke avklart om det skal etableres en felles nasjonal fullmaktsløsning. Vurderingen av dette gjøres som en del av pågående SKATE-prosjekt. Det er som følge av dette lagt til et spørsmålstegn på komponenten.</p> |
|  | <p>Personregisteret (helsesektorens kopi av Det sentrale folkeregister). Inneholder informasjon om alle innbyggere i Norge inkludert familierelasjoner.</p> |
|  | <p>Helsepersonellregisteret inneholder en oversikt over alt helsepersonell i Norge med tilhørende helsepersonellnummer. I tillegg til opplysning om gjeldende autorisasjon, lisens og forskrivningsrett, og eventuelle begrensninger i disse, samt eventuell spesialitet for leger, tannleger og optikere. Dette vil være viktige opplysninger for å vurdere autorisasjon. For eksempel er det ikke sikkert at en fotterapeut skal ha tilgang til samme helseopplysninger som en psykiater. Denne komponenten vil være sentral for å kunne tilby sperrefunksjonalitet mot enkelte helsepersonell.</p> |
|  | <p>Utlevering av helseopplysninger.</p> |
|  | <p>Utlevering av personvernopplysninger.</p> |
|  | <p>Autorisasjonsprosesser for å håndtere tilgangsstyring på helsenorge.no.</p> |




3.3.1 Innsynstjeneste for Helsenorge.no



Figur 16 viser konseptuell arkitektur for innsynstjenesten på helsenorge.no, og Tabell 33 gir en beskrivelse av de ulike komponentene. Tjenesten understøtter den funksjonelle komponenten innsyn som er beskrevet i kapittel 2.2.3.



Figur 16: Konseptuell arkitektur for innsyn på helsenorge.no.

Tabell 33: Beskrivelse av de ulike komponentene for innsyn på helsenorge.no.

| Komponent | Beskrivelse |
|--|--|
|  Innbygger | Innbygger som logger seg på helsenorge.no via ID porten. Da tjenestene behandler sensitive helseopplysninger kreves sikkerhetsnivå 4. Følgende løsninger tilfredsstiller dette sikkerhetsnivået: BankID, BankID på mobil, Buypass og Commfides. |
|  Helsenorge.no | Helsenorge.no. Digital kanal for å tilby helsetjenester til innbyggeren. |
|  Innsyn | Tjeneste for å gi innbyggeren innsyn i sine helseopplysninger. Dette kan være helseopplysninger fra pasientjournal, helseregistre, eller kjernejournal. Tjenesten må ivareta tilfeller der behandler har begrenset innbyggers innsyn i sine egne eller andres helseopplysninger. Det er opp til den enkelte aktør som tilbyr datagrunnlaget å sikre at dette er ivaretatt. Dette utgjør per 1. juni 2015 to |

| Komponent | Beskrivelse |
|---|--|
| | <p>ulike tilfeller</p> <ol style="list-style-type: none"> 1. Begrense innbyggers innsyn i sine egne helseopplysninger. Dette gjøres ved å merke utvalgte opplysninger med UNNTATT_INNSYN. 2. Begrense foresattes innsyn for barn 12-16 år sine helseopplysninger ved å unnta opplysninger fra foreldreinnsyn, dvs. merke utvalgte opplysninger med UNNTATT_FORELDREINNSYN. <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Innsynskomponenten (Beskrevet under kapittel 2.2.3). |
|  | <p>Tjeneste for å gi innbyggeren mulighet til utføre dialog med helseaktør/behandler for å kunne forespørre retting og sletting av helseopplysninger, i tillegg til sperring av enkeltelementer. Dette kan være ulike type elementer som eksempelvis dokumenter, timeavtaler og dialog.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Innsynskomponenten (Beskrevet under kapittel 2.2.3). |
|  | <p>Tjeneste for å gi innbyggeren mulighet til å se en logg over helsepersonells tilgang og bruk av sine helseopplysninger.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Innsynskomponenten (Beskrevet under kapittel 2.2.3). |

3.3.1.1 Avgrensninger og grensesnitt

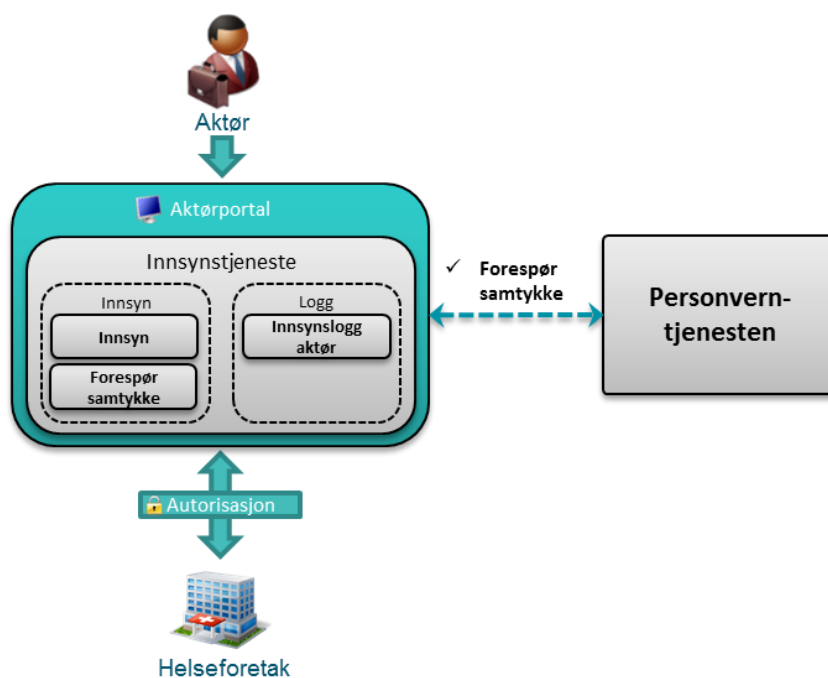
Tabell 34: Ansvarsmatrise ved realisering av innsynstjenesten

| Funksjon | Hn.no standard-funksjonalitet | Hn.no innsynstjeneste | PVK | Aktør |
|--|-------------------------------|-----------------------|-----|-------|
| Innsynstjeneste | | | | |
| Brukerflate for innsyn | | x | | |
| Håndtere innlogging for innbygger og henting av data | x | | | |
| Hente innbyggers helseopplysninger ved oppslag mot aktør. Kall skal også inneholde informasjon om eventuelle representasjonsforhold. | | x | | |

| Funksjon | Hn.no standard-funksjonalitet | Hn.no innsynstjeneste | PVK | Aktør |
|---|-------------------------------|-----------------------|-----|-------|
| Tilgjengeliggjøre grensesnitt for uthenting av data for hn.no, eller alternativt håndtere manuell prosess for uthenting av data. Ved manuell uthenting kan svaret sendes til innbygger gjennom fremtidig skjemaløsning eller Sikker Digital postkasse på hn.no. | | | | x |
| Utføre logging av innbygger selv, eller representasjonsforhold ved oppslag fra helsenorge.no. | | | | x |
| Logging av egen og andres bruk (fullmakt/foreldre) av innsynstjenesten på et overordnet nivå | | | x | |
| Tilgjengeliggjøre overordnet brukslogg for innbygger | | | x | |
| Utføre detaljert logging av helsepersonell innsyn og bruk av helseopplysninger | | | | x |
| Tilgjengeliggjøre detaljert logg for innbygger i visningen | | x | | |
| Tilby grensesnitt for henting av detaljert logg for innbygger | | | | x |
| Håndheve sperre mot helsepersonell dersom aktuelt. | | | | x |
| Tilbakeholde informasjon ved innsynsbegrensning dersom aktuelt | | | | x |




3.3.2 INNSYNTJENESTE FOR AKTØRPORTAL

Figur 17 Figur 18 viser konseptuell arkitektur for aktørportalen, og Tabell 35 gir en beskrivelse av de ulike komponentene. Tjenesten understøtter funksjonaliteten for at innbygger skal kunne samtykke til utlevering av helseopplysninger som beskrevet under kapittel 2.2.2.3.



Figur 17: Konseptuell arkitektur for aktørportal.

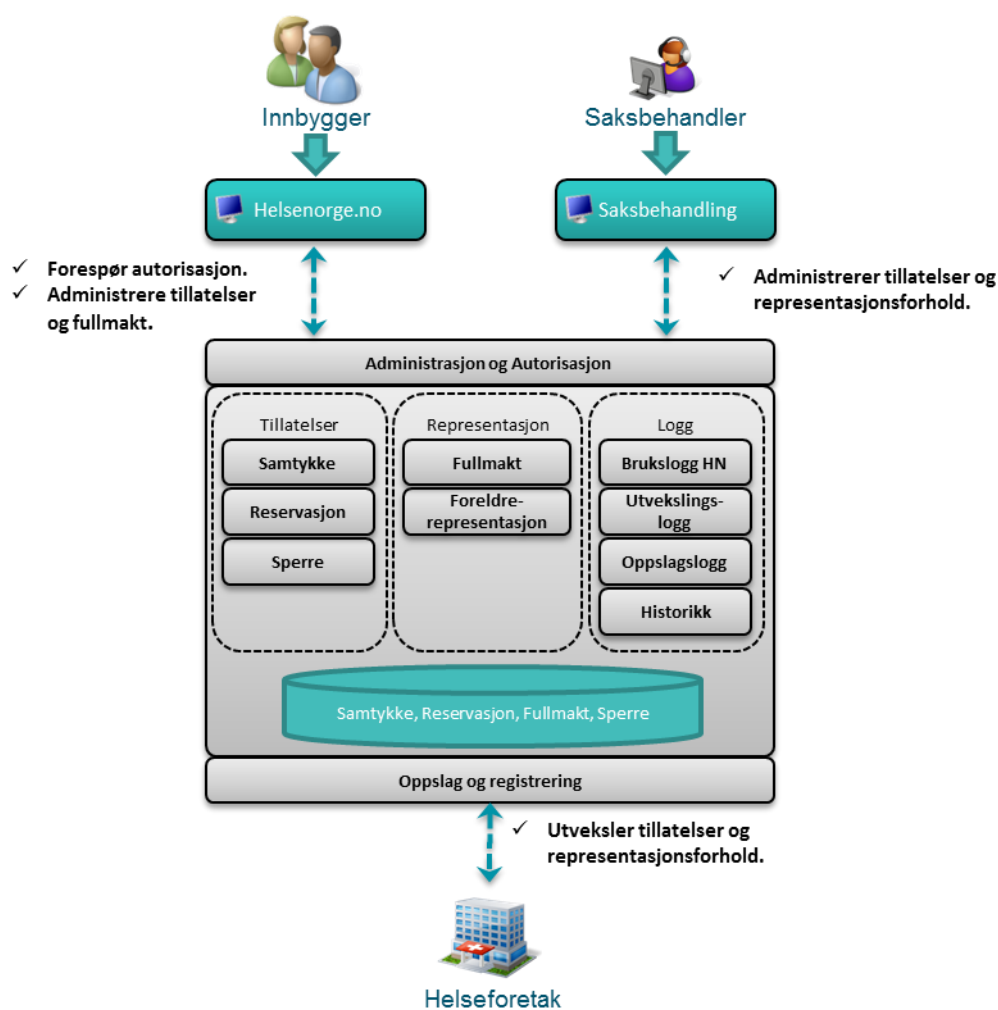
Tabell 35: Beskrivelse av de ulike komponentene for aktørportal.

| Komponent | Beskrivelse |
|--|---|
|  Aktor | Aktører som har behov for helseopplysninger for å tilby tjenester til innbyggeren. Dette kan eksempelvis være forsikringsselskap som har behov for helseopplysninger ved etablering av personforsikring. |
|  Aktørportal | Aktørportal. Digital kanal for å tilby tjenester til aktører som har behov for helseopplysninger. Realisering av selve aktørportalen vil ikke bli tatt inn som en del av målbildet for helsenorge.no da fokuset her i hovedsak dreier seg om innbyggertjenester. Derimot vil det tilrettelegges ved oppslag-/registreringstjenester slik at en slik portal kan realiseres i samarbeid med aktører i sektoren på sikt. |
|  Innsyn | Tjeneste for å gi en aktør innsyn i en innbyggers helseopplysninger forutsatt at innbygger har akseptert samtykke om innsyn/utlevering. |

| Komponent | Beskrivelse |
|--------------------------|--|
| | <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> Funksjonalitet for å kunne samtykke til utlevering (Beskrevet under kapittel 2.2.2.3). En aktørportal er ikke eksplisitt nevnt, men er en løsning for å muliggjøre utlevering ved innsyn uten å måtte duplisere helseopplysningene. |
| <p>Forespør samtykke</p> | <p>Tjeneste for å gi aktøren mulighet til å forespør helseopplysninger for en innbygger. Det vil kreve samtykke fra innbyggeren før helseopplysningene faktisk blir tilgjengeliggjort.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> Funksjonalitet for å kunne samtykke til utlevering (Beskrevet under kapittel 2.2.2.3). |
| <p>Innsynslogg aktør</p> | <p>Tjeneste for å gi aktøren en oversikt over hvilke saksbehandlere som har vært inne og hentet opp helseopplysninger. En aktørportal er ikke eksplisitt nevnt, men er en løsning for å muliggjøre utlevering ved innsyn uten å måtte duplisere helseopplysningene.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> Funksjonalitet for å kunne samtykke til utlevering (Beskrevet under kapittel 2.2.2.3). En aktørportal er ikke eksplisitt nevnt, men er en løsning for å muliggjøre utlevering ved innsyn uten å måtte duplisere helseopplysningene. |


3.3.3 PERSONVERTJENESTE

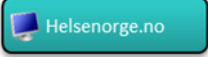


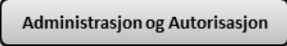
Figur 18 viser konseptuell arkitektur for personverntjenesten, og Tabell 36 gir en beskrivelse av de ulike komponentene. Tjenesten understøtter de funksjonelle komponentene tilgangsstyring og profil som er beskrevet i henholdsvis kapittel 2.2.1 og 2.2.2.



Figur 18: Konseptuell arkitektur for personverntjenesten.



