Direktoratet for e-helse

Veileder for åpne API i helse- og omsorgssektoren

Versjon 1.0

Merknad 10.12.2024:
Denne rapporten ble utgitt av
Direktoratet for e-helse

HITR 1229:2020

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

Rapportnummer:
HITR 1229:2020

Utgitt:
05/2020

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
www.ehelse.no

Innholdsfortegnelse

1 Hvordan kan åpne API bidra til bedre helse?

1.1 Økt fokus på datadeling

Den norske helse- og omsorgstjenesten er fragmentert og kompleks. Pasientene behandles i ulike institusjoner og behandlingen dokumenteres i mange ulike fagsystemer. Pasienter og helsepersonell er derfor helt avhengige av at virksomhetene og systemene samhandler og deler helseopplysninger for å yte god helsehjelp. Deling av informasjon om diagnose, medikamenter og behandlingsforløp er grunnleggende for pasientsikkerheten og effektiv behandling.

Virksomheter og helsepersonell som yter helsehjelp skal innenfor rammene av taushetsplikten samhandle og dele relevant og nødvendig helseinformasjon med annet helsepersonell med tjenstlig behov uavhengig av hvor de jobber. Samhandling kan i dag skje på mange ulike måter, for eksempel gjennom telefon, møter, brev, faks og elektronisk meldingsutveksling. Meldingsutveksling fungerer i dag godt i planlagte pasientforløp der det er få aktører som samarbeider. Men meldingsutvekslingen dekker ikke dagens behov for samhandling godt nok. Det er behov for å legge til rette for samhandling via datadeling. Datadelingen er en samhandlingsform som er basert på deling av og samarbeid om strukturerte data som helseaktører og leverandører av e-helseløsninger kan benytte for å dekke helsepersonell sine samhandlingsbehov.

Nasjonal e-helsestrategi[1] 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. En økt satsning på datadeling er et område som er omtalt i "Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten"[2]. For å få nå de helsepolitiske målene som er angitt i nasjonal e-helsestrategi og plan for felles grunnmur så må det gjennomføres tiltak på flere nivåer, og åpne API er et av mange virkemidler.

1.2 Hva er åpne API?

Sentralt i samhandling med datadeling er bruk av API. Begrepet API betegner et grensesnitt i en programvare hvor spesifikke deler av denne kan aktiveres (kjøres) fra en annen programvare gjennom kall til grensesnittet. I dette dokumentet er API brukt i en kontekst hvor en virksomhet tilgjengeliggjør et grensesnitt i en programvare som andre kan aktivere. Dagens praksis er å tilby API ved hjelp av webteknologi som benytter protokollen http. Vi definerer begrepet *åpne API* som følger:

[1] Nasjonal e-helsestrategi og handlingsplan 2017-2022, Direktoratet for e-helse, 2019
[2] Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten, Direktoratet for e-helse, 2019

Åpne API i helse og omsorgssektoren 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[3] hvor data er åpent tilgjengelig for alle. Åpne API i helse- og omsorgssektoren vil muliggjøre sikker tilgang til sensitiv informasjon for aktører som har tjenstlig behov for tilgang til relevant informasjon. Selv om API er åpent, krever både utlevering og innhenting av taushetsbelagte opplysninger selvstendig hjemmelsgrunnlag.

Åpne API betyr ikke at selve grensesnittet er åpent for tilgang, men at spesifikasjonene for grensesnittet er tilgjengelige for flere – dvs. at de er åpne i betydningen ikke hemmelige eller diskriminerende. Personvern og informasjonssikkerhet er fortsatt 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.

Det er krevende å etablere datadeling som en standardisert samhandlingsform i i helsesektoren. Denne veilederen er bare én brikke i en større helhet for å få til dette. På sikt bør det etableres en felles strategi for datadeling som må inkludere mange tiltak på forskjellige lag og hos forskjellige aktører. Åpne API og økt fokus på datadeling tar heller ikke vekk behovet for økt investering i fagsystemer og andre datadelingstiltak, 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 kan også gjøre investeringer i fagsystemer mer lønnsomme ettersom man åpner for økt gjenbruk av fagsystemer.

