Direktoratet for e-helse

Utkast til innspill – v0.8

Veileder for åpne API i helse- og omsorgssektoren

HITR 1229 utkast 2019

Publikasjonens tittel:
Veileder for åpne API i helse- og omsorgssektoren

Rapportnummer:
HITR 1229 utkast 2019

Utgitt:
18.11.2019

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

Leseveiledning:

Om innspillsrunden

Dette dokumentet inneholder et utkast til en veileder for åpne API. Dokumentet skal ikke anses for ferdig, men som et innspill i en diskusjon rundt deling av data gjennom API.

Direktoratet for e-helse ønsker tilbakemelding fra aktører i helse- og omsorgssektoren på dokumentet.

Direktoratet ønsker tilbakemeldinger på alle aspekter ved dokumentet, inkludert hvert enkelt punkt i 2.1 og 2.2. Direktoratet ønsker også tilbakemelding på om veilederen bør stille krav innen flere områder. Innspill kan ta utgangspunkt i tabellene i 2.1 og 2.2, men kan også struktureres på en annen måte hvis dette er mest praktisk.

Innspill til dokumentet sendes innen 2. mars 2020 til postmottak@ehelse.no med referanse til sak 19/1004. En oppsummering av innspillene vil bli publisert når innspillsrunden er ferdig. Beslutning om videre prosess vil bli tatt etter innspillsrunden

Om dokumentet

Formålet med dokumentet er å definere hva begrepet åpne API skal bety innen helse- og omsorg og beskrive de viktigste kravene som bør stilles til aktører som tilbyr åpne API. Dokumentet retter seg primært mot noen grunnleggende forretningsmessige (organisatoriske) aspekter ved åpne API, men beskriver også noen av de mest grunnleggende juridiske aspektene ved området. Tekniske og semantiske problemstillinger er planlagt beskrevet i andre veiledere som for eksempel "Anbefaling om bruk av HL7 FHIR for datadeling".

Dokumentet er inspirert av arbeid fra andre land, som for eksempel "21st Century Cures Act" og tilhørende arbeid i USA, samt "Open API Policy" fra NHS England.

Direktoratet for e-helse utarbeider forskjellige typer normerende dokumenter som har ulikt normeringsnivå. Dette dokumentet er tenkt som en veileder, som er det laveste normeringsnivået[1]. Dette betyr at innholdet skal anses som råd innen spesifikke områder basert på beste praksis fra flere virksomheter. En slik veileder dekker ikke alle scenarier og kan avvikes av forskjellige årsaker. Slike veiledere kan likevel brukes som absolutte krav fra aktører som mener dette er hensiktsmessig, for eksempel i en anskaffelsesprosess. På sikt kan dokumentet også videreutvikles til et høyere normeringsnivå. Veilederen er skrevet for helse- og omsorgsektoren, men flere av kravene er generiske og kan gjelde for flere sektorer.

[1] https://ehelse.no/standarder/normeringsniva-og-dokumenttyper

1 Hvordan kan åpne API bidra tilbedre helse?

Den norske helse- og omsorgstjenesten er fragmentert og kompleks. Pasientforløpene flyter gjerne frem og tilbake, mellom ulike institusjoner og forvaltningsnivåer. Pasienter og helsepersonell er derfor helt avhengige av at informasjon deles mellom virksomheter og systemer. Deling av informasjon om diagnose, medikamenter og behandlingsforløp er grunnleggende for pasientsikkerheten og effektiv behandling.

Innenfor rammene av taushetsplikten skal virksomheter som yter helsehjelp dele relevant og nødvendig helseinformasjon med annet helsepersonell med tjenstlig behov uavhengig av hvor de jobber. Dette gjøres i dag på mange måter; telefon, faks og elektronisk meldingsutveksling. Meldingsutveksling fungerer i dag godt i planlagte pasientforløp der det er få aktører som samarbeider. Men meldingsutvekslingen dekker ikke alle behov for samhandling godt nok, og ytterligere datadeling er derfor påkrevet. Datadelingen er en samhandlingsform som er basert på deling av og samarbeid om strukturerte data som helseaktører og leverandører av e-helseløsninger kan benytte seg av ved utvikling av nye tjenester. I realisering av datadeling er bruk av API sentralt. API er programmeringsgrensesnitt som systemer bruker til å kommunisere og dele informasjon.