Tabell 36: Beskrivelse av de ulike komponentene for personverntjenesten.

| Komponent | Beskrivelse |
|--|--|
|  Innbygger | <p>Innbygger som logger seg på helsenorge.no via ID porten. Da tjenestene behandler sensitive helseopplysninger kreves sikkerhetsnivå 4. Følgende løsninger tilfredsstiller dette sikkerhetsnivået: BankID, BankID på mobil, Buypass og Commfides.</p> |

| Komponent | Beskrivelse |
|--|---|
|  | <p>Helsenorge.no. Digital kanal for å tilby helsetjenester til innbyggeren.</p> |
|  <p>Saksbehandler</p> | <p>Saksbehandler som kan bistå innbygger med administrasjon av personverntjenester. Dette vil eksempelvis kunne være 800HELSE.</p> |
|  | <p>Saksbehandlerløsning for administrasjon av personverntjenester. Dette vil eksempelvis kunne være en utvidelse av HELFO sin eksisterende saksbehandlerløsning eSaks.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Profil med personverninnstillinger (Beskrevet under kapittel 2.2.2) <ul style="list-style-type: none"> ○ Understøtter funksjonalitet innenfor alle de funksjonelle komponenter ved å tilby en analog kanal for å endre personverninnstillinger for innbyggeren. |
|  | <p>Tjenester for å kunne tilby administrasjon og autorisasjon for personverntjenester. Dette vil inkludere autorisasjonstjenester for å kunne vurdere innbyggers tilgang, i tillegg til administrasjonstjenester som både benyttes av innbygger ved administrasjon fra helsenorge.no, men også av saksbehandler ved administrasjon fra en saksbehandlerløsning på vegne av innbyggeren.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Understøtter funksjonell komponent for tilgangsstyring (Beskrevet under kapittel 2.2.1). |

| Komponent | Beskrivelse |
|---|--|
| <div data-bbox="268 383 421 439" style="border: 1px solid black; padding: 2px; text-align: center;">Oppslag og registrering</div> | <p data-bbox="528 383 1398 573">Oppslag- og registreringstjeneste for å tilby personvernfunksjonalitet til helsesektoren. Denne vil bli benyttet for å tilgjengeliggjøre innbyggerens personverninnstillinger for å muliggjøre autorisasjon både i forhold til tillatelser og representasjon. I tillegg vil tjenesten muliggjøre registrering i tilfeller der en aktør eksempelvis ønsker å forespørre samtykke eller reservasjon fra en innbygger.</p> <p data-bbox="528 607 983 633">Understøtter funksjonelle komponenter:</p> <ul data-bbox="576 674 1398 1223" style="list-style-type: none"> • Deling av informasjon - sperring og utlevering (Beskrevet under kapittel 2.2.2.3) <ul style="list-style-type: none"> ○ Oppslagstjeneste for å at HF skal kunne sjekke om det foreligger sperre mot helsepersonell eller behandlingsløp. ○ Registreringstjeneste for at HF skal kunne registrere en forespørsel om samtykke til eller reservasjon mot utlevering av helseopplysninger • Fullmakter (Beskrevet under kapittel 2.2.2.1) <ul style="list-style-type: none"> ○ Oppslagstjeneste for at aktører i helsetjenesten skal kunne gjøre oppslag om det foreligger en fullmakt. • Tilgangsstyring (Beskrevet under kapittel 2.2.1) <ul style="list-style-type: none"> ○ Oppslagstjeneste for at aktører i helsetjenesten skal kunne slå opp representasjonsforhold i forhold til foreldreansvar. • Bruk av helsetjenester og ordninger (Beskrevet under kapittel 2.2.2.2) <ul style="list-style-type: none"> ○ Oppslagstjeneste for at aktører i helsesektoren kan sjekke om innbygger har samtykket til eller reservert seg mot programmer eller ordninger. |
| <div data-bbox="268 1267 421 1323" style="border: 1px solid black; padding: 2px; text-align: center;">Samtykke</div> | <p data-bbox="528 1267 1362 1357">Tjeneste for å håndtere funksjonalitet for samtykke. Dvs. å kunne gi innbyggeren mulighet til å si seg enig i at en handling skal utføres, oppheve noens taushetsplikt eller gi tillatelse til at behandling av personopplysninger.</p> <p data-bbox="528 1391 983 1417">Understøtter funksjonelle komponenter:</p> <ul data-bbox="576 1458 1398 1547" style="list-style-type: none"> • Bruk av helsetjenester og ordninger (Beskrevet under kapittel 2.2.2.2) • Deling av informasjon - sperring og utlevering (Beskrevet under kapittel 2.2.2.3) |
| <div data-bbox="268 1592 421 1648" style="border: 1px solid black; padding: 2px; text-align: center;">Reservasjon</div> | <p data-bbox="528 1592 1339 1648">Tjeneste for å håndtere funksjonalitet for reservasjon. Dvs. å kunne gi innbyggeren mulighet til å benytte sin lovfestede rett til å ikke ta del i noe.</p> <p data-bbox="528 1682 983 1709">Understøtter funksjonelle komponenter:</p> <ul data-bbox="576 1749 1398 1839" style="list-style-type: none"> • Bruk av helsetjenester og ordninger (Beskrevet under kapittel 2.2.2.2) • Deling av informasjon - sperring og utlevering (Beskrevet under kapittel 2.2.2.3) |

| Komponent | Beskrivelse |
|--|---|
| <div data-bbox="268 383 421 434" style="border: 1px solid gray; border-radius: 5px; padding: 2px; text-align: center;">Sperre</div> | <p>Tjeneste for å gi innbyggeren mulighet til å begrense helsepersonells tilgang til sine helseopplysninger ved sperring. Dette inkluderer funksjonalitet for å kunne sperre alle helseopplysninger for enkelte helsepersonell, eller utvalgte opplysninger for alt helsepersonell. Sperren gjelder på tvers av hele helsesektoren, og er tilgjengeliggjort for sektoren ved oppslagstjenesten beskrevet over.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Deling av informasjon - sperring og utlevering (Beskrevet under kapittel 2.2.2.3) |
| <div data-bbox="260 770 429 822" style="border: 1px solid gray; border-radius: 5px; padding: 2px; text-align: center;">Fullmakt</div> | <p>Tjeneste for å gi innbyggeren mulighet til å gi eller motta en fullmakt. Fullmakten kan gjelde digitale tjenester på helsenorge.no eller andre typer fullmakt som eksempelvis muligheten for å hente ut resepter i apotek. Hva en fullmakt omfatter vil variere i det enkelte tilfelle. Vergemål vil bli håndtert som et spesialtilfelle av fullmakt og også bli håndtert av denne tjenesten.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Fullmakter (Beskrevet under kapittel 2.2.2.1) |
| <div data-bbox="260 1099 429 1151" style="border: 1px solid gray; border-radius: 5px; padding: 2px; text-align: center;">Foreldre-representasjon</div> | <p>Tjeneste for å kunne gi innbyggeren mulighet til å representere sine barn frem til fylte 16 år.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Tilgangsstyring (Beskrevet under kapittel 2.2.1) |
| <div data-bbox="268 1330 421 1382" style="border: 1px solid gray; border-radius: 5px; padding: 2px; text-align: center;">Brukslogg HN</div> | <p>Tjeneste for å gi innbyggeren mulighet til å se en overordnet logg over egen og andres bruk (ved representasjon) av tjenester på helsenorge.no.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Understøtter komponenten «Logg over bruk på hn.no» (Beskrevet under kapittel 2.2.2.4). |
| <div data-bbox="268 1592 421 1644" style="border: 1px solid gray; border-radius: 5px; padding: 2px; text-align: center;">Oppslagslogg</div> | <p>Tjeneste for å gi innbyggeren mulighet til å se en oversikt over eksterne forespørsler mot personverninnstillingene fra helsesektoren.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Understøtter komponenten «Logg over ekstern bruk av personverninnstillinger» (Beskrevet under kapittel 2.2.2.4). |

| Komponent | Beskrivelse |
|---|--|
|  | <p>Tjeneste for å kunne gi innbyggeren en totaloversikt over all utlevering av sine helseopplysninger mellom helsevirksomhetene. Dette vil eksempelvis være utlevering mellom fastlege og spesialisthelsetjenesten, eller utlevering mellom helseforetakene i de ulike regionene.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Deling av informasjon - sperring og utlevering (Beskrevet under kapittel 2.2.2.3) |
|  | <p>Tjeneste som gir innbyggeren en oversikt over historikk for personverninnstillinger.</p> <p>Understøtter funksjonelle komponenter:</p> <ul style="list-style-type: none"> • Understøtter komponenten «Historikk/logg over endringer i personverninnstillinger». (Beskrevet under kapittel 2.2.2.4) |

3.3.3.1 Avgrensninger og grensesnitt

Tabell 37: Ansvarsmatrise ved realisering av personverntjenesten

| Funksjonell prosess | Operasjon | Hn.no standard-funksjonalitet | Hn.no Innsynstjeneste | PVK | Aktør |
|---------------------|---|-------------------------------|-----------------------|-----|-------|
| Innlogging | Håndtere autentisering av innbygger gjennom ID porten. | x | | | |
| | Håndheve autorisasjon for innbygger | x | | | |
| | Beslutte autorisasjon for innbygger basert på personverninnstillinger | | | x | |
| Logging | Utføre logging av egen og andres bruk av tjenester på et overordnet nivå på helsenorge.no (fullmakt/foreldre) | x | | | |
| | Tilby tjeneste for registrering og henting av logg for innbygger | | | x | |
| | Utføre detaljert logging over egen og andres bruk av tjenesten. | | | | x |

| Funksjonell prosess | Operasjon | Hn.no standard-funksjonalitet | Hn.no Innsyns-tjeneste | PVK | Aktør |
|--|--|-------------------------------|------------------------|-----|-------|
| Samtykke/Reservasjon til sekundærbruk | Tilby brukergrensesnitt for å sette samtykke/reservasjon for sekundærbruk | x | | | |
| | Tilby tjeneste for lagring og henting av reservasjon/samtykke | | | x | |
| | Informere aktør om at det er registrert et samtykke/reservasjon for innbygger ved event på kø | | | x | |
| | Abonnere på hendelse og håndtere sletting eller godkjenning av datalagring basert på samtykke/reservasjon | | | | x |
| | Tilby tjeneste for synkrone oppslag av samtykke og reservasjoner | | | x | |
| | Kalle PVK for å slå opp reservasjon/samtykke ved behov (Valgfritt) | | | | x |
| | Tilby tjeneste for å kunne forespør samtykke eller reservasjon fra innbygger | | | x | |
| | Kalle PVK for å informere innbygger om reservasjonsmulighet eller forespør samtykke | | | | x |
| Samtykke til/reservasjon mot tjenester på Helsenorge.no | Tilby brukergrensesnitt for sette og trekke samtykke og reservasjoner | x | | | |
| | Tilby CRUD tjeneste for samtykke og reservasjon | | | x | |
| | Håndheve autorisasjon ved å tilpasse tjenestetilgangen basert på kall mot PVK | x | | | |
| | Tilby en tjeneste for å kunne beslutte autorisasjon/tjenestetilgang basert på innbyggers personverninnstillinger | | | x | |
| | Abonnere på, eller slå opp samtykke og reservasjoner ved behov (ikke påkrevd) | | | | x |
| Fullmakt til tjenester på Helsenorge.no | Tilby brukergrensesnitt for registrering og administrasjon av fullmakt | x | | | |

| Funksjonell prosess | Operasjon | Hn.no standard-funksjonalitet | Hn.no Innsyns-tjeneste | PVK | Aktør |
|--|--|-------------------------------|------------------------|-----|-------|
| | Tilby CRUD tjeneste for fullmakt | | | x | |
| | Tilby fullmakt i personvelger i brukergrensesnittet der en innlogget bruker med fullmakt kan representere en annen. | x | | | |
| | Tilby en tjeneste for evaluering av hvem en innbygger kan representere ved fullmakt | | | x | |
| | Håndheve autorisasjon ved å tilpasse tjenestetilgangen når en innlogget innbygger velger å representere en annen i personvelgeren | x | | | |
| | Tilby en tjeneste for å kunne beslutte autorisasjon/tjenestetilgang basert på innbyggers fullmakter | | | x | |
| | Validere innlogget innbygger og representasjonsforhold ved kall på tjenesteoperasjoner fra hels norge.no. (Valgfritt, støttes ikke i dag, kun trust mot hels norge.no) | | | | x |
| Fullmakt til helsetjenester og ordninger utenfor hels norge.no. | Tilby brukergrensesnitt for registrering og administrasjon av fullmakt | x | | | |
| | Tilby CRUD tjeneste for fullmakt | | | x | |
| | Tilgjengeliggjøre CRUD operasjoner for fullmakt som event på kø. | | | x | |
| | Abonnere på fullmaktsevent for lokal lagring (Valgfritt om dette foretrekkes fremfor synkront kall) | | | | x |
| | Tilby tjeneste for synkront oppslag for fullmakt | | | x | |
| | Slå opp om det foreligger en fullmakt ved synkront kall mot PVK | | | | x |

| Funksjonell prosess | Operasjon | Hn.no standard-funksjonalitet | Hn.no Innsyns-tjeneste | PVK | Aktør | |
|--|--|-------------------------------|------------------------|-----|-------|---|
| Foreldrerepresentasjon for tjenester på Helsenorge.no | Tilgjengeliggjøre foreldrerepresentasjon i personvelgeren ved kall mot PVK | x | | | | |
| | Tilby tjeneste for hente barn en foresatt kan representere | | | x | | |
| | Håndheve autorisasjon ved å tilpasse tjenestetilgangen når en innlogget foresatt velger å representere sitt barn i personvelgeren | x | | | | |
| | Tilby en tjeneste for å kunne beslutte autorisasjon/tjenestetilgang basert på foreldrerepresentasjon | | | x | | |
| | Validere innlogget innbygger og representasjonsforhold ved kall på tjenesteoperasjoner fra helsenorge.no. (Valgfritt, støttes ikke i dag, kun trust mot helsenorge.no) | | | | | x |
| Sette nasjonale sperre mot helsepersonell | Tilby brukergrensesnitt for registrering og administrasjon av nasjonale sperrer | x | | | | |
| | Tilby CRUD tjeneste for nasjonale sperrer | | | x | | |
| | Tilgjengeliggjøre CRUD operasjoner for fullmakt som event på kø. | | | x | | |
| | Abonnere på fullmaktsevent for lokal lagring (Valgfritt om dette foretrekkes fremfor synkront kall) | | | | | x |
| | Tilby tjeneste for synkron oppslag for nasjonale sperrer | | | x | | |
| | Håndheve nasjonale sperrer ved tilgangsstyring av helseopplysninger | | | | | x |

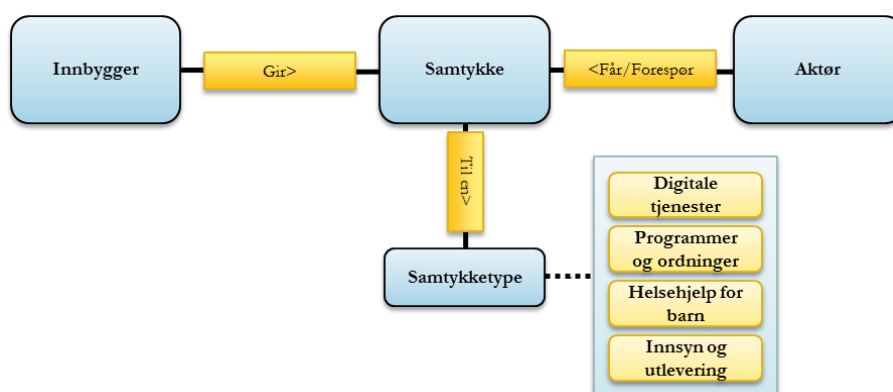
3.4 Beskrivelse av personverntjenester

Dette kapitlet gir en mer detaljert beskrivelse av funksjonalitet for tjenestene definert i målarkitekturen under kapittel 3.2.1.