EU har definert et rammeverk for samhandling som definerer juridisk, organisatorisk, semantiske og tekniske samhandlingsevne, "European Interoperability Framework". DIFI har oversatt dette rammeverket til norsk[4].

[3] Veileder for tilgjengeliggjøring av åpne data, Digitaliseringsdirektoratet (tidl. Difi), 2018
[4] https://www.difi.no/arkitektur/nytt-nasjonalt-rammeverk-samhandling

Figur 1 viser DIFIs oversettelse av European Interoperability Framework.

Denne veilederen adresserer først og fremst barrierer mot datadeling knyttet til organisatorisk samhandlingsevne. I tillegg beskriver veilederen juridiske rammebetingelser for behandling og deling av helseopplysninger. Norm for informasjonssikkerhet i helse- og omsorgssektoren[5] har også mer utfyllende krav og veiledningsmateriale om informasjonssikkerhet og personvern som er relevant for åpne API.

Veilederen omhandler ikke standarder for API-er og datadeling. Bruk av internasjonale standarder for API er et viktig virkemiddel for å øke samhandling med datadeling. Det anbefales derfor til å benytte standarder ved utvikling av nye API der det er mulig. Direktoratet for e-helse har utarbeidet andre anbefalinger og veiledere som retter seg inn på disse områdene. Se www.ehelse.no for oversikt over publiserte dokumenter.

1.3 Hvorfor åpne API?

Erfaringer 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. Internasjonalt innfører flere land tiltak for å tilrettelegge for mer åpenhet. I USA er det for eksempel innført lover for åpning av helseinformasjonsystemer og forbud mot "information blocking"[6]. England har i mange år hatt retningslinjer for åpne API innen helse[7]. Betalingstjenestedirektivet[8] er et eksempel på et europeisk tiltak i en annen sektor som også har sett utfordringer med lukkede systemer.

[5] https://ehelse.no/normen

[6] 21st Century Cures Act section 4004, US Government, 2016

[7] Open API policy, NHS England, 2018

[8] PSD2 eller betalingstjenestedirektivet, Finans Norge, 2019

En annen barriere er at 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 restriktive på å gi tilgang.

Hensikten med å oppfordre til bruk av åpne API i norsk helse- og omsorgssektor er å skape en kultur blant helsetilbydere og systemleverandører hvor man tilrettelegger for mer åpenhet mellom disse aktørene. Det bør være et mål at åpne API er gratis å bruke for de konsumerende virksomhetene, men i en generell veiledning er det vanskelig å gi konkrete råd om hvilke API og hvilke data som må være gratis. Det er for eksempel naturlig at innbyggere får gratis tilgang til sine data, men det kan være bruksområder der det er naturlig at aktører betaler for data og ressurser som ligger bak API. De dataansvarlige har en plikt å dele helseopplysninger med samarbeidende personell i andre virksomheter. Tilgjengeliggjøring av helseopplysninger ved bruk av datadeling medfører mindre bruk av telefoner og fax, og frigjør dermed verdifull tid for helsepersonell.

Åpne API er et viktig virkemiddel for å oppnå gevinster som økt innovasjon, økt innbyggermedvirkning og økt samhandling mellom helsepersonell. Åpne API vil bidra til økt datadeling, som igjen vil bidra til at helsepersonell vil bruke mindre tid på å hente ut pasientinformasjon fra ulike kilder og gi høyere kvalitet på helsetjenestene. Helsesektoren har mye å spare ved å gjenbruke mer pasientinformasjon i arbeidsprosessene.

1.3.1 Formålet med veilederen

Som et av flere tiltak for å senke barrierer mot datadeling har Direktoratet for e-helse etablert "Veileder for åpne API" (dette dokumentet) som gir føringer og anbefalinger for hva som definerer API som åpent. Dette bidrar til at sektoren kan gjøre sine API åpne for andre, sette krav om åpne API ved bestillinger til sine leverandører og at leverandører kan markedsføre sine produkter med åpne API. Ved at det blir stilt krav om åpne API ved innkjøp av systemer vil noen av barrierene mot datadeling bli redusert.