Nasjonal e-helsestrategi[2] er helse- og omsorgssektorens felles strategi for IKT og digitalisering. Strategien angir målene for IKT og digitalisering i sektoren og hvordan disse bidrar til å realisere overordnede helse- og omsorgspolitiske mål. Åpne API er et av mange virkemidler for å oppnå målene. En økt satsning på datadeling også et område som er omtalt i "Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten"[3].

Internasjonalt sliter mange land med barrierer mot datadeling i helsesektoren, og de innfører derfor tiltak for å tilrettelegge for mer åpenhet. I USA er det for eksempel innført lover for åpning av helseinformasjonssystemer og forbud mot "information blocking"[4]. England har i mange år hatt retningslinjer for åpne API innen helse[5]. Betalingstjenestedirektivet[6] er et eksempel på et europeisk tiltak i en annen sektor som også har sett utfordringer med lukkede systemer. Tilgang på åpne API er et viktig virkemiddel for å økt innovasjon, økt innbyggermedvirkning og økt samhandling mellom helsepersonell.

1.1 Hensikt

Erfaringen viser at det er betydelige barrierer mot datadeling i helsesektoren i dag. Leverandører av e-helseløsninger beskytter sine interesser gjennom konfidensialitetsavtaler eller andre begrensende vilkår og har lisensmodeller som ikke er tilpasset nye samhandlingsformer. Mange virksomheter og leverandører av e-helseløsninger er usikre på hvordan de skal håndtere sikkerhet og personvern når de deler på tvers og er derfor

[2] https://ehelse.no/aktuelt/oppdatert-nasjonal-e-helsestrategi-og-ny-plan

[3] https://ehelse.no/publikasjoner/plan-for-utvikling-av-felles-grunnmur-for-digitale-tjenester-i-helse-og-omsorgstjenesten

[4] 21st Century Cures Act section 4004

[5] https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/interoperability/open-api/

[6] https://www.finansnorge.no/tema/bank/psd2-eller-betalingstjenestedirektivet/

restriktive på å gi tilgang. I tillegg er kostnader og insentiver for å implementere delingsløsninger skjevt fordelt mellom den som har for behov for tilgang og den som har informasjon som skal deles.

Som et av flere tiltak for å senke barrierer mot datadeling har Direktoratet for e-helse etablert "Veileder for åpne API". Mange av barrierene mot datadeling gjelder for mange bransjer og sektorer, men en del av kravene og barrierene som gjelder informasjonssikkerhet og personvern er spesifikke for helse- og omsorgstjenesten.

For å belyse at samhandlingsutfordringer trenger brede tiltak som dekker juridisk, organisatorisk, semantiske og tekniske problemstillinger har EU utarbeidet "European Interoperability Framework" og DIFI har oversatt dette rammeverket til norsk[7].

Figur 1 viser DIFIs oversettelse av European Interoperability Framework. Denne veilederen adresserer overordnet juridisk og organisatorisk samhandlingsevne, men er heller ikke utfyllende på disse områdene. Veilederen dekker kun delvis semantisk og teknisk samhandlingsevne.

Etterlevelse av denne veilederen vil bidra til en felles forståelse av hva aktørene i helse- og omsorgstjenesten bør forvente av hverandre. Målet er å tilrettelegge for en kultur hvor det skal lønne seg å satse på åpenhet, og hvor lukkede systemer blir valgt bort. Veilederen retter seg primært mot klargjøring av organisatoriske områder som avtaler, dokumentasjonspraksis og forretningsmodell, samt noen juridiske problemstillinger om personvern og behandlingsformål for data og datadeling. Norm for informasjonssikkerhet i helse- og omsorgssektoren[8] har krav og veiledningsmateriale om informasjonssikkerhet og personvern som er relevant for åpne API. Veilederen retter seg i noe mindre grad mot semantiske og

[7] https://www.difi.no/arkitektur/nytt-nasjonalt-rammeverk-samhandling
[8] https://ehelse.no/normen

tekniske problemstillinger, der Direktoratet for e-helse har utarbeidet andre anbefalinger og veiledere.

Veileder for åpne API i helse- og omsorgssektoren skal:

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

1.2 Hva er åpne API?

Åpne API er gjenbrukbare, sikre, godt dokumenterte og tilgjengelige programmeringsgrensesnitt som kan benyttes av alle relevante aktører uten diskriminerende og konkurransevridende vilkår.