3.4.1 Tillatelser

Tilbyr tjenester for å gi innbyggeren mulighet til å administrere hvem som har tilgang til sine helseopplysninger. Dette inkluderer mulighet til å opprette, endre og slette ulike tillatelser. Tillatelsene kan både være relatert til deling av helseinformasjon men også andre type tillatelser som eksempelvis deltagelse i forskningsprosjekt eller behandlingsløp. En beskrivelse av hver av komponentene er som følger.

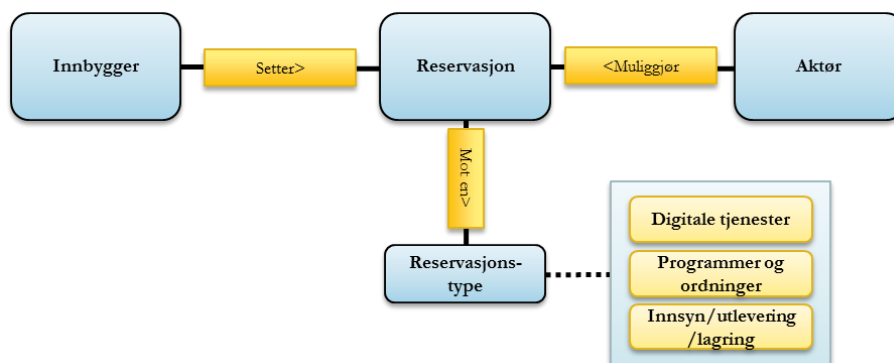
3.4.1.1 Samtykke



Figur 19: Logisk informasjonsmodell for samtykke.

Figur 19 viser logisk informasjonsmodell for samtykke. Som det her illustreres skal samtykketjenesten dekke funksjonalitet for at innbyggeren skal kunne si seg enig i at en handling skal utføres, oppheve noens taushetsplikt eller gi tillatelse til behandling av personopplysninger. Dette vil typisk være samtykke til eksempelvis lagring av sensitiv informasjon om brukeren i registre som ikke har lovfestet rett til lagring av data. Denne typen tilfeller av registrering blir ofte omtalt som «Optional-In» (Opt-In), da brukeren her som utgangspunkt ikke vil være registrert i registeret, men derimot har mulighet til å få informasjonen lagret ved å gi samtykke til denne funksjonaliteten.

3.4.1.2 Reservasjon



Figur 20: Logisk informasjonsmodell for reservasjon.

Figur 20 viser logisk informasjonsmodell for reservasjon. Som det her illustreres skal reservasjonstjenesten dekke funksjonalitet for å kunne gi innbyggeren mulighet til å benytte sin lovfestet rett til å ikke ta del i noe. Dette vil eksempelvis gjelde registrering eller innsyn i registre som brukeren som utgangspunkt automatisk vil være registrert. Dette er ofte omtalt som «Optional Out» (Opt-Out). Dette fordi brukeren aktivt må reservere seg mot tjenesten for å unngå og være registrert.

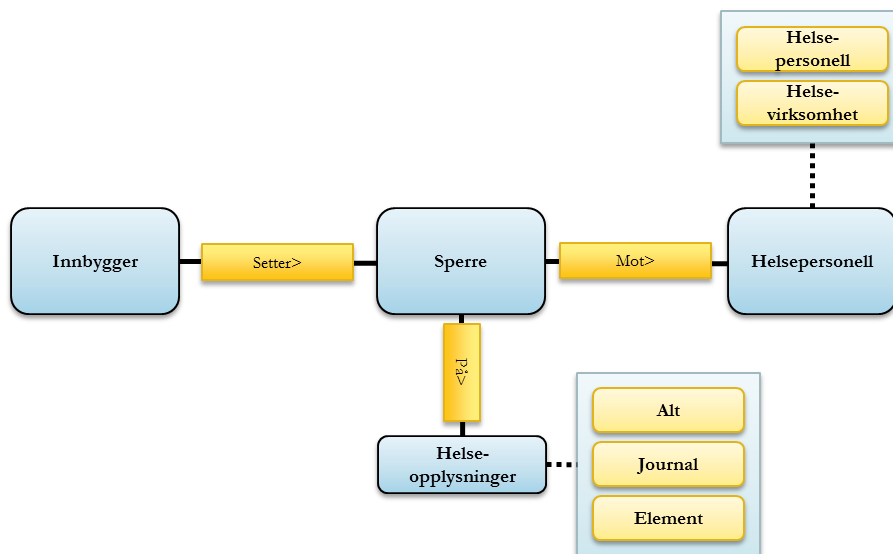
3.4.1.3 Tjenestetyper for samtykke og reservasjon

For å kunne håndtere ønsket funksjonalitet for samtykke og reservasjon er det i hovedsak 3 ulike tjenestetyper som må støttes.

| Tjenestetype | Beskrivelse |
|--|---|
| 1 Samtykke og reservasjon for tjenester på helsenorge.no | <p>Dekker funksjonalitet for at innbyggeren skal kunne samtykke til eller reservere seg mot tjenester som er eksponert gjennom, eller er en del av helsenorge.no portalen. Her tilpasses også visningen og tilgangen til tjenesten basert på om det foreligger et samtykke eller en reservasjon.</p> <p>Eksempel:</p> <ul style="list-style-type: none"> - Reservasjon mot tjenester på nett. - PHA-samtykke |

| Tjenestetype | Beskrivelse |
|---|--|
| <p>2 Samtykke og reservasjon for faste ordninger og tjenester som ikke er eksponert gjennom helsenorge.no.</p> | <p>Dekker funksjonalitet for at innbyggeren skal kunne samtykke til, eller reservere seg mot tjenester som ikke er eksponert gjennom helsenorge.no portalen. Dette er typisk eksterne tjenester eller ordninger som ønsker å benytte helsenorge.no som en digital kanal for å gi innbyggeren mulighet til å administrere samtykke og reservasjon. Dette krever at det etableres en oppslagstjeneste for kontroll, eller alternativt lagring av samtykke/reservasjon hos eksternt aktør.</p> <p>Eksempel:</p> <ul style="list-style-type: none"> - Reservasjon mot å delta i fastlegeordningen. - Reservasjon mot automatisk frikort. - Bredt samtykke for deltagelse til forskning. - Samtykke til/reservasjon mot deltagelse i helseregistre. - Samtykke til/reservasjon mot organdonasjon. |
| <p>3 Forespør samtykke eller reservasjon for enkelthendelser på vegne av eksterne foretak.</p> | <p>Tilbyr funksjonalitet for å innhente et samtykke eller en reservasjon fra innbyggeren ved enkelthendelser på vegne av eksterne foretak og tjenester. Her kan foretaket ved enkelthendelser fortløpende forespør samtykke eller reservasjon fra innbyggeren.</p> <p>Eksempler:</p> <ul style="list-style-type: none"> - Samtykke til utlevering av helseopplysninger til forsikring. - Informere om forskningsprosjekter og gi muligheten til å reservere seg mot enkelte prosjekter. |

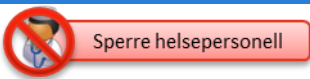
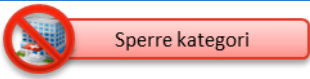

3.4.1.4 Sperre

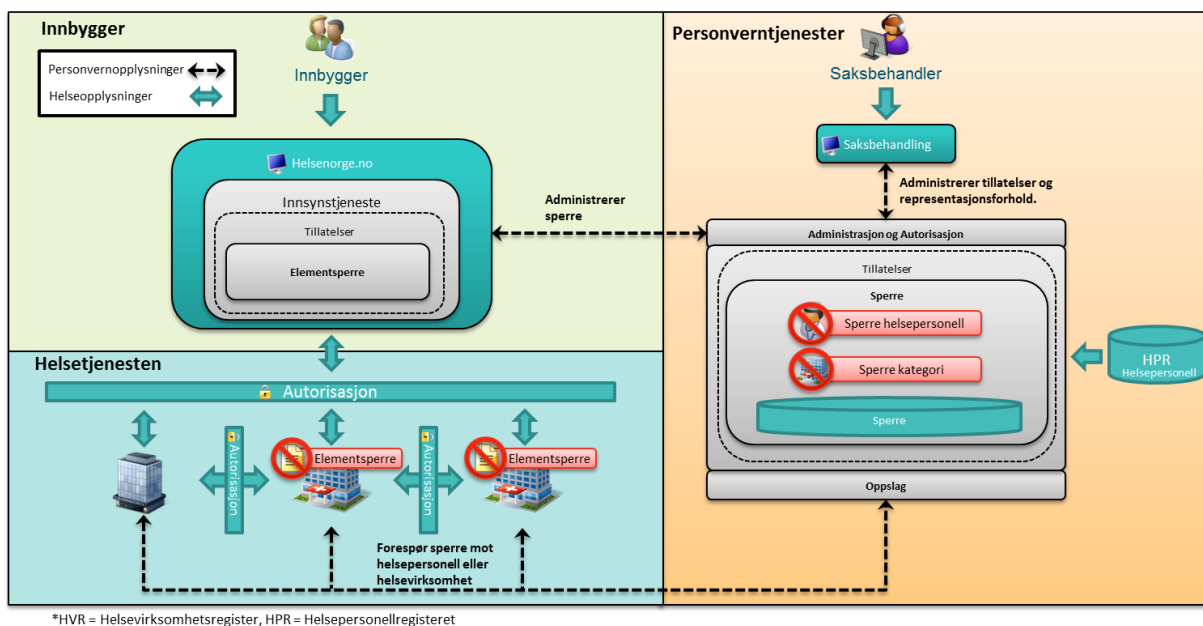


Figur 21: Logisk informasjonsmodell for sperre.

Figur 21 viser logisk informasjonsmodell for sperre. Som det her illustreres skal sperrefunksjonaliteten gi innbyggeren mulighet til å sperre for helsepersonells tilgang til sine helseopplysninger. Ny pasientjournallov åpner for muligheten for tilgang til helseopplysninger mellom helsevirksomheter, men samtidig skal innbyggeren ha rett til å sperre hele eller deler av journalen for innsyn for enkelte helsepersonell eller grupper av helsepersonell. For å ivareta en slik funksjonalitet må det derfor tilbys støtte for sperre på flere ulike nivåer både i forhold til bredde med tanke på hvor stor del av helsesektoren, og dybde, hele eller deler av journalen. I hovedsak er det sett for seg 3 hovedtyper av sperrefunksjonalitet

Tabell 38: Hovedtyper for sperring.

| Nr. | Sperretype | Beskrivelse |
|-----|---|---|
| 1 |  Sperre helsepersonell | Sperring av alle innbyggerens helseopplysninger for enkelte helsepersonell. |
| 2 |  Sperre kategori | Sperre utvalgte opplysninger for alt helsepersonell. Dette kan eksempelvis være et behandlingsløp, eller all helseinformasjon før et gitt tidspunkt. |
| 3 |  Elementsperre | Sperring av enkeltelementer. Da både i forhold til <ul style="list-style-type: none"> ✓ At enkelte helsepersonell <u>ikke skal</u> ha tilgang til deler av journalen. ✓ At kun enkelte helsepersonell <u>skal</u> ha tilgang til deler av journalen. Eksempelvis innbyggerens fastlege. |

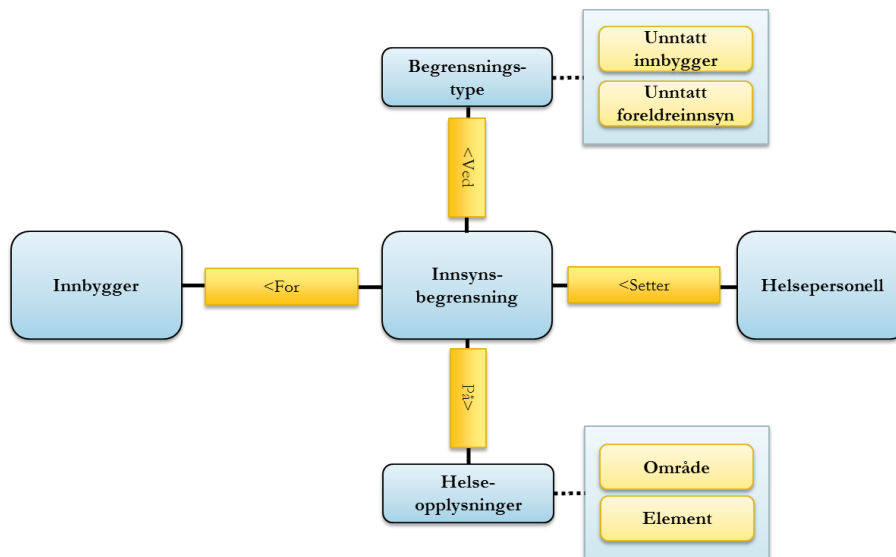


Figur 22: Illustrasjon av sperrefunksjonalitet.

Som illustrert i Figur 22 er det for sperre mot helsepersonell og for en kategori tenkt at disse sperrere bør lagres sentralt i personverntjenesten da innbyggeren her kan søke opp enten enkelte helsepersonell eller en kategori og sette en sperre som gjelder på tvers av sektoren. Den enkelte helsevirksomhet vil da kunne gjøre et oppslag mot personverntjenesten for å avgjøre om det foreligger en sperre.