Etterlevelse av denne veilederen vil føre til forretningsmessig åpenhet rundt datadeling og lettere dialog rundt datadeling mellom de ulike aktørene i helse- og omsorgstjenesten. Målet er å tilrettelegge for en kultur hvor det skal lønne seg å satse på åpenhet, og hvor lukkede systemer blir valgt bort.

Målet med veilederen er å definere åpne API gjennom et sett med felles krav. I tillegg skal den sikre kunnskap om relevante regelverkskrav for datadeling som del av rammebetingelsene for å tilby åpne API.

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 API dokumentasjon
4. Gi en oversikt over de mest grunnleggende rammebetingelsene for deling av personopplysninger

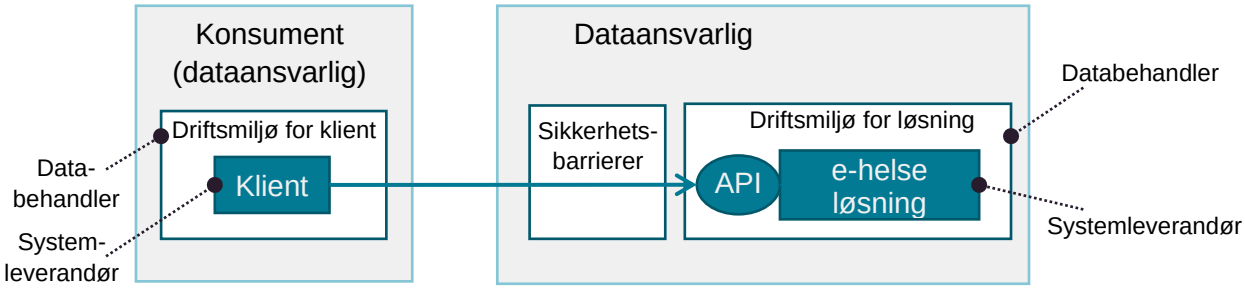
1.3.2 Aktører og målgruppe

Hovedmålgrupper for veilederen:

- Dataansvarlige og nasjonale aktører som har systemer som det er aktuelt å tilgjengeliggjøre helseopplysninger med bruk av datadeling
- Databehandlere, systemleverandører og utviklere som drifter, forvalter, utvikler og/eller selger API-baserte løsninger.
- Dataansvarlig, databehandlere og systemleverandører som drifter, forvalter, utvikler klienter som konsument av helseopplysninger ved bruk av datadeling

Figur 2 viser en forenklet skisse over komponenter og roller som kan inngå i bruk av API og som bli berørt av veilederen for åpne API. Det er den dataansvarlige som er ansvarlig for at tilgjengeliggjøring av sine API er basert på åpne API, men det kan være konsumentene som vil få den største gevinsten av åpne API. Konsumentene kan være andre virksomheter, innbyggere eller den dataansvarlige selv.

Ved etablering av nye e-helseløsninger som inkluderer åpne API, må den dataansvarlige velge databehandlere og/eller produktleverandører som følger kravene og retningslinjene for åpne API. Det at alle dataansvarlige stiller samme krav til åpne API vil medføre at leverandørmarkedet må følge etter og som en konsekvens danne en kultur for mer åpenhet rundt datadeling. Dette vil hjelpe til å sikre at forretningsmessige barrierer forsvinner.



Figur 2 Forenklet skisse som viser bruk av API og roller som kan inngå i bruk av API. Med sikkerhetsbarrierer menes her brannmur, API Gateway, tilgangsstyringssystem m.m. som regulerer tilgang til et API.

1.3.3 Bruksområder

Denne veilederen er skrevet generisk slik at kravene skal gjelde uavhengig av bruksområde. Eksempler på bruksområder for åpne API kan være:

- Deling av helseopplysninger mellom helseaktører. Her vil aktørene ofte både tilby og konsumere API-er.
- Deling av helseopplysninger fra en helseaktør til innbygger
- Utvikling av innovative apper for innbyggere
- Utvikling av innovative løsninger på en plattform
- Tilgjengeliggjøring av informasjon fra ett system til et annet innad i en virksomhet.

