Direktoratet for e-helse

Én innbygger – én journal

Overordnet vurdering av personvernspørsmål

Nasjonal løsning for kommunal helse- og omsorgstjeneste

Vedlegg H

IE-1029

Publikasjonens tittel:
Vedlegg H Overordnet personvernvurdering
Konseptvalgutredning - Nasjonal løsning for kommunal helse- og omsorgstjeneste

Rapportnummer
IE-1029

Utgitt:
August 2018

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Postadresse:
Postboks 6737 St. Olavs plass, 0130 OSLO

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

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Sammendrag

Konseptene reiser personvernspørsmål
Denne vurderingen behandler tre konseptalternativer som i ulike grad vil kunne oppnå målet om "en nasjonal løsning for kommunal helse- og omsorgstjeneste" og målbildet beskrevet i Meld. St. 9 (2012-2013). De tre konseptene innebærer nye måter å behandle helseopplysninger på i kommunal helse- og omsorgstjeneste. Konsept 7 innebærer etablering av én nasjonal journalløsning. Alt helsepersonell som er ansatt i virksomheter som tar i bruk løsningen vil arbeide i denne, og mye av samhandlingen skjer der. Konsept 1 og konsept 4 er i stor grad en videreføring av dagens situasjon ved at innbyggers journal er delt, med mange ansvarlige, og at helseopplysninger behandles i flere systemer. I alle konseptene skal det etableres en nasjonal samhandlingsløsning for deling av helseopplysninger.

Dette dokumentet beskriver en overordnet vurdering av personvernspørsmål for de tre konseptene, i henhold til gjeldende rett og sett i lys av kravene i EUs personvernforordning. Vurderingen er en del av alternativanalysen, og den har fokus på hva som skiller de ulike konseptene. Den inngår i vurderingen for å kunne anbefale ett konsept.

Innholdet i vurderingen
Den overordnede vurderingen starter med en gjennomgang av prinsippene for behandling av personopplysninger, jf. EUs personvernforordning art 5, en kort vurdering av kravet om innbygd personvern og vurderinger rundt formålet med behandlingen. Deretter gjøres en vurdering av følgende krav i personvernregelverket som er relevante for konseptene:

- Rettsgrunnlag
- Ansvar
- Den registrertes rettigheter

Krav om sikkerhet i behandlingen av helseopplysningene (informasjonssikkerhet) vil ikke bli vurdert her, men i en egen overordnet risiko- og sårbarhetsvurdering (ROS)1. Denne personvernvurderingen må derfor ses i sammenheng med ROS-vurderingen.

Konseptene og løsningene er ikke beskrevet på et detaljert nok nivå til at det på nåværende tidspunkt kan gjennomføres en fullverdig personvernkonsekvensvurdering. EUs personvernforordning artikkel 35 stiller krav om at det skal gjennomføres en "Data Protection Impact Assessment" (DPIA) ved behandling av helseopplysninger og der risikoen ved behandlingen ikke er ubetydelig. En fullverdig DPIA vil gjennomføres for valgt konsept på et senere tidspunkt.

Det er foreløpig ikke gjort noen vurdering etter sikkerhetsloven. I videre arbeid vil det være aktuelt å vurdere anbefalt konsept etter den nye sikkerhetsloven som ventes å tre i kraft i 2019.

Resultatet av vurderingen

[1] Se vedlegg G Overordnet risiko- og sårbarhetsanalyse.

Alle konseptene vil, forutsatt regelverksutvikling, kunne ivareta personvernprinsippene og oppfylle relevante krav i personvernregelverket. Som følge av at arbeidet er på et strategisk og konseptuelt nivå er det imidlertid vanskelig å utpeke ett konsept som klart bedre egnet enn de øvrige konseptene totalt sett. Endelig omfang av samhandlingsløsningen er for eksempel ikke definert i denne fasen av arbeidet.

Alle konseptene vil kunne ivareta den registrertes rettigheter, men konseptene muliggjør i ulik grad hvor helhetlig og effektivt dette kan håndteres. En nasjonal løsning i konsept 7 vil muliggjøre en helhetlig og effektiv håndtering av rettigheter, herunder retten til individuelt innsyn og retten til å motsette seg behandling av helseopplysninger. På den måten vil den registrerte kunne få bedre muligheter til å gjøre sine rettigheter gjeldende, til medvirkning og til å få kontroll med behandlingen av sine helseopplysninger. Samtidig vil konseptet kunne berøre innbyggers mulighet til å starte med "blanke ark" hos ny behandler. Konsept 4 vil også kunne tilrettelegge for helhetlig og effektiv håndtering av rettigheter, men uten samlet oversikt over opplysninger. Konsept 1, som i stor grad viderefører eksisterende løsninger og dagens situasjon med lokale journaler, gir ikke samme muligheter for helhetlig og effektiv håndtering av rettigheter. Det vil videre generelt kunne være vanskeligere og mer ressurskrevende å etablere innebygd personvern ved realiseringen av konsept 1, enn å legge dette som er forutsetning for utvikling av nye nasjonale løsninger i konsept 4 og konsept 7.