For punkt 3 anses det ikke her som hensiktsmessig at sperre på enkeltdokumenter eller kun deler av journalen ligger lagret sentralt i personverntjenesten. Dette vil medføre en veldig kompleks løsning for å vedlikeholde sperrer da personverntjenesten i en slik løsning vil måtte ha kjennskap til detaljer rundt hvilke elementer som foreligger i den enkelte EPJ. For å støtte en slik funksjonalitet anses det som mest gunstig at dette tilbys som en del av innsynstjenestene for den enkelte journal på helsenorge.no. Her vil innbyggeren kunne få innsyn i sin journal og da samtidig kunne forespør å sperre av enkeltelementer gjennom dialogfunksjonalitet med behandler. Ved sperring av enkeltelementer vil dette bli lagret lokalt i det enkelte journalsystem, men samtidig vil det bli tilgjengeliggjort for innbyggeren at det foreligger en sperre gjennom innsynstjenesten på helsenorge.no. På sikt kan det tenktes at en mer sentralisert løsning for sperrefunksjonalitet kan etableres som en del av en felles journalløsning. Dette må ses i sammenheng med pågående utredning «En innbygger, en journal».

3.4.1.5 Innsynsbegrensning

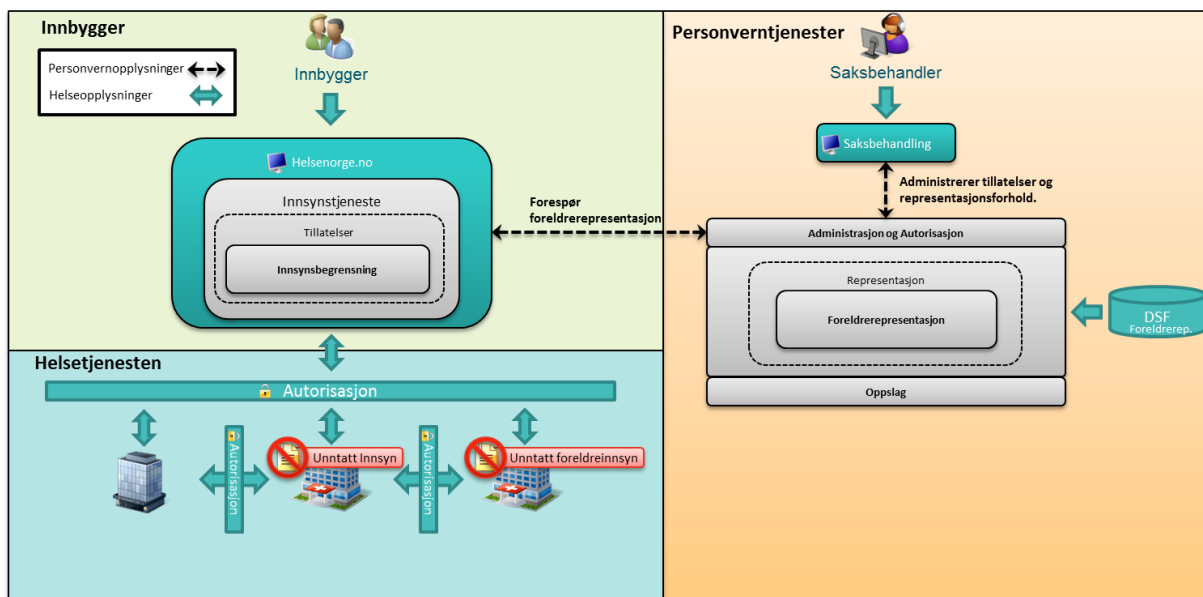


Figur 23: Logisk informasjonsmodell for innsynsbegrensning.

Figur 23 viser logisk informasjonsmodell for innsynsbegrensning. Som det her illustreres skal behandler kunne begrense innbyggers innsyn i sine egne eller andres helseopplysninger ved å unnta opplysninger fra innsyn. Dette gjelder ifølge ny pasientjournallov i hovedsak to ulike tilfeller

1. Pasientens innsyn kan bare begrenses der det er nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv eller det er helt klart utilrådelig å gi innsyn av hensyn til personer som står pasienten nær.
2. Ungdom 12-16 år kan i samråd med behandler begrense foresattes innsyn i sine helseopplysninger ved å unnta opplysninger fra foreldreinnsyn.

Figur 24 viser en konseptuell skisse for håndtering av innsynsbegrensning. Selv om funksjonaliteten for å registrere selve innsynsbegrensningen er tenkt å ligge utenfor personverntjenesten vil den allikevel være sentral ved etablering av journalinnsynstjenester. Dette gjelder både ved innsyn for innbyggeren selv, og ved foreldrerepresentasjon der det vil være behov for å begrense foresattes innsyn for barn 12-16 år. For å støtte denne funksjonaliteten må hele eller deler av journalen kunne merkes for begrenset innsyn i det enkelte tilfelle. For å ivareta dette foreslås det å merke utvalgte opplysninger med betegnelsen «UNNTATT» og så etterfulgt av type innsynsbegrensning. Det vil eksempelvis for gjeldene tilfeller utgjøre «UNNTATT_INNSYN» for begrenset innsyn for innbyggeren selv, og «UNNTATT_FORELDREINNSYN» for begrenset innsyn for foresatte ved foreldrerepresentasjon.



Figur 24: Konseptuell skisse for håndtering av innsynsbegrensning.

For realisering av denne funksjonaliteten vil det tilsvarende som for sperre på dokumentnivå være behov for å kunne begrense innsyn for enkeltdokumenter. Som beskrevet under kapittelet om sperrefunksjonalitet over, vil det være veldig kompliserende å realisere slik funksjonalitet i en sentral personverntjeneste. Det anbefales derfor at informasjon om denne typen innsynsbegrensning ligger lagret lokalt i den enkelte EPJ. Ved realisering av de ulike journalinnsynstjenestene på helsenorge.no vil den enkelte aktør måtte sikre at helseopplysninger som er merket med begrenset innsyn tilbakeholdes innbygger i den enkelte oppslagstjeneste.

DELING AV HELSEOPPLYSNINGER MELLOM HELSEVIRKSOMHETER

Ved deling av helseopplysninger mellom helsevirksomheter må det tas stilling til om en sperre eller innsynsbegrensning som er satt i EPJen hos en aktør skal følge dokumentet ved utlevering. Dersom det er ønske om å ivareta denne funksjonaliteten er det viktig at meldingsstandarden som benyttes for utlevering av helseopplysningene inneholder noe metainformasjon for å angi at det foreligger en innsynsbegrensning eller sperre.

3.4.1.6 Aktørportal: Innsyn VS utlevering

En utfordring ved utlevering av helseopplysninger som for eksempel til forsikringsselskap er at når helseopplysningene først er utlevert mister innbyggeren kontroll over hva som skjer med helseopplysningene i etterkant. Så lenge det er snakk om manuell utlevering per post vil det være naturlig at helseopplysningene overleveres til aktøren som har forespurt informasjonen. Derimot er helseopplysningen i dag i stor grad basert på digitalt lagret informasjon. Et alternativ til utlevering er å gi aktøren, som har behov for tilgang til helseopplysninger om en innbygger,

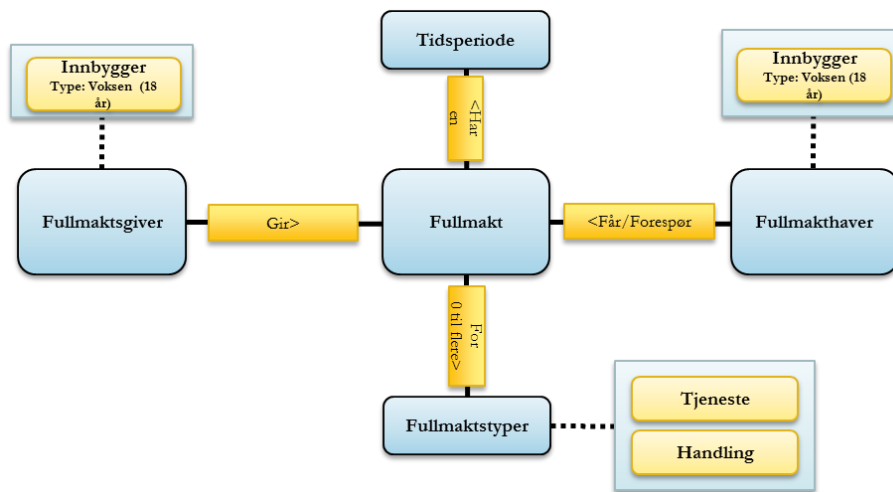
innsyn i hele eller deler av journalen i en begrenset periode. Informasjonen blir da aldri duplisert ved at den overleveres til aktøren. For å realisere en slik løsning vil dette kunne gjøres på flere måter. Enten kan det eksponeres et grensesnitt for oppslag til eksterne aktører som da presenterer informasjonen i sitt saksbehandlersystem uten at informasjonen lagres lokalt. Et annet alternativ er at det etableres en aktørportal der den enkelte aktør kan logge seg på for å forespørre om helseopplysninger for en innbygger. Helseopplysningene vil da bli tilgjengeliggjort for aktøren såfremt innbyggeren godkjenner dette. Fordelen med en slik løsning er at helseopplysningene kun vil bli tilgjengeliggjort i en sentral portal, og man har da langt bedre kontroll på tilgangen til helseopplysningene. Eksempelvis kan det da legges på funksjonalitet som gjør at helseopplysningene ikke kan kopieres, og det kan også kontrolleres at den kun er tilgjengelig i den perioden det er relevant. I tillegg er andre fordeler blant annet:

- Hver aktør slipper å implementere sin egen løsning for visning av helseopplysningene. Dette er spesielt gunstig for mindre aktører som kanskje ikke har ressurser til å tilpasse systemene for en slik visning.
- Det muliggjør full kontroll i forhold til logging og hvilken aktør som aksesserer informasjonen.
- Det vil være mulig å mellomlagre helseopplysninger temporært dersom det er behov for innsyn i pasientjournaler fra eksempelvis fastlege som ofte ikke har journalsystemet tilgjengelig 24/7.

3.4.2 Representasjon

Som beskrevet i den funksjonelle beskrivelsen i kapittel 3.2.1 skal personverntjenesten kunne håndtere representasjon både i form av fullmakt, foreldrerepresentasjon og verge. Foreldrerepresentasjon er en lovfestet rett basert på en familierelasjon, så selve etableringen av representasjonsforholdet ligger utenfor personverntjenesten. I disse tilfellene må derimot personverntjenesten ta stilling til hvilke tjenester som skal være tilgjengelig ved bruk av representasjonsforholdet. For fullmakt er funksjonaliteten litt annerledes da personverntjenesten her også må tilby funksjonalitet for å etablere et representasjonsforhold mellom to innbyggere. Dette vil være tilsvarende for vergemål som håndteres som et spesialtilfelle av fullmakt. Tjenestene for å realisere de ulike representasjonsforholdene vil bli beskrevet videre i detalj i dette kapitlet.

3.4.2.1 Fullmakt

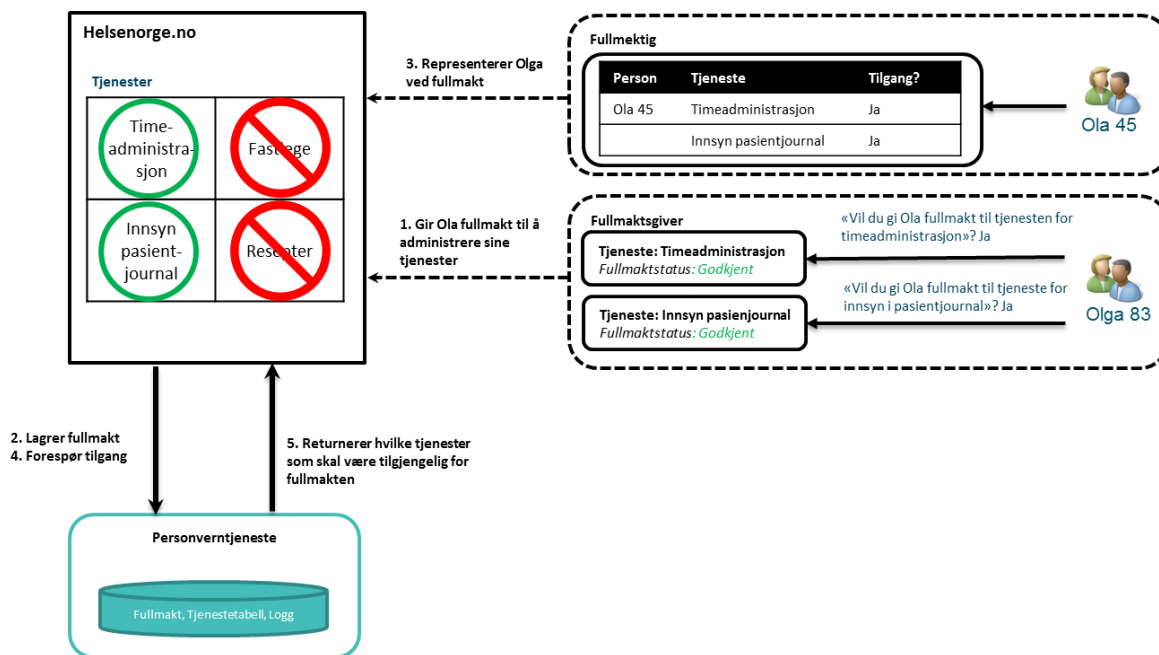


Figur 25: Logisk informasjonsmodell for fullmakt.

Figur 25 viser logisk informasjonsmodell for fullmakt. Som det her illustreres skal tjenesten for fullmakt muliggjøre at en innbygger skal kunne gi fullmakt til en annen. Nøyaktig hva en enkelt fullmakt skal omfatte vil være avhengig av det enkelte tilfellet. Da det er 3 hovedtyper av fullmakt som vil avvike noe i forhold til hvordan de realiseres er det valgt å skille mellom 1) Fullmakt for tjenester på helsenorge.no, 2) Fullmakt for eksterne tjenester eller handlinger 3) Fullmakt for vergemål.

FULLMAKT FOR TJENESTER PÅ HELSENORGE.NO

Fullmakt for bruk av digitale tjenester eksponert gjennom Helsenorge plattformen bør ha en felles og enhetlig måte for å tilby denne funksjonaliteten. Måten det er tenkt å løse dette på er å ha en felles tjenestetabell som er master for alle tjenester som tilbys på helsenorge.no. Personverntjenesten vil være master både for tjenesteoversikten og selve fullmakten. Fordelen med en slik arkitektur er at både administrasjon av hvilke tjenester som skal være tilgjengelig via fullmakt, og selve fullmakten er samlet i en sentral løsning. Tilgangen via fullmakt er derved uavhengig av hvilken plattform som benyttes for realisering av tjenestene. Dette er illustrert nærmere i Figur 26 der Olga på 83 år gir sin sønn Ola fullmakt til å utføre tjenester for timeadministrasjon og innsyn pasientjournal på helsenorge.no. Som det her vises vil både tjenestetabellen over tilgjengelige tjenester, selve fullmakten og tilhørende representasjonslogg over bruk lagres i personverntjenesten. Det vil også gjøres separate kall fra Helsenorge plattformen for å evaluere hvilke tjenester som skal være tilgjengelig for Ola når han utfører tjenester på vegne av sin mor.