Åpne API må ikke forveksles med åpne data, da åpne API i helse- og omsorgssektoren også skal gi en sikker tilgang til sensitive opplysninger som er underlagt taushetsplikt til aktører som har tjenstlig behov for tilgang til relevante og nødvendige opplysninger.

Selv om API er åpent, krever både utlevering og innhenting av taushetsbelagte opplysninger selvstendig hjemmelsgrunnlag.

Åpne API betyr heller ikke at all informasjon skal være tilgjengelig for alle. Personvern og informasjonssikkerhet er også gjeldende for systemer som har åpne API, og det er viktig at den som har dataansvaret har mekanismer på plass som sørger for at sensitive opplysninger ikke kommer på avveie.

Åpne API og økt fokus på datadeling tar ikke vekk behovet for økt investering i kjernesystemer, men bør ses på som en forutsetning for at slike investeringer blir fremtidsrettede og fleksible for fremtidig endring og innovasjon. Fleksibiliteten som gis fra satsning på åpne API og plattformkonsepter kan også gjøre investeringer i kjernesystemer mer lønnsomme ettersom man åpner for økt gjenbruk av kjernesystemer.

1.3 Målgruppe for veilederen

- Målgrupper for dette dokumentet: Virksomheter som har systemer som det er aktuelt å tilgjengeliggjøre opplysninger fra
- Systemleverandører og utviklere
- Virksomheter som kan benytte seg av opplysninger som blir gjort tilgjengelig

Ansvaret for å tilby åpne API og tilrettelegge for åpenhet ligger både hos systemleverandøren og virksomhetene som har e-helseløsninger. Dokumentet er tenkt brukt av virksomheter som realiserer nye e-helseløsninger, nye API til eksisterende e-helseløsninger og grunnmurstjenester. Veilederen kan for eksempel benyttes i anskaffelser der det bør stilles krav om åpne API.

2 Veileder for åpne API

2.1 Krav til et åpent API

For at et API skal være definert som åpent skal/bør følgende krav følges:

Nr	Krav	Kommentar
1.	Det skal benyttes forståelige og rettferdige vilkår og betingelser som regulerer datadeling mellom virksomheter i helsesektoren. Vilkårene må være langsiktige, transparente og ikke-eksklusive. Det skal blant annet ikke gjøres forskjell på offentlige og private helseaktører.	
2.	Avtaler og bruksvilkår skal regulere alle parters immaterielle rettigheter (IPR) og være rettferdige slik at ingen aktører kan frata andre aktørers immaterielle rettigheter.	
3.	Det skal tilstrebes at åpne API er gratis å bruke. Når det er nødvendig å ta seg betalt for bruk av API, må kostnadens størrelse være rimelig og ikke-diskriminerende, og det bør også være en forståelig og forutsigbar prismodell.	Det kan være aktuelt å ta seg betalt for bruk av åpne API da dette kan være en måte å finansiere nye tjenester på eller erstatte brukerlisensiering.
4.	Eksistensen av et API skal være kjent og være publisert på et egnet sted.	På sikt bør dette være en felles API-katalog
5.	Ingen leverandører skal ta i bruk konkurransevridende metoder som på en diskriminerende måte motvirker eller reduserer tilgangen til åpne API for andre aktører og konkurrenter.	Mer arbeid gjenstår på dette punktet. ONC har for eksempel utarbeidet retningslinjer for hva de mener er legitime tiltak og ikke bør regnes som "Information blocking" (delingsmotstand). Noe tilsvarende kan gjøres for Norge.
6.	Tilgang til utvikling og testing av åpne API skal ikke være diskriminerende eller benyttes til å oppnå konkurransefordeler. Alle som ønsker å utvikle mot et åpent API må få tilgang til dette.	
7.	Det bør være mulig for konsumentene av API-ene å teste selv, og tilgang til slik egentesting bør være gratis.	Testing bør være mulig uten at leverandøren er involvert. Dersom brukerne ønsker å involvere leverandøren er