Aktører som benytter veilederen kan velge å sette *bør-krav* i veilederen som *skal-krav* i en konkret anskaffelse eller i et utviklingsprosjekt.

En viktig faktor for utvikling av digitale tjenester er å sørge for å tilby all vesentlig informasjon via åpne API-er, slik at all relevant pasientinformasjon enkelt kan deles til eksisterende og nye konsumenter.

Ved behov vil Direktoratet for e-helse komplettere denne veilederen med mer spesifikke veiledere for de ulike bruksområdene.

2 Krav til åpne API

Kravtabellen beskriver et sett med krav som definerer åpne API. *Skal*-krav må være oppfylt for å kalle et API for åpent og er angitt med O (Obligatorisk) i tabellen. *Bør*-krav som ikke er oppfylt vil ikke utelukke API-et som åpent, men utelatelse bør begrunnes godt. *Bør*-krav er angitt med A (Anbefalt) i tabellen.

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

Nr.	Krav	Type
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.	O
2.	Avtaler og bruksvilkår skal regulere alle parters immaterielle rettigheter (IPR) og være rettferdige slik at ingen aktører kan frata andre aktørers immaterielle rettigheter.	O
3.	Dataansvarlige bør tilby sine åpne API gratis til konsumentene. Når det anses nødvendig å ta seg betalt for bruk av åpne API, skal pris og vilkår være rimelige, transparente og ikke-diskriminerende. *Kommentar*: Det kan være aktuelt å ta seg betalt for bruk av åpne API innenfor noen bruksområder, for eksempel kan det være nødvendig for å finansiere nye tjenester og stimulere til innovasjon.	A
4.	Eksistensen av et API skal være kjent og publisert på et egnet sted. *Kommentar*: Målarkitektur for datadeling[9] beskriver at alle produksjonssatte API-er i helsesektoren bør registreres i Digitaliseringsdirektoratets felles API-katalog hvor det legges opp til mulighet for at det linkes til dertil egnede portaler hvor API-dokumentasjon er tilgjengelig.	O
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. *Kommentar*: ONC i USA har for eksempel utarbeidet retningslinjer[10] for hva de anser som legitime tiltak og ikke bør regnes som "Information blocking" (delingsmotstand). Tilsvarende arbeid med å utforme retningslinjer for legitime tiltak bør gjøres for Norge.	O

[9] Målarkitektur for nasjonal datadeling i helse- og omsorgssektoren, Direktoratet for e-helse, 2020
[10] Notice of Proposed Rulemaking to Improve the Interoperability of Health Information, The Office of the National Coordinator for Health Information Technology (ONC), 2020

Nr.	Krav	Type
6.	Tilgang til utvikling mot 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.	O
7.	Det bør være mulig for konsumentene av API-ene å teste bruk av API selv, og tilgang til slik egentesting bør være gratis. *Kommentar*: Testing bør være mulig uten at leverandøren er involvert. Dersom brukerne ønsker å involvere leverandøren er det ikke gitt at testingen skal være gratis.	A
8.	Åpne API skal ha dokumentasjon som er åpent tilgjengelig på internett. Tilgang til dokumentasjonen må være gratis og ikke beskyttet av konfidensialitetsavtaler.	O
9.	Dokumentasjon av API bør tilbys i henhold til "OpenAPI Specification", "FHIR Capability Statement" eller et tilsvarende åpent og maskinlesbart format.	A
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) Beskrivelse av tilgjengelighet for API-et, og hvordan planlagt vedlikehold gjennomføres h) Beskrivelse av begrensninger og andre driftsmessige egenskaper 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 levetid for API-et og hvordan versjonering av API-et håndteres.	O

3 Rammebetingelser for behandling og deling av helseopplysninger

Det er flere ulike regler som regulerer behandling av helseopplysninger. Med behandling menes enhver bruk av helseopplysningene, som for eksempel innsamling, registrering, lagring, jf. EUs personvernforordning artikkel 4 nr. 2[11].