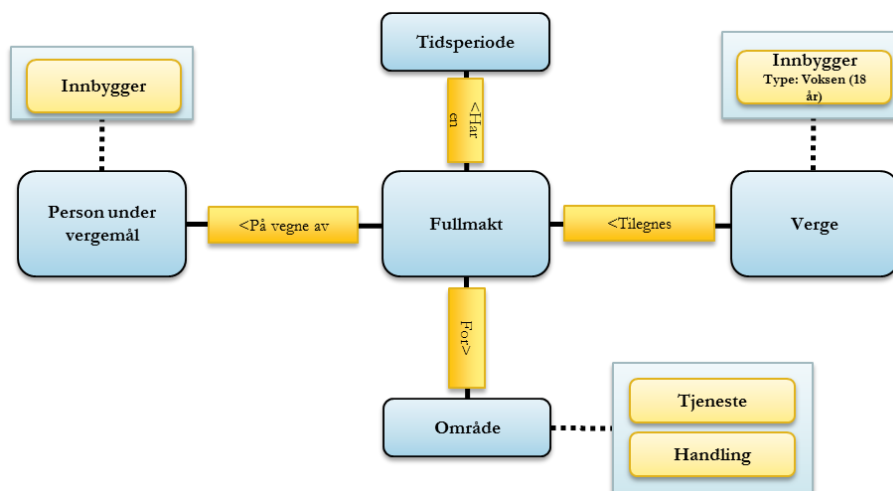
Figur 26: Konseptuell skisse for håndtering av fullmakt.

En fullmakt kan både gjelde en enkelt tjeneste, men også være en mer utvidet fullmakt der fullmaktsgiver gir fullmektig tilgang til alle tjenester som det er mulig å gi fullmakt for på helsenorge.no. Det er ønskelig å kunne tilby en slik funksjonalitet for å gjøre det enkelt for brukere som ikke ønsker å spesifisere hver enkelt tjeneste.

FULLMAKT FOR EKSTERNE TJENESTER ELLER HANDLINGER.

For eksterne tjenester eller handlinger som eksempelvis fullmakt til å hente ut resepter på vegne av andre i apotek vil helsenorge.no kunne fungere som en digital kanal for å gi innbyggeren mulighet til å registrere fullmakten digitalt på nett. Fullmakten vil da bli lagret i personverntjenesten og de eksterne aktørene som i dette eksemplet apotek vil kunne få tilgjengeliggjort en tjeneste (API) for å kunne slå opp fullmakten fra apotekerløsningen.

FULLMAKT FOR VERGEMÅL



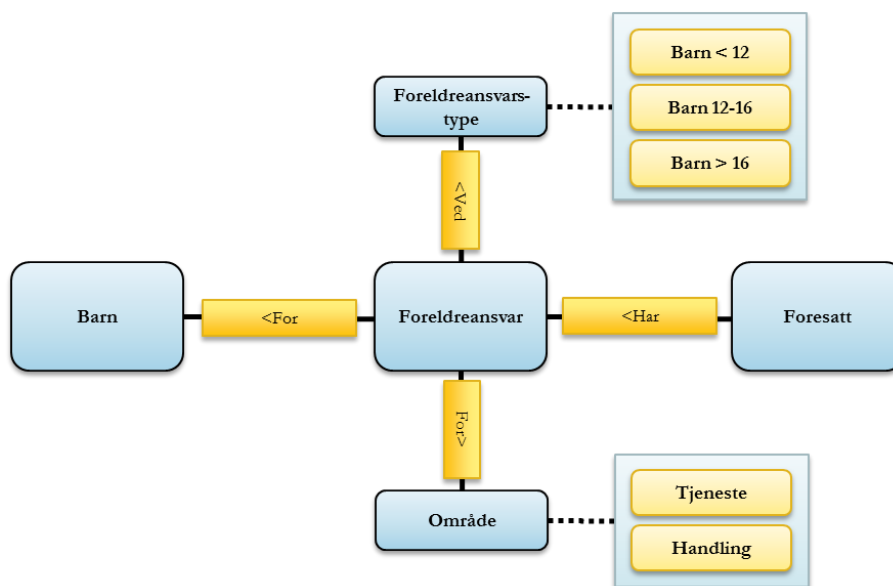
Figur 27: Logisk informasjonsmodell for vergemål.

Figur 27 viser logisk informasjonsmodell for fullmakt som følge av vergemål. Til forskjell fra vanlig fullmakt illustrert i Figur 25 vil fullmakten her tilegnes fullmektig gjennom en analog kanal basert på vedtakets omfang.

3.4.2.1.1 Felles nasjonal fullmaktskomponent

Som beskrevet under kapittel 1.3 er det etablert et pågående SKATE prosjekt for å se på muligheten for å etablere en felles nasjonal komponent for å håndtere fullmakt og mulig også andre representasjonsforhold. En endelig konklusjon i forhold til om, og evt. hvordan en slik løsning skal implementeres er enda ikke avklart. Derimot er en hybridløsning det alternativet som kommer best ut i foreløpig evaluering. Hybridløsningen er basert på at det etableres en sentral felleskomponent som hver sektorvis løsning kan gjøre oppslag mot. Dette er også ivare tatt i arkitekturen beskrevet for personverntjenesten. Løsningen vil da gjøre oppslag mot en sentral komponent og tilpasser brukerens rettigheter basert et gitt sett med kriterier. Eksempelvis kan det tenkes at det i en nasjonal løsning vil etableres en generalfullmakt for å kunne utføre helsetjenester på vegne av en annen innbygger på nett. Personverntjenesten vil tilpasse innbyggerens tilganger basert på om det foreligger en slik fullmakt i sentral komponent.

3.4.2.2 Foreldrerepresentasjon



Figur 28: Logisk informasjonsmodell for foreldrerepresentasjon.

Figur 28 viser logisk informasjonsmodell for foreldrerepresentasjon. Som det her illustreres skal tjenesten gi innbyggeren mulighet til å representere sine barn frem til fylte 16 år. Informasjon om hvem som har foreldreansvar ligger i dag lagret i folkeregisteret, og kan benyttes for å evaluere hvem som skal kunne representere barnet. En svakhet ved bruk av DSF er at det ikke foreligger noe informasjon om foresatte også har daglig omsorg for barnet. For å kunne vurdere dette vil det for foresatte som har foreldreansvar for barnet måtte sjekkes om de også har samme bostedsadresse. En annen utfordring ved bruk av folkeregisteret er at informasjonsfeltet for foreldreansvar ofte ikke blir oppdatert i tilfeller der omsorgsansvaret er overført til den kommunale barneverntjenesten ved rettslig vedtak. Foresatte skal da ha betydelig innskrenket foreldreansvar. Dette kan medføre feilaktig autorisert for bruk av en rekke tjenester. Det anbefales derfor å følge opp at datakvaliteten for foreldreansvar følges opp tettere hos DSF.

LØSNING FOR FORELDREPRESENTASJON PÅ HELSENRGE.NO

I løsningen for å støtte foreldrerepresentasjon på helsenorger.no vil det være viktig å skille mellom følgende tilfeller

Tabell 39: Ulike tilfeller av foreldrerepresentasjon.

| Tilfeller | Beskrivelse |
|---------------|---|
| Barn < 12 år | Foresatte skal ha full tilgang til barnets tjenester ved foreldrerepresentasjon. |
| Barn 12-16 år | Foresatte skal ha begrenset tilgang til barnets tjenester ved foreldrerepresentasjon. |

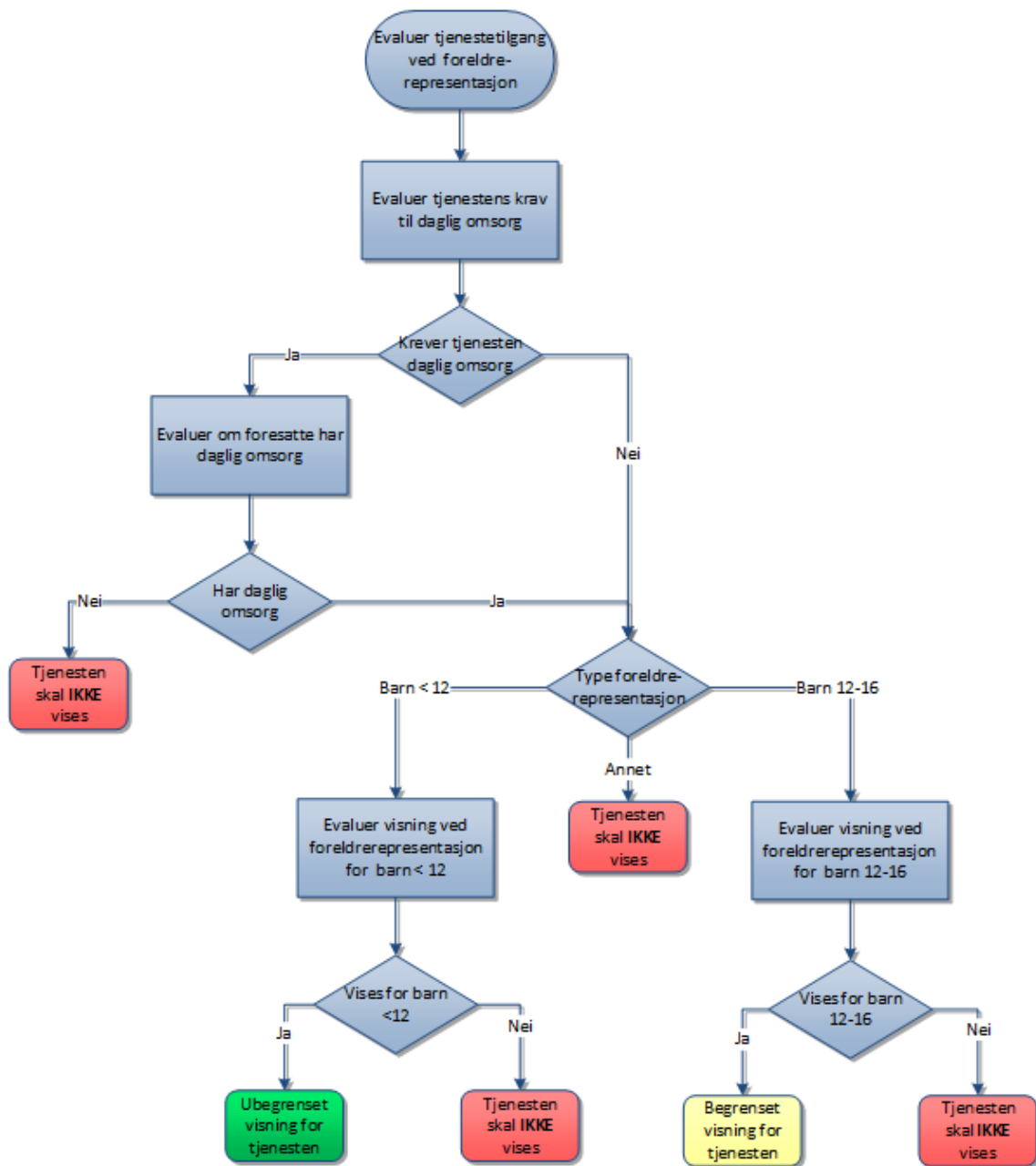
| Tilfeller | Beskrivelse |
|------------------------|---|
| Barn > 16 år | Foresatte skal ha ingen tilgang til barnets tjenester ved foreldrerepresentasjon. |

Håndtering av Barn < 12 og Barn > 16

Som illustrert i flytdiagrammet i Figur 29, vil tilfeller der barnet enten er under 12 eller over 16 år være enkle å håndtere da foresatte enten skal ha full tilgang eller ingen tilgang til barnets tjenester. Dersom barnet er under 12 år skal i utgangspunktet foresatte alltid ha tilgang, men for enkelte tjenester i helsesektoren har det vist seg at dette enda ikke er mulig da de ikke har støtte for tilfredsstillende logging ved representasjon. Det er derfor behov for å begrense foresattes tilgang for enkelte tjenester. Det vil også kunne være noen unntak innenfor helseøkonomi der foresatte skal kunne handle på vegne av sine barn som er mellom 16 og 18 år. Funksjonalitet for å håndtere dette vil i så fall måtte avklares nærmere for den enkelte tjeneste.

Håndtering av Barn 12-16

Tilfellet der barnet er mellom 12 og 16 år, er derimot mer komplekst å håndtere da barnet i samhandling med behandler har mulighet til å begrense innsyn for foresatte. Dette krever at hver enkelt tjeneste må ha funksjonalitet for å kunne holde tilbake helseopplysninger som ikke skal vises for foresatte. De tjenestene som ikke har støtte for slik funksjonalitet vil foresatte ikke kunne få tilgang til. Dette er illustrert i flytdiagrammet i Figur 29.

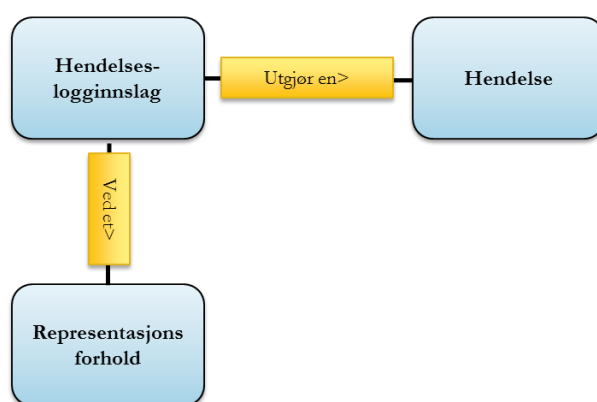


Figur 29: Flytdiagram for evaluering av tilgang til tjenester ved foreldrerepresentasjon

3.4.3 Logg

3.4.3.1 Logg over bruk på helsenorge.no

Bruksloggen skal håndtere funksjonalitet for logging av hendelser for en innbygger både ved egen og andres bruk av tjenester på helsenorge.no. Dette er viktig for å kunne gi innbyggeren en overordnet oversikt over hvilke tjenester som er blitt benyttet og når handlingen ble utført. Dette gjelder både ved egen og andres bruk av tjenestene ved representasjon.



Figur 30: Logisk informasjonsmodell for hendelseslogg.