		det ikke gitt at testingen skal være gratis. *Burde det også være slik at for noen typer API så må tilgang til testmiljø være gratis?*
8.	Åpne API skal ha dokumentasjon som er åpent tilgjengelig på internett. Tilgang til dokumentasjonen må være gratis og ikke beskyttet av konfidensialitetsavtaler.	
9.	Dokumentasjon av API bør også tilbys i henhold til "OpenAPI Specification", "FHIR Capability Statement" eller et tilsvarende åpent og maskinlesbart format.	
10.	Dokumentasjonen skal være så komplett at en erfaren utvikler kan bruke API-et uten mer informasjon, og skal inneholde: a) Hvordan man bruker API-et, inkludert eksempelkode. b) Hvilke og hvordan feilsituasjoner håndteres c) Hvilke bruksområder API-et har. d) Hvilken funksjonalitet/ressurser som det tilbyr. e) Krav til identiteten til brukere og beskrivelse av tilgangsstyring. Må inneholde beskrivelse av sikkerhetsmekanismene som beskytter API-et. f) Beskrivelser av testmuligheter og bruk av testfasiliteter inkludert kontaktinformasjon. g) Tilgjengelighet til API-et, og hvordan planlagt vedlikehold gjennomføres h) Trafikkbegrensninger og forventet responstid på kall. i) Lisensiering og eventuelle kostnader knyttet til bruk av API-et i produksjon. j) Bruksvilkår på data mottatt fra API-et. Må inkludere krav og vilkår for sikkerhet, lagring, behandling, videreformidling og sletting. k) Forventet stabilitet, langsiktighet og levetid for API-et og lagrede data inkludert hvordan endringer og versjonering av API-et håndteres.	*Bør noen av disse legges under avtale eller vilkår istedenfor dokumentasjon? Eventuelt ha et lignende punkt med opplisting av innhold i avtale og vilkår.*
11.	Åpne API bør være basert på åpne, internasjonale standarder og spesifikasjoner der dette er mulig.	*Til diskusjon.*
12.	Systemer bør eksponere vesentlig forretningsfunksjonalitet og data gjennom åpne API.	*Til diskusjon.*

Tabell 1 krav til åpne API

2.2 Rammebetingelser for behandling og deling av personopplysninger

Norm for informasjonssikkerhet i helse- og omsorgssektoren gir detaljert veiledning, praktiske eksempler og informasjon som også er relevant for åpne API. Tabellen nedenfor er ikke uttømmende, men gir en oversikt over de noen av de mest grunnleggende rammebetingelsene for behandling – herunder deling – av personopplysninger (for definisjoner, se personvernforordningen artikkel 4):

	Behandling av personopplysninger i åpne API-er
1.	Informasjonen det gis tilgang til gjennom API-et bør på forhånd klassifiseres og vurderes. Det er forskjellige krav til deling av åpne data, personopplysninger og personopplysninger av særlige kategorier (som for eksempel helseopplysninger). Dersom opplysningene som tilgjengeliggjøres er personopplysninger gjelder de øvrige kravene i tabellen her. Behandlingsprotokoll – som dataansvarlig er pålagt å ha - er et godt verktøy for å vurdere hvilke personopplysninger som kan deles med hvilke typer API. Se tabell 2 punkt 9.
2.	**Behandlingsgrunnlag** **Personvernforordningen** Behandling av personopplysninger krever **behandlingsgrunnlag** – hjemmel i lov eller samtykke, jf. personvernforordningen artikkel 6. Det er ikke adgang til å tilegne seg eller utlevere opplysninger fra/til en annen virksomhet gjennom et API uten at det foreligger et gyldig behandlingsgrunnlag. **Spesielt for helse- og omsorgssektoren** Pasientjournalloven § 19, ref. helsepersonelloven §§ 45 og 25 gir dataansvarlig plikt til å dele relevant og nødvendig informasjon uten hinder av taushetsplikten for den som har tjenstlig behov for å yte, administrere eller kvalitetssikre helsehjelp med mindre pasienten har motsatt seg dette (se pkt. 3). For andre formål enn helsehjelp, kreves eksplisitt samtykke fra pasient eller annen hjemmel i lov, jf. pasientjournalloven § 20.
3.	**Sperringer** Taushetsplikten trer inn der den registrerte har motsatt seg at opplysninger om ham utleveres. Dette er sperrer som er satt lokalt i systemene til dataansvarlige virksomhet. API må ha funksjonalitet for å sjekke om det foreligger sperrer som hindrer utlevering til tross for at det finnes et behandlingsgrunnlag, ref. pkt. 2 over. Eventuelt må datasettet som tilgjengeliggjøres ikke inneholde opplysninger noen har motsatt seg at kan utleveres. **Spesielt for helse- og omsorgssektoren**