3.1 Personvern

Den mest sentrale loven for behandling av helseopplysninger er personvernforordningen. Den dataansvarlige skal anvende prinsippene om innebygd personvern. Den dataansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen ved behandlingen av opplysningene, jf. artikkel 32. Det skal iverksettes tiltak for å sikre opplysningenes konfidensialitet, integritet og tilgjengelighet. Pasientjournalloven[12], som gir det rettslige behandlingsgrunnlaget for pasientjournaler, gjentar sentrale bestemmelser i forordningen i pasientjournalloven § 22 om informasjonssikkerhet.

3.2 Helseopplysninger

De viktigste lovene når det det gjelder helseopplysninger er pasientjournalloven og bestemmelser i helsepersonelloven[13] og pasient- og brukerrettighetsloven[14] gjelder som særlovgivning, og presiserer eller begrenser behandlingen av journalopplysninger. De generelle reglene i forordningen gjelder, så langt ikke annet følger av helselovgivningen.

Pasientjournalloven gir rettslig grunnlag for deling av opplysninger med helsepersonell og samarbeidende personell når det er nødvendig for å kunne gi helsehjelp, jf. §§ 6 og 19. Dette gjelder også på tvers av virksomheter. Dataansvarlig har blant annet en plikt til å sørge for å tilgjengeliggjøre helseopplysninger i samsvar med helsepersonelloven §§ 25 og 45. Opplysningene kan bare gjøres tilgjengelig når de er relevante og nødvendige for å kunne gi forsvarlig helsehjelp og i samsvar med reglene om taushetsplikt, jf. helsepersonelloven § 21 flg. Det er kun de som har tjenstlig behov som skal få tilgang til opplysningene, og de skal ikke ha flere opplysninger enn det som er relevant og nødvendig for å yte helsehjelpen.

Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Helseopplysninger i journalen kan som hovedregel ikke gjøres tilgjengelig for annet helsepersonell dersom pasienten motsetter seg det, jf. pasientjournalloven § 17 a). Opplysningene skal gjøres tilgjengelig på en måte som ivaretar informasjonssikkerheten. Videre stiller pasientjournalforskriften konkrete krav til tilgangsstyringen. Dataansvarlig skal ha kontroll og oversikt over all behandling av helseopplysninger som de selv er ansvarlig for, inkludert tilgjengeliggjøring av opplysninger til andre virksomheter, jf. pasientjournalforskriften

[11] Lov om behandling av personopplysninger (personopplysningsloven)
[12] Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)
[13] Lov om helsepersonell m.v. (helsepersonelloven)
[14] Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)

§ 12 tredje ledd. Tilgang til helseopplysninger skal bygge bl.a. på autorisasjon, sikker autentisering og løpende kontroll, jf. pasientjournalforskriften §§ 13 og 14.

3.3 Informasjonssikkerhet i helse- og omsorgssektoren

Norm for informasjonssikkerhet i helse- og omsorgssektoren[15] detaljerer og supplerer gjeldende regelverk og gir detaljert veiledning, praktiske eksempler og informasjon om behandling av helseopplysninger ved helsehjelpsytelse.

3.4 Oversikt over grunnleggende rammebetingelser

Tabellen nedenfor er ikke uttømmende, men gir en oversikt over de grunnleggende rammebetingelsene for behandling og herunder deling av helseopplysninger:

	Behandling av helseopplysninger i åpne API-er
1.	**Behandlingsgrunnlag** For å behandle helseopplysninger til dette formålet krever EUs personvernforordning artikkel 6 og 9 og pasientjournalloven § 6 at det skal foreligge et rettslig grunnlag for behandlingen av helseopplysningene. Pasientjournalloven § 19, ref. helsepersonelloven §§ 45 og 25 regulerer kommunikasjon av helseopplysninger. Den dataansvarlig kan 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). *Virksomheter som deler helseopplysninger gjennom et API må sikre at det foreligger et slikt rettslig grunnlag.*
2.	**Dataansvar** Behandlingen av helseopplysningene må knyttes til en dataansvarlig. Dette følger av EUs personvernforordning og pasientjournalloven. Den dataansvarlige har ansvaret for at behandlingen av helseopplysningene er i samsvar med gjeldende regelverk. *Virksomheter som skal tilgjengeliggjøre helseopplysninger via API må på forhånd ha avklart dataansvaret. Det er normalt den enkelte virksomheten som er dataansvarlig for helseopplysninger i journalsystemene.*
3.	**Rett til å motsette seg deling (sperre)** Pasientjournalloven § 17 gir pasienten rett til å motsette seg at helseopplysninger gjøres tilgjengelig for annet helsepersonell. Den dataansvarlige virksomhet må ha systemer for tilgangsstyring med innstillinger som ivaretar denne retten. Det må bl.a. kunne settes sperre på rolle, virksomhet, avdeling og enkeltperson. I tillegg må det kunne sperres på hele eller deler av helseopplysningene i journalen. 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.

[15] Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten versjon 6.0, 2020

	Virksomheter som skal tilgjengeliggjøre helseopplysninger gjennom API må ha funksjonalitet for å sjekke om det foreligger sperrer som hindrer utlevering til tross for at det finnes et behandlingsgrunnlag, ref. pkt. 1 over. Eventuelt må datasettet som tilgjengeliggjøres ikke inneholde opplysninger noen har motsatt seg at kan utleveres.
4.	**Rett til informasjon, innsyn, retting og sletting** EUs personvernforordning kapittel 3 angir den registrertes rettigheter. Helselovene gir særregler knyttet til pasientens rett til informasjon, innsyn, retting og sletting. *Virksomheter som skal gjøre tilgjengelig helseopplysninger mellom virksomheter via API må bl.a. sikre at pasientene får informasjon om tilgjengeliggjøringen.*
5.	**Dataminimering** EUs personvernforordning art 5 nr. 1 c) angir at dataansvarlige ikke skal samle inn flere personopplysninger enn det som er nødvendig for å oppnå formålet med behandlingen av opplysningene. Ved 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 for å kunne avgjøre hvilke opplysninger som er nødvendige. Da er det viktig at mottagervirksomheten har gode rutiner for sletting av opplysninger. *Virksomheter som skal gjøre tilgjengelig helseopplysninger via API må sette opp API-et eller API-ene 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.*
6.	**Lagringsbegrensning** EUs personvernforordning art 5 nr. 1 c) angir at personopplysninger ikke skal lagres lengre enn nødvendig for å oppnå formålet med behandlingen av opplysningene. 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. *Virksomheter som aksesserer opplysninger gjennom et API må vurdere om det er grunnlag for å lagre (en egen kopi av) opplysningene.*
7.	**Informasjonssikkerhet** EUs personvernforordning og pasientjournalloven krever at helseopplysningene skal beskyttes mot uberettiget innsyn og endringer. Samtidig må helseopplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for det *Virksomhetene som deler helseopplysninger gjennom API må ha tiltak for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet. Det må etableres system for identitets- og tilgangsstyring som ivaretar regler om personvern, taushetsplikt og tjenstlig behov for informasjonen.*

8.	**Internkontroll** EUs personvernforordning artikkel 24 angir at for å kunne kontrollere at personopplysninger blir behandlet riktig er det nødvendig å ha oversikt over *hvem* som har tilgang til hvilke opplysninger. Dette er nødvendig for å kunne føre etterkontroll og tilfredsstille den registrertes rettigheter 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.
9.	**Databehandleravtale** EUs personvernforordning artikkel 28 angir at det må inngås databehandleravtale med virksomheter som behandler helseopplysninger på vegne av den dataansvarlige. I helsesektoren deles opplysninger mellom virksomheter som på hver sin side er dataansvarlige for opplysninger som er relevante og nødvendige å nedtegne i journalen.
10.	**Protokoll** EUs personvernforordning artikkel 30 angir at virksomheter som behandler personopplysninger skal holde en protokoll over databehandlingsaktiviteter. 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 helseopplysninger