Figur 30 viser en logisk informasjonsmodell for hendelsesloggen. Hendelseslogginnslaget har både en hendelse som beskriver hvilken hendelse som er utført, i tillegg til representasjonsforholdet som beskriver hvem som har utført handlingen. Følgende representasjonsforhold anses som aktuelle for målbildet

Tabell 40: Type representasjonsforhold i hendelsesloggen.

| Representasjonsforhold | Beskrivelse |
|-------------------------------------|--|
| Meg selv | Bruk av egne tjenester på helsenorge.no |
| Fullmakt (Gitt av innbygger) | Andres bruk av egne tjenester ved fullmakt |
| Fullmakt (Vergemål) | Andres bruk av egne tjenester ved fullmakt som følge av vergemål |
| Foreldreansvar | Andres bruk av egne tjenester ved foreldreansvar |

Både med tanke på ytelse og kompleksitet anbefales det at hendelsesloggen (i hvert fall som en førsteversjon) holdes på et overordnet nivå. Den kan heller utvides til mer detaljert logging ettersom man bygger erfaring på hvordan tjenesten vil fungere i produksjon. I hovedsak vil da tjenesten logge hvilke tjenester som ble benyttet og tidspunkt for hendelsen. Dersom det er behov for ytterligere detaljer i forhold til logging av hvilke endringer som ble gjort innenfor en enkelt tjeneste, anses dette som funksjonalitet som heller bør være en del av tjenesten.

3.4.3.2 Oppslagslogg

Oppslagsloggen er en tjeneste som muliggjør at innbyggeren skal få se en oversikt over eksterne forespørsler mot personverninnstillingene fra helsesektoren. Dette kan eksempelvis være ved henting av resepter i apotek. Det vil da logges når den eksterne aktøren gjør et oppslag for å evaluere et representasjonsforhold. Aktøren bør da også måtte oppgi formålet for oppslaget.

3.4.3.3 Utleveringslogg

Utleveringsloggen skal gi en samlet oversikt over utlevering av innbyggerens helseopplysninger i helsesektoren. Tjenesten vil kunne realiseres ved at det gjøres et synkront oppslag mot den enkelte EPJ, eller ved at det etableres en tjeneste i personverntjenesten for å melde inn utlevering av helseopplysninger mellom to aktører. Dette bør ses i sammenheng med løsningen for å innhente samtykke for utlevering av helseopplysninger. Det ideelle hadde vært å samle disse opplysningene sentralt i personverntjenesten, og latt den enkelte helsevirksomhet ha mulighet til å slå opp eller abonnere på sine utleveringer. Spørsmålet er da om det kan etableres en felles tjeneste i personverntjenesten for utlevering av helseopplysninger. Her kan aktøren enten informere, eller forespørre samtykke ved behov for utlevering/innhenting av personopplysninger. Innbygger kan da enten samtykke, eller ha mulighet til å reservere seg. Aktøren bør da også være pliktig til å melde inn hvilken informasjon som faktisk er utlevert og tidspunktet for utleveringen til personverntjenesten. Dette vil da bli registrert i utleveringsloggen. Hvilken løsning som velges bør avklares i samarbeid med EPJ leverandørene.

3.4.3.4 Brukslogg helsepersonell

Bruksloggen for helsepersonells bruk av helseopplysninger skal gi innbyggeren en oversikt over hvilke helsepersonell som har vært inne og sett på sine helseopplysninger for den enkelte innsynstjeneste. Da dette anses som informasjon som typisk vil ligge lagret i den enkelte EPJ eller helseregister er det tenkt at denne tjenesten bør realiseres ved synkront oppslag mot de eksterne tjenestene.

3.4.4 Oppslag og registreringstjenester for helsesektoren

Oppslag og registreringstjenesten inneholder all personvernfunksjonalitet som skal være tilgjengelig for oppslag og registrering fra eksterne aktører i helsesektoren. Basert på evalueringen av de ulike tjenesteområdene over i målbildet er det identifisert behov for en rekke oppslag og registreringstjenester. Disse er gitt i Tabell 41.

Tabell 41: Oppslag og registreringstjenester for helsesektoren.

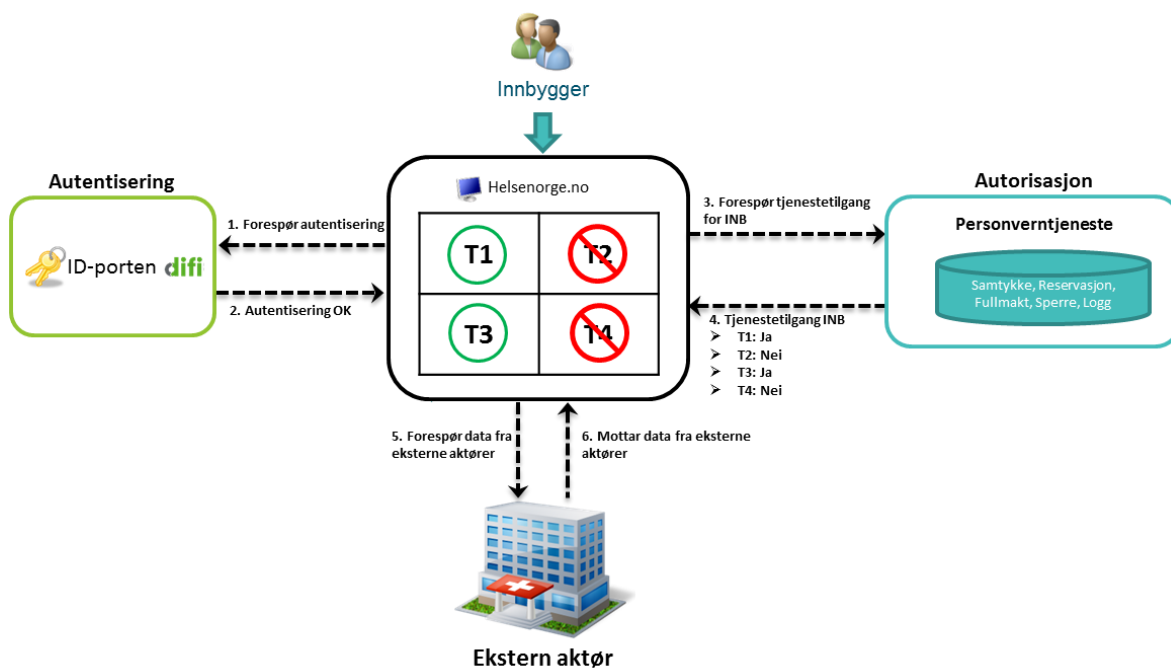
| Tjenesteområde | Tjeneste | Beskrivelse |
|--|---|---|
| Tillatelse: Samtykke og Reservasjon | Forespør samtykke | Tjeneste der en aktør kan forespørre et samtykke fra en innbygger. |
| | Hent samtykke for innbygger | Tjeneste der en aktør kan sjekke om en innbygger har samtykket til en tjeneste eller handling. |
| | Hent reservasjon for innbygger | Tjeneste der en aktør kan sjekke om en innbygger har reservert seg mot en tjeneste eller handling. |
| | Informer innbygger om handling med reservasjonsmulighet | Tjeneste som muliggjør at en aktør kan informere innbyggeren om at det er planlagt å utføre en handling på vegne av innbyggeren med reservasjonsmulighet. |
| Tillatelser: Sperre | Hent sperre for innbygger | Tjeneste som muliggjør at en aktør kan sjekke om en innbygger har sperret alle sine helseopplysninger for enkelte helsepersonell, eller utvalgte opplysninger for alt helsepersonell. |
| Representasjon | Hent representasjonsforhold for innbygger | Henter alle gjeldende representasjonsforhold for en innbygger. Dette gjelder mulige representanter og omfang både i form av foreldrerepresentasjon og fullmakt. |

I tillegg til å eksponere ut en rekke oppslagstjenester for å tilby personvernfunksjonalitet ut mot helsesektoren, vil aktørene i helsesektoren også kunne få støtte for personvernfunksjonalitet ved å tilby sine digitale tjenester til innbyggeren som en integrert del av Helsenorge plattformen. Her vil den eksterne aktøren typisk være dataleverandør i tillegg til å tilby enkle oppslagstjenester for funksjonalitet på Helsenorge plattformen. For disse tjenestene vil helsenorge.no som en integrert og standardisert del av plattformen kunne tilby en rekke personverntjenester. En oversikt over tjenestene er gitt i Tabell 42.

Tabell 42: Personvernfunksjonalitet for tjenester eksponert gjennom helsenorge.no.

| Tjenestemråde | Tjeneste | Beskrivelse |
|-----------------------|--|---|
| Tillatelse | Reservasjon mot tjenester på nett | Dette vil være funksjonalitet som gir innbyggeren mulighet til å reservere seg mot å ha hele eller deler av tjenesten tilgjengelig på nett. Det vil her også tilbys en separat kanal for manuell opphevelse av reservasjonen. |
| | Foreldresamtykke | Funksjonalitet for at foresatt kan samtykke til at sine barn mellom 12 og 16 år kan ta i bruk hele eller deler av tjenesten. |
| Innsyn | Dialogfunksjonalitet for retting og sletting | Dialogfunksjonalitet der innbyggeren kan forespør retting og sletting av helseopplysninger. Dette krever at den eksterne aktøren har en EPJ løsning som har støtte for dialogfunksjonalitet. |
| | Dialogfunksjonalitet for elementsperre | Dialogfunksjonalitet der innbyggeren kan forespør sperring av enkeltelementer for innsyn fra helsepersonell. Dette krever at den eksterne aktøren har en EPJ løsning som har støtte for sperrefunksjonalitet. |
| Representasjon | Foreldrerepresentasjon | Funksjonalitet for at foresatte skal kunne ta i bruk hele eller deler av tjenesten på vegne av sine barn. Her vil det gjøres automatisk oppslag mot PREG (DSF) for å evaluere om det foreligger et foreldreforhold |
| | Fullmakt | Funksjonalitet for at en innbygger kan gi fullmakt til en annen innbygger for hele eller deler av tjenesten. I tillegg vil en vergerepresentasjon støttes som et spesialtilfelle av fullmakt. |
| Logg | Brukslogg på Hn.no | En overordnet logg over innbyggerens egen og andres bruk av tjenester på helsenorge.no |

Figur 31 viser konseptuell skisse for håndtering av personvernfunksjonalitet og derav autentisering og autorisasjon for tjenester eksponert gjennom Helsenorge plattformen.



Figur 31: Konseptuell løsning for personverntjenester ved eksponering gjennom Helsenorge plattformen.

| Steg | Beskrivelse |
|---|--|
| Steg 1-2: Innbyggeren autentiseres | Innbyggeren logger seg inn og blir autentisert gjennom ID porten. |
| Steg 3-4: Utfører autorisasjon | Helsenorge.no kaller personverntjenesten for å kunne autorisere hvilke tjenester innbyggeren skal ha tilgang til. Hvilke tjenester som skal være tilgjengelig vil være en kombinasjon av hvilke samtykker, reservasjoner og representasjonsforhold som foreligger for innbyggeren. |
| Steg 5-6: Kaller eksterne aktører | Henter nødvendig datagrunnlag for tjenesten ved å gjøre kall mot eksterne aktører. |

Som illustrert i figuren vil personverntjenesten fungere som en adskilt autorisasjonstjeneste der helsenorge.no kan forespørre om hvilke tjenester som skal være tilgjengelig for innbyggeren. Selve prosessen vil være lik dersom brukeren ønsker å utføre tjenester på vegne av en annen innbygger ved representasjon. Helsenorge.no-plattformen vil da forespørre personverntjenesten hvilke representasjoner som er tilgjengelig for innbyggeren. Innbyggeren vil da få mulighet til å bytte til en annen bruker, og en ny tjenesteliste (tilsvarende som i steg 4) vil bli returnert i forhold til hvilke tjenester som skal være tilgjengelig ved representasjonsforholdet.

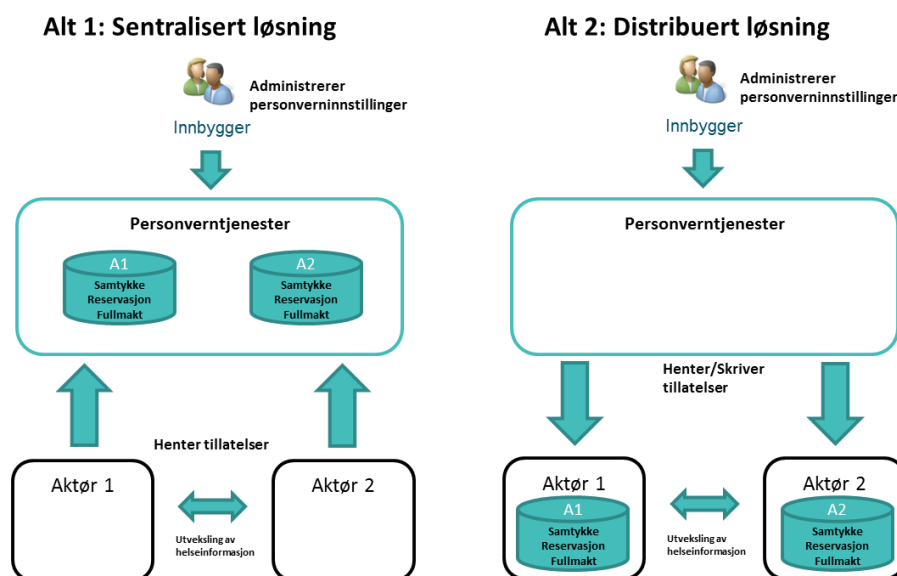
3.5 Personverninnstillinger og masterdatastrategi

Uavhengig av tjenestetype vil en sentral diskusjon være hvor personverninnstillinger skal være lagret og hvilken komponent som skal være master. For å kunne evaluere fordeler og ulemper ved valg av masterdatastrategi vil det være viktig å se på tiltenkt bruk av tjenesten og prioriterte kvalitetsparametere. I hovedsak så er det 3 ulike kanaler/behov som må hensyntas:

1. *Innbygger som administrerer sine personverninnstillinger på helsenorge.no* og har behov for tilgangsstyring av sine tjenester basert på personverninnstillingene.
2. *Forvaltningen som utfører ulike forvaltningsoppgaver* og som er avhengig av personverninnstillinger. Både i forhold til generell saksbehandling og rapportering. Eksempelvis ved administrasjon av Fastlegeordningen må det gjøres oppslag i forhold til om innbyggeren har reservert seg mot ordningen.
3. *Innbyggere som har behov for å administrere sine personverninnstillinger gjennom en analog kanal.* Dette vil være innbyggere som av ulike grunner ikke har mulighet til å administrere sine personverninnstillinger på nett.