	Pasientjournalloven § 17 gir pasienten rett til å motsette seg at helseopplysninger gjøres tilgjengelig for helsepersonell. Det er dataansvarlige virksomhet som definerer nivå for disse sperrene, og de kan settes på rolle, virksomhet, avdeling mv i tillegg til enkeltperson. I tillegg kan sperren gjelde hele eller deler av et dokument, eller kun opplysninger i et dokument. Manglende struktur i pasientjournal fører til at mange dokumenter må gjøres helt utilgjengelige for digitale søk selv om det kun er enkelte opplysninger som skal unntas.
4.	**Dataminimering** **Personvernforordningen** En virksomhet skal ikke samle inn flere personopplysninger enn det som er nødvendig for å oppnå formålet med behandlingen av opplysningene. Dette følger av artikkel 5 1. c). Dersom en virksomhet skal gjøre tilgjengelig opplysninger via API må API-et eller API-ene settes opp slik at det ikke gis tilgang til unødvendige opplysninger, ved å dele opp datasettene og bruke mekanismer for å styre hva det gis tilgang til. **Spesielt for helse- og omsorgssektoren** Dersom formålet med deling av opplysninger er pasientjournalloven § 19 (se punkt 2) vil det kunne være nødvendig å tilgjengeliggjøre flere opplysninger enn det som er nødvendig for å yte helsehjelp – nettopp for å kunne avgjøre hvilke opplysninger som er nødvendige. Da er det viktig at mottagervirksomheten har gode rutiner for sletting av opplysninger.
5.	**Lagringsbegrensning** **Personvernforordningen** Personopplysninger skal ikke lagres lengre enn nødvendig for å oppnå formålet med behandlingen av opplysningene. Dette følger av artikkel 5 1. e). Virksomheter som aksesserer opplysninger gjennom et API må vurdere om det er grunnlag for å lagre (en egen kopi av) opplysningene. **Spesielt for helse- og omsorgssektoren** Pasientjournal skal bare inneholde det som er relevant og nødvendig i den aktuelle behandlingssituasjonen, jfr. Pasientjournalforskriften § 6. Det betyr at man gjennom API-et bør kunne trekke ut bare disse nødvendige opplysningene, istedenfor å lagre kopier av hele datasett.
6.	**Internkontroll** **Personvernforordningen** For å kunne kontrollere at personopplysninger blir behandlet riktig er det nødvendig å ha oversikt over *hvem* som har tilgang til hvilke opplysninger, jf. personvernforordningen artikkel 24. Dette er nødvendig for å kunne føre etterkontroll og tilfredsstille den registrertes rettigheter

	Spesielt for helse- og omsorgssektoren Virksomheten som ønsker tilgang til opplysningene må dokumentere oppslag på innbyggere for å kunne avdekke forsøk på uautorisert tilegnelse av taushetsbelagte opplysninger, jfr. helsepersonelloven § 21 a. Virksomheten som skal gi fra seg opplysninger skal ha oversikt over hvem som har tilgang til hvilke typer opplysninger og kunne kontrollere i ettertid hvem som har benyttet seg av tilgangen. Dette følger av pasientjournalforskriften § 13.
7.	**Databehandleravtale** **Personvernforordningen** Dersom den virksomhet personopplysninger deles med behandler personopplysningene på vegne av den dataansvarlige, kreves det at man på forhånd inngår en databehandleravtale. Dette følger av artikkel 28. **Spesielt for helse-og omsorgssektoren** I helsesektoren deles opplysninger som regel på tvers av virksomheter som på hver sin side er dataansvarlige for opplysninger som er relevante og nødvendige å nedtegne i journalen.
8.	**Protokoll** Enhver virksomhet som behandler personopplysninger skal holde en protokoll over behandlingsaktiviteter, jf. personvernforordningen artikkel 30. Protokoll er pålagt, og kan være til stor hjelp under planleggingen av deling av opplysninger som ikke er gjenstand for manuell behandling

Tabell 2 Grunnleggende rammebetingelser for behandling og deling av personopplysninger

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no