For valg av masterdatastrategi er det her i hovedsak to ulike alternativer

1. **Sentralisert løsning – Personverntjenesten er master:** Personverninnstillinger ligger lagret i personverntjenesten og de eksterne tjenestene kaller på personverntjenesten for å kontrollere om det foreligger tillatelser eller representasjonsforhold.
2. **Distribuert løsning – Aktørene er master:** Personverninnstillinger ligger lagret i de eksterne tjenestene og personverntjenesten oppdaterer de eksterne tjenesten ved innhenting av personverninnstillinger fra innbyggeren.



Figur 32: Illustrasjon av forskjellen mellom sentralisert og distribuert løsning for tillatelser

En sentralisert løsning (alternativ 1) vil med tanke på kontroll av data og informasjonsflyt være mest optimal da man i dette tilfellet vil få lagret alle tillatelser et sted. Dette vil sikre bedre kontroll på datagrunnlaget, i tillegg til at man ved tjenester som er eksponert på helsenorge.no vil slippe å gjøre kall mot eksterne tjenester for evaluering av autorisasjon. Dette er en fordel for å sikre responsive tjenester og høy tilgjengelighet for innbyggeren. I tillegg vil personverntjenesten i mange tilfeller tilby ferdig funksjonalitet som kan gjenbrukes. Eksempelvis ved registrering av fullmakt vil tilgjengeliggjøring av tjenestene for fullmektig i tillegg til logging automatisk bli håndtert ved eksponering gjennom helsenorge.no. Ulempen med denne løsningen er at man vil få et «Single-Point-Of-Failure». Dersom personverntjenesten er nede vil dette kunne hindre tilgangskontroll for en rekke systemer i helsesektoren.

En distribuert løsning (alternativ 2) vil med tanke på datakontroll og informasjonsflyt være mindre optimal, derimot vil det for noen tjenester kunne være kompliserende å tilpasses for en sentralisert løsning. Dette vil eksempelvis være tjenester som allerede har implementert støtte for reservasjon eller samtykket lokalt, og evt. også har en samsvarende sakbehandlerløsning for håndtering av tillatelser. Dette gjelder eksempelvis Kjernejournal. En fordel med alternativ 2 er at det enkelte system blir mindre avhengig av personverntjenesten som følge av lokal lagring av tillatelsene.

Den mest optimale løsningen vil trolig være å benytte en sentralisert løsning der alle personverninnstillinger lagres sentralt i personverntjenesten, men samtidig benytte ulike tiltak for å sikre robusthet og høy tilgjengelighet, selv om personverntjenesten eventuelt skulle være nede. Dette vil blant annet være

- Sikre høy opptid for personverntjenesten ved å benytte flere instanser og høy redundans.
- Muliggjøre lokale instanser for tilgangskontroll ved å tilby abonnement baserte synkroniseringstjenester for endringer, tilsvarende som er benyttet for DSF i dag. Hvert helseforetak vil da kunne ha sin egen lokale instans for kontroll av tillatelser. De vil da motta oppdateringer dersom innbyggeren gjør endringer i sine personverninnstillinger.

Da helsesektoren består av veldig mange ulike systemer og aktører med ulikt behov vil det trolig være behov for å tilby en arkitektur som muliggjør å benytte både en sentralisert og distribuert løsning. Derimot bør det da etableres en strategi som tilrettelegger for å gå mot en sentralisert løsning på sikt.

3.6 Overordnede løsningskonsepter

For realisering av personverntjenesten vil det være flere ulike alternativer. Det vil være behov for en plattform som støtter lagring av personvernopplysningene, i tillegg til etablering av de

nødvendige grunntjenestene sektoren og innbygger (via helsenorge.no) har behov for. Følgende alternativer er vurdert

1. Basert på en felles nasjonal komponent på tvers av etater
2. Basert på videreutvikling av eksisterende komponent på helsenorge.no.
 - a. Reimplementere personverntjenesten på Helsenorge plattformen med en full implementasjon av XACML standarden inkludert policies.
 - b. Videreutvikling personverntjenesten på Helsenorge plattformen med egendefinerte grensesnitt.
 - c. Benytte registerplattformen hos Norsk helsenett.
3. Basert på å anskaffe en ny hyllevareløsning.

Alternativ 1, å basere seg på en felles nasjonal komponent for håndtering av personvernfunksjonalitet på tvers av sektorer anses ikke som et realistisk alternativ på nåværende tidspunkt. Det pågår noe arbeid med å se på en slik løsning i forbindelse med SKATE prosjektet (se kapittel 1.3), men det vil ligge lagt frem i tid før en slik løsning faktisk vil bli implementert. Derimot vil løsningen legge til rette for å integrere mot en slik løsning dersom det skulle bli aktuelt i fremtiden.

I forhold til alternativ 2a, skal personverntjenesten fungere som en PDP for helsenorge.no, men kun som en PIP for resten av helsesektoren. Da grensesnittet for tilgangsstyring på helsenorge.no er veldig skreddersydd i forhold til tjenestemodellen på helsenorge.no, anses det ikke som hensiktsmessig å basere seg på XACML standarden for dette tilfellet. For resten av sektoren vil personverntjenesten kun fungere som en PIP så det er da opp til NSI, eller den enkelte aktør å velge format for autorisasjonsgrensesnittet.

For alternativ 3 anses det ikke som hensiktsmessig å etablere en ny hyllevareløsning for dette formålet. Både fordi det allerede eksisterer to alternative plattformer (2b og 2c) der slik funksjonalitet vil kunne implementeres, og fordi det er mange spesialtilfeller som uansett ville måtte konfigureres/implementeres i en hyllevareløsning. Det utelukkes dog ikke at en hyllevareløsning for å håndtere mye av tilgangsstyringen på tvers av helsesektoren vil etableres som en del av NSI prosjektet eller som en del av «En innbygger, en journal». Personverntjenesten vil da fungere som en PIP for disse komponentene.

Da mye av personvernfunksjonaliteten allerede er blitt implementert som en separat personverntjeneste på Helsenorge plattformen (alternativ 2b) anbefales det at denne videreutvikles på kort sikt. Tjenesten er implementert som en separat komponent som enkelt vil

kunne migreres over til registerplattformen hos NHH. Det anbefales derfor å gjøre en videre vurdering av om alternativ 2c bør benyttes på sikt.

3.7 Målarkitektur og avhengigheter

Helsedirektoratet har flere pågående prosjekter og aktiviteter som vil ha store avhengigheter i forhold til personverntjenesten og fremtidig målarkitektur. Dette er blant annet

Tabell 43: Oversikt over målarkitektur og avhengigheter.

| Prosjekt/Initiativ | Beskrivelse | Avhengighet |
|---|---|---|
| Personlig helsearkiv | <p>Personlig helsearkiv skal gi innbyggeren oversikt sin helseinformasjon. Dette inkluderer både</p> <ol style="list-style-type: none"> 1. Dialog med fastlege og timeavtaler. Elektronisk dialog med fastlege i tillegg til timeavtaler skal lagres i innbyggerens personlige helsearkiv. 2. Egne notater og tilleggsinformasjon som innbyggeren selv ønsker å ta vare på/legge til. | <p>Tilgangen til helseopplysningene i innbyggerens personlige helsearkiv må være i tråd med innbyggerens personverninnstillinger. Eksempelvis må PHA ivareta tilgangsstyring av meldinger basert på omfanget av innbyggerens fullmakter.</p> |
| En innbygger, en journal | <p>«En innbygger, en journal» er en pågående konseptvalgutredning som ser på muligheten for å etablere en felles pasientjournal på tvers av helsesektoren.</p> | <p>Hvor og hvordan innbyggerens helseopplysninger lagres og struktureres vil være avgjørende for å kunne ivareta tilgangsstyring av enkeltelementer både i form av samtykke, reservasjon, sperre og innsynsbegrensning.</p> |
| Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren | <p>Fokus for NSI er sikker samhandling og informasjonsdeling på tvers av virksomheter i helse- og omsorgssektoren slik at helsepersonell og annet personell med behov skal ha tilgang til all relevant pasientinformasjon uavhengig av hvor informasjonen er lagret. Felleskomponentene skal dekke helse- og omsorgssektorens behov for identitets- og tilgangsstyring på tvers av hele sektoren.</p> | <p>En sentral løsning for autentisering og autorisasjon vil være helt avgjørende for å kunne ivareta innbyggerens personvern. Eksempelvis vil det ikke ha noen funksjon å sette en sperre dersom det ikke finnes noen funksjonalitet for å sikre at sperren blir ivaretatt.</p> |

Utfallet av prosjektene over vil være av stor betydning i forhold til realisering av målarkitekturen for personvern. For «Personlig helsearkiv» og «En innbygger, en journal» vil avhengigheten i hovedsak dreie seg om hvordan tilgangsstyring av helseinformasjonen gjøres. Da både mot helsepersonell og innbyggeren selv. Dersom eksempelvis prosjektet for «En innbygger, en journal» konkluderer med at det skal etableres en felles nasjonal pasientjournaløsning for hele helsesektoren, vil valg av datamodell og standarder være helt avgjørende for hvordan strukturen for registrering av tilganger gjennom personverntjenesten bør implementeres. Dette vil igjen ha en konsekvens for NSI prosjektet som er ansvarlig for å se på etablering av selve autorisasjonsløsningen på nasjonalt plan.

3.8 Sikkerhetsarkitektur og infrastruktur

Her skal det beskrives noe rundt bruk av STS for sikker autentisering i forhold til innloggede innbyggere hos aktører i sektoren gjennom en federeringstjeneste STS hos helsenorge.no.

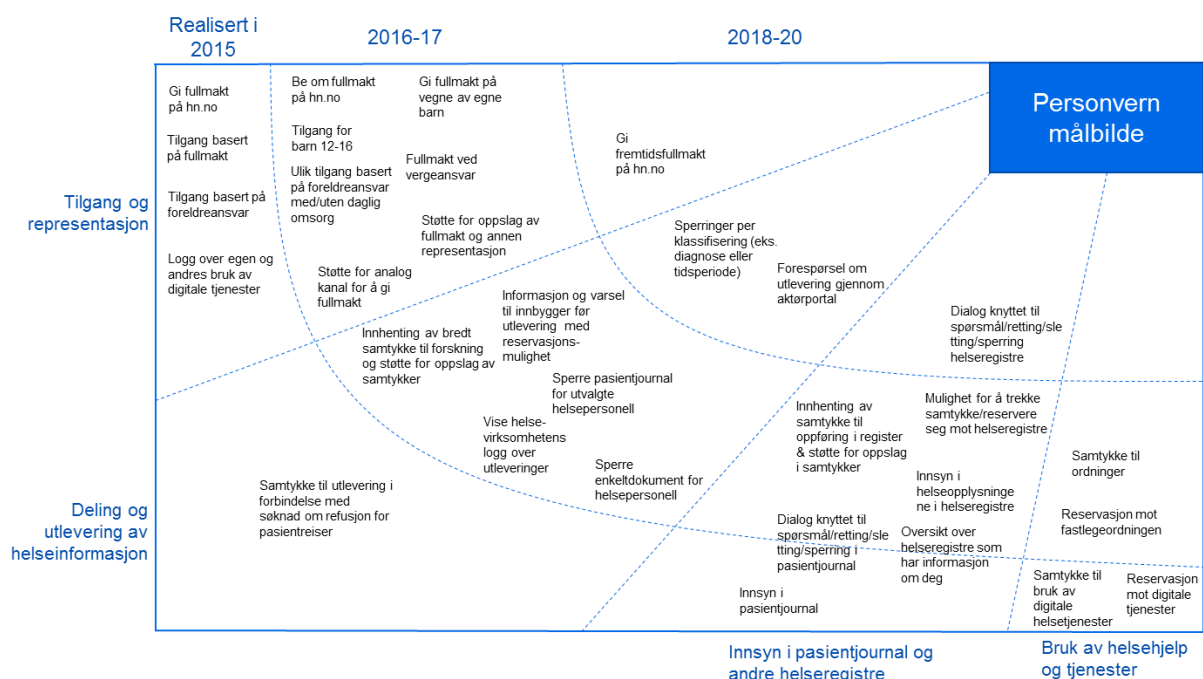
4 VEIKART FOR GJENNOMFØRING

4.1 Veikart

Figur 33 viser et forslag til veikart for realisering av personvernfunksjonalitet på helsenorge.no, og Tabell 7 gir en tilhørende beskrivelse av de ulike elementene. Plasseringen av funksjonaliteten i tid er gjort basert på analysen i kapittel 4.2, i tillegg til en vurdering av hva som er hensiktsmessig i forhold til etablerte prosjekter og forespørsler fra de ulike aktørene i sektoren.

Et viktig aspekt ved veikartet er at det viser når en funksjonalitet er tilgjengelig på helsenorge.no, men ikke omfanget av tjenesten. For eksempel har man i 2015 etablert funksjonalitet som støtter «innsyn i pasientjournal», men per januar 2015 er det bare pasientjournal fra sykehus i helse nord som er gjort tilgjengelig fra sektoren. Det planlegges for å knytte inn helse vest og helse sør-øst i 2016, men det er per i dag ikke planer for når/om man vil gjøre pasientjournal fra fastlege eller kommunehelsetjeneste kan gjøres tilgjengelig.

Det kanskje viktigste aspektet ved veikartet er at realiseringen av veikartet avhenger av beslutninger, budsjetter og prioritering i sektoren. Det kan bare realiseres i samarbeid med de ulike aktørene.



Figur 33: Veikart for personvernfunksjonalitet

Tabell 44: Beskrivelse av funksjonalitet i veikart for personvernfunksjonalitet.

| Funksjonalitet | Hva og hvordan? | Når? |
|--|--|------|
| Tilgang og representasjon | | |
| Gi fullmakt på hn.no | Funksjonalitet for å kunne gi fullmakt til enkelte tjenester på helsenorge.no. Funksjonaliteten ble implementert for Vestlandspasienten til september 2015. Løsningen skal utvides til å støtte flere tjenester. | 2015 |
| Tilgang basert på fullmakt | Funksjonalitet for at innbyggeren skal kunne få tilgang til en annen innbyggers tjenester på helsenorge.no ved bruk av fullmakt. | 2015 |
| Tilgang basert på foreldreansvar | Funksjonalitet for at en innbygger skal kunne få tilgang til sine barns tjenester på helsenorge.no. Tiltak: <ul style="list-style-type: none"> • Kvalitetssikre datakvaliteten for foreldreansvar i DSF i forhold til om den blir oppdatert dersom foresatte mister foreldreansvaret for barnet. | 2015 |
| Logg over egen og andres bruk av digitale tjenester | En overordnet logg som viser egen og andres bruk av innbyggerens tjenester på helsenorge.no. Logg over andres bruk av innbyggerens tjenester ble levert til september 2015. Utvidet støtte for logg over egen bruk blir levert til november 2015. | 2015 |
| Be om fullmakt på hn.no | Videreutvikle funksjonalitet for fullmakt på helsenorge.no ved å legge til funksjonalitet for å be om, akseptere og avslå fullmakter, samt varsling. | 2016 |
| Gi fullmakt på vegne av egne barn. | Gi fullmakt på vegne av egne barn for tilgang til tjenester på helsenorge.no. Spesielt relevant ved delt omsorg. | 2016 |
| Tilgang for barn 12-16 | Funksjonalitet for at barn 12-16 år skal få begrenset tilgang til tjenester på helsenorge.no. | 2016 |
| Ulik tilgang i forhold til foreldreansvar med/uten daglig omsorg | Funksjonalitet for å muliggjøre begrenset handlingsmulighet for tjenester som krever daglig omsorg. Tiltak: <ul style="list-style-type: none"> • Identifisere omfanget av foreldre med daglig omsorg ved bostedsadresse • Gi foreldre med daglig omsorg mulighet til å opprette fullmakt slik at andre kan opptre på vegne av barnet, da særlig tilknyttet tilfeller med delt omsorg hvor kun én av | 2016 |

| foreldrene vil fanges opp ved hjelp av bostedsadresse | | |
|--|--|------|
| Støtte for analog kanal for å gi fullmakt | Etablere en analog kanal gjennom 800HELSEder innbyggeren kan sende inn et manuelt skjema for å endre personverninnstillinger. Tiltak: <ul style="list-style-type: none"> Inngå samarbeid med 800HELSE og ny avdeling for Produksjon & Tjenesteoppfølging for å få etablert arbeidsprosesser, skjema og saksbehandlingsgrensesnitt for registrering av fullmakter og aktivering av fremtidsfullmakter. | 2016 |
| Fullmakt ved vergeansvar | Funksjonalitet for at verger kan få tilgang til en annen innbyggers tjenester gjennom fullmakt på helsenorge.no. Omfanget av fullmakten må gis av fylkesmannen. Tiltak: <ul style="list-style-type: none"> Gå i dialog med Fylkesmannen i Oslo og Akershus for å utarbeide prosess for å kunne definere og registrere omfanget av fullmakt for vergemålet. Utvidelse med fullmaktstype på helsenorge.no | 2016 |
| Støtte oppslag av fullmakt og annen representasjon | Funksjonalitet for å muliggjøre oppslag av fullmakt og annen representasjon for eksterne aktører Tiltak: <ul style="list-style-type: none"> Kjøre pilot med apotekene for fullmakt til utlevering av legemidler Inngå dialog med spesialisthelsetjenesten for oppslag i representasjonsforhold | 2017 |
| Gi fremtidsfullmakt på hn.no | Funksjonalitet for at en innbygger skal kunne gi en fremtidsfullmakt gjennom helsenorge.no. | 2018 |
| Deling og utlevering av helseopplysninger | | |
| Samtykke til utlevering i forbindelse med refusjon pasientreiser | Funksjonalitet for at innbyggeren skal kunne samtykke til at det innhentes informasjon om innbyggern i forbindelse med søknad om refusjon av utgifter i forbindelse med pasientreiser. Denne funksjonaliteten blir levert til november 2015, men lanseres først i 2016. | 2015 |
| Sperre enkeltdokumenter for helsepersonell | Funksjonalitet for at innbyggeren skal kunne sperre enkeltdokumenter mot innsyn fra helsepersonell. | 2016 |
| Vise helsevirksomhetens | Funksjonalitet for å gi innbyggeren en oversikt over hvilke helseopplysninger som er blitt utlevert fra en helsevirksomhet til | 2016 |

| | | |
|--|--|------|
| logg over utleveringer | andre aktører | |
| | Tiltak: | |
| | <ul style="list-style-type: none"> • Hente informasjon om utlevering av helseopplysninger fra UNN • Hente informasjon om utlevering av helseopplysninger fra andre helsevirksomheter | |
| Innhenting av bredt samtykke til forskning og støtte for oppslag | Funksjonalitet for at innbyggeren skal kunne gi et bredt samtykke til at helseopplysninger innefor et behandlingsløp eller område kan benyttes til forskningsformål. | 2017 |
| | Tiltak: | |
| | <ul style="list-style-type: none"> • Utvikle funksjonalitet for å håndtere forespørsel om samtykke til utlevering • Pilot med OUS om utlevering av helseopplysninger i forbindelse med forskningsprosjekter | |
| Sperre pasientjournal for utvalgte helespersonell | Funksjonalitet for at innbygger kan sperre den enkelte pasientjournal mot utvalgte helsepersonell | 2017 |
| | Tiltak: | |
| | <ul style="list-style-type: none"> • Utvikle funksjonalitet for sperring av helsepersonell • Pilot med Sykehuspartner for sperring av helsepersonell i Helse Sør-Øst • Utvide med andre helsevirksomheter | |
| Varsle innbyggeren om utlevering med reservasjonsmulighet | Funksjonalitet for at innbyggeren skal kunne få et varsel om utlevering av helseopplysninger og muligheten for å reservere seg. | 2017 |
| | Tiltak: | |
| | <ul style="list-style-type: none"> • Utvikle funksjonalitet for å håndtere reservasjon mot utlevering • Pilot med OUS om utlevering av helseopplysninger i forbindelse med forskningsprosjekter | |
| Sperre per dokumenttype (Eks: Diagnose eller tidsperiode) | Funksjonalitet for at innbyggeren skal kunne sperre all helseinformasjon relatert til en dokumenttype/klassifisering. Dette kan eksempelvis være for en diagnose eller tidsperiode. | 2018 |
| | Tiltak: | |
| | <ul style="list-style-type: none"> • Samarbeide med Helse regionene om å bedre kvalitet på | |

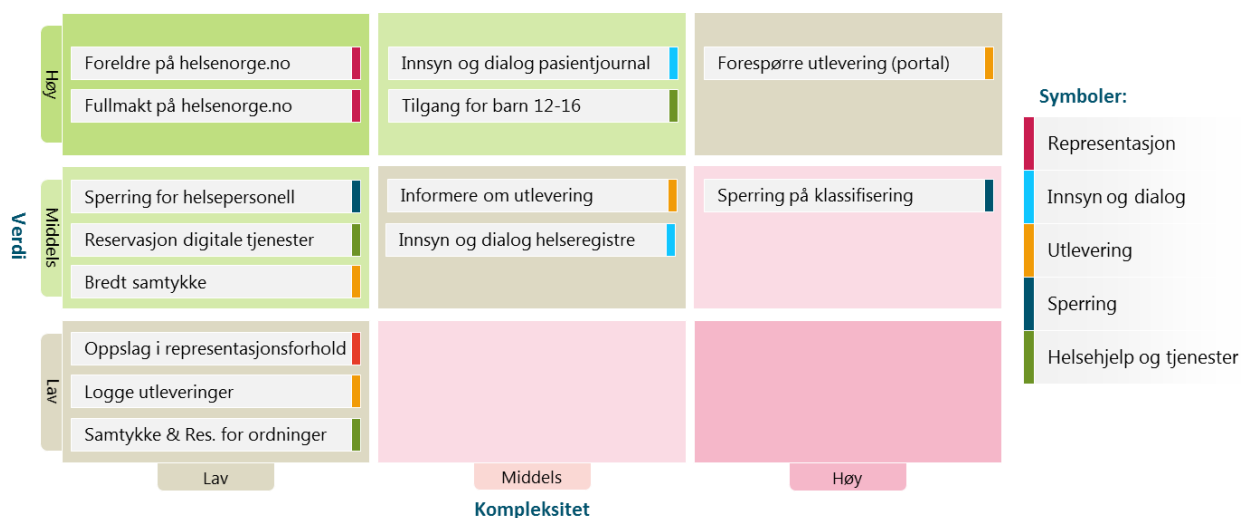
| | | |
|---|---|------|
| | <p>diagnoseklassifisering av helseopplysninger.</p> <ul style="list-style-type: none"> • Utvikle funksjonalitet for sperring på klassifisering, i første omgang på tidsperiode, i framtiden på diagnose. | |
| Forespørsel om utlevering gjennom en aktørportal | Funksjonalitet for at aktører skal kunne forespør og få innsyn i innbyggerens helseopplysninger gjennom en aktørportal. Dette vil muliggjøre innsyn uten utlevering (dupplisering) av helseopplysningene. | 2019 |
| Innsyn i pasientjournal og andre helseregister | | |
| Innsyn i pasientjournal | <p>Funksjonalitet for at innbygger skal få innsyn i sin pasientjournal. Denne funksjonaliteten ble levert til september 2015 for innsyn i journal hos Helse Nord.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Fortsette arbeidet med innsynsfunksjonalitet mot UNN • Fortsette arbeid med å etablere innsynsfunksjonalitet for andre helsevirksomheter. | 2015 |
| Dialog knyttet til retting/sletting og sperring av innhold i pasientjournal | <p>Funksjonalitet for at innbyggeren skal kunne føre en dialog med behandler for å kunne få rettet, slettet eller sperret innhold i sin pasientjournal.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Fortsette arbeid med dialogfunksjonalitet for innsynstjenesten mot UNN, inkludert prosesser for å rette, slette og sperre helseopplysninger • Fortsette arbeid med dialogfunksjonalitet for innsynstjenester mot andre helsevirksomheter. | 2016 |
| Oversikt over helseregister som har informasjon om deg | <p>Funksjonalitet der innbygger kan få oversikt over hvilke helseregister han/hun er oppført.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Utvikle funksjonalitet for å vise oversikt over registre • Hente informasjon om registre som innbygger er oppført i fra FHI, SKDE og HSØ | 2016 |
| Innsyn i helseregistre | <p>Funksjonalitet for at innbyggeren skal kunne få innsyn i helseregistre.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Utvikle funksjonalitet for innsyn i helseregistre | 2016 |

| | | |
|--|---|------|
| | <ul style="list-style-type: none"> • Integrere mot helseregistre til FHI, SKDE og HSØ, med pilot på følgende helseregister : <ul style="list-style-type: none"> ○ KRG: Kreftregisteret (HSØ) ○ MFR: Medisinsk fødselsregister (FHI) ○ SYSVAK: Nasjonalt vaksinasjonsregister (FHI) ○ Utvalgte nasjonale medisinske kvalitetsregister (SKDE) | |
| Innhenting av samtykke til oppføring i helseregistre & støtte for oppslag av samtykket | <p>Funksjonalitet for at innbygger skal kunne samtykke til oppføring i helseregistre på helsenorge.no.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Utvikle funksjonalitet for samtykke/reservasjon for helseregistre • Integrere mot helseregistre til FHI, SKDE og HSØ. | 2017 |
| Muligheten for å trekke samtykke/reservere seg mot helseregistre | <p>Funksjonalitet for at innbyggeren skal kunne trekke et samtykke eller reservere seg mot helseregistre.</p> <p>Tiltak: Se punktet over.</p> | 2017 |
| Dialog knyttet til spørsmål, retting, sletting og sperring for helseregistre | <p>Funksjonalitet for at innbygger skal kunne føre en dialog med registreier for generelle spørsmål, eller forespørsel om retting, sletting eller sperring av innhold.</p> <ul style="list-style-type: none"> • Utvikle dialogfunksjonalitet for helseregistre • Integrere mot helseregistre til FHI, SKDE og HSØ. | 2018 |
| Bruk av helsehjelp og tjenester | | |
| Samtykke til bruk av digitale tjenester | <p>Funksjonalitet for at innbyggeren skal kunne samtykke til bruk av digitale tjenester på nett. Funksjonalitet for samtykke til bruksvilkår og samtykke til bruk av personlig helsearkiv ble levert på helsenorge.no til henholdsvis februar og september 2015.</p> | 2015 |
| Reservasjon mot digitale tjenester | <p>Funksjonalitet for at innbyggeren skal kunne reservere seg mot å ha digitale tjenester på nett. Denne funksjonaliteten ble levert for innsyn pasientjournal på helsenorge.no til september 2015.</p> | 2015 |
| Reservasjon mot Fastlegeordningen | <p>Funksjonalitet for at innbyggeren skal kunne reservere seg mot fastlegeordningen på nett.</p> <p>Tiltak:</p> <ul style="list-style-type: none"> • Fortsette arbeidet med prosjektet for Bytt Fastlege for å få | 2016 |

| | | |
|--|--|------|
| støtte for å kunne reservere seg mot fastlegeordningen på helsenorge.no. | | |
| Samtykke til ordninger | Funksjonalitet for at innbyggeren skal kunne samtykke til ordninger på nett. | 2017 |

4.2 Evaluering av effektoppnåelse og kompleksitet

For å danne et bedre underlag i forhold til å kunne prioritere hvilken funksjonalitet som bør prioriteres i målbildet er effekten (verdi) av å realisere de ulike funksjonelle komponentene blitt evaluert opp mot effektmålene sikrere, enklere og mer effektiv som beskrevet under kapittel 1.2. Evalueringen er gjort ved å evaluere hvert av effektmålene basert på en skala fra -2 til +2. Verdien utgjør deretter summen av de 3 effektmålene med lik fordeling. Skalaen er deretter blitt normalisert til å passe innenfor de 3 områdene Lav, Middels, og Høy. Tilsvarende er det gjort en enkel evaluering av kompleksiteten for realisering basert på en skala fra 1-5. For å forenkle figuren er resultatet også her blitt presentert innfor områdene Lav, Middels og Høy. Evalueringen er gjort basert på innspill innhentet under intervju med de ulike aktørene, i tillegg til erfaringstall basert på tidligere implementasjon på helsenorge.no. En oppsummering av resultatet er gitt i Figur 34. Ytterligere detaljer for analysen er gitt i vedlegg 4.



Figur 34: Evaluering av effektoppnåelse og kompleksitet for realisering.

Som det fremgår fra figuren er det å tilby representasjon i form av foreldreansvar og fullmakt for tjenester på helsenorge.no noe som gir høy verdi og samtidig har relativ lav kompleksitet i forhold til realisering. Dette er derfor områder som bør prioriteres høyt i målbildet. Derimot vil eksempelvis funksjonalitet for sperring på klassifiseringsnivå være noe som kun gir middels verdi sett i lys av annen personvernfunksjonalitet og samtidig er komplekst å realisere. Denne funksjonaliteten anses derfor som å ha lavere prioritet på kort sikt. Det skal dog merkes at det

kan være andre utenforstående forutsetninger som eksempelvis lovpålagte krav eller tilsvarende som vil kunne endre denne prioriteringen.