Alle konseptene vil kunne medføre behov for rettslige endringer for å etablere rettslig grunnlag for nye nasjonale journal- og samhandlingsløsninger. Konseptene 1 og 4 vil delvis kunne realiseres innenfor gjeldende rett. Men for å realisere konseptene fullt vil det trolig være behov for lov eller forskriftsendringer for å etablere rettsgrunnlag for en ny nasjonal samhandlingsløsning. For konsept 4 og konsept 7 vil det i tillegg måtte vurderes om det vil være behov for endringer i lov eller forskrift for eventuelt å pålegge virksomheter å ta i bruk løsningen. Konsept 7 vil kreve lovendring for å etablere rettsgrunnlag for en nasjonal journalløsning for kommunal helse- og omsorgstjeneste. En nasjonal journal, som i konsept 7, kan medføre press på å bruke helseopplysningene til andre formål. Slik endret bruk vil i så fall kreve en ny vurdering og evt. rettslige endringer.

Alle konseptene vil kunne ha konsekvenser for roller og ansvar. Konsept 7 legger opp til at dataansvaret for den nasjonale journalløsningen skal samles hos en virksomhet. Dette vil kunne gi grunnlag for en tydelig ansvarsplassering. Det vil måtte avklares hvem som kan være dataansvarlig, og denne vil måtte utpekes i lov eller forskrift. De enkelte helsevirksomhetene vil imidlertid fortsatt måtte ha et selvstendig ansvar knyttet til behandling av helseopplysningene. Det må derfor avklares hva dataansvaret skal omfatte konkret for denne løsningen, og hva som ikke omfattes og som dermed må ligge igjen hos virksomhetene. Krav basert på pasientrettigheter vil for eksempel måtte vurderes av helsepersonell i helsevirksomhetene. I konseptene 1 og 4 vil dataansvaret hovedsakelig, som i dag, være hos helsevirksomhetene. Ansvaret vil da fortsatt være fragmentert, og myndighetene vil derfor ikke ha det samme grunnlaget for en helhetlig tilnærming til blant annet å sikre informasjonssikkerhet, innbyggers rettigheter mv. På den andre siden vil ansvaret da være plassert i nærhet til virksomheten som behandler helseopplysningene, og som for eksempel kan vurdere krav som følge av pasientrettigheter. Plassering av dataansvaret for en nasjonal samhandlingsløsning er ikke definert i denne fasen av arbeidet, og vil derfor måtte vurdere senere.

Det vil for alle konseptene være nødvendig å etablere tekniske, fysiske og organisatoriske tiltak for å redusere personvernulemper. Identifiserte personvernkonsekvenser vil danne grunnlag for å bestemme hvilke tiltak som skal treffes for å redusere risikoen.

2 Innledning

Denne vurderingen behandler tre konseptalternativer som i ulik grad vil kunne oppnå målet om "en nasjonal løsning for kommunal helse- og omsorgstjeneste" og målbildet beskrevet i Meld. St. 9 (2012-2013). De tre konseptene innebærer nye måter å behandle helseopplysninger på i kommunal helse- og omsorgstjeneste. Konsept 7 innebærer etablering av en nasjonal journalløsning. Alt helsepersonell som er ansatt i virksomheter som tar i bruk løsningen vil arbeide i denne, og mye av samhandlingen vil skje der. Konsept 1 og konsept 4 er i stor grad en videreføring av dagens situasjon ved at innbyggers journal er delt, med mange ansvarlige, og at helseopplysninger behandles i flere systemer. I alle konseptene skal det etableres en nasjonal samhandlingsløsning for deling av helseopplysninger.

Dette dokumentet beskriver en overordnet vurdering av personvernspørsmål for de tre konseptene, i henhold til gjeldende rett og sett i lys av kravene i EUs personvernforordning. Vurderingen er en del av alternativanalysen, og den har fokus på hva som skiller de ulike konseptene. Den inngår i vurderingen for å kunne anbefale ett konsept.

Den overordnede vurderingen av de tre konseptene starter med en gjennomgang av prinsippene for behandling av personopplysninger etter EUs personvernforordning art 5. (kapittel 3), en kort vurdering av kravet om innebygd personvern (kapittel 4) og vurderinger rundt formålet (kapittel 5). Deretter vurderes følgende krav:

- Rettsgrunnlag (kapittel 6)
- Ansvar (kapittel 7)
- Den registrertes rettigheter (kapittel 8)

Krav om sikkerhet i behandlingen av helseopplysninger (informasjonssikkerhet) vil ikke bli vurdert her, men i en overordnet risiko- og sårbarhetsanalyse. Denne personvernvurderingen må derfor ses i sammenheng med risiko- og sårbarhetsanalysen (ROS) for konseptene, se vedlegg G Overordnet risiko- og sårbarhetsvurdering.

Konseptene og løsningene er ikke beskrevet på et detaljert nok nivå til at det på nåværende tidspunkt kan gjennomføres en fullverdig personvernkonsekvensvurdering. EUs personvernforordning artikkel 35 stiller krav om at det skal gjennomføres en "Data Protection Impact Assessment" (DPIA) ved behandling av helseopplysninger og der risikoen ved behandlingen ikke er ubetydelig. En fullverdig DPIA vil gjennomføres for valgt konsept på et senere tidspunkt.

Det er heller ikke gjort en vurdering av de tre konseptene etter sikkerhetsloven. I videre arbeid vil det være aktuelt å vurdere anbefalt konsept etter den nye sikkerhetsloven som ventes å tre i kraft i 2019.

Det er en forutsetning at alle konseptene skal ivareta pasientens rettigheter og helsepersonells og virksomheters plikter. Hvordan dette skal ivaretas, må vurderes nærmere for valgt konsept i forbindelse med planleggingen og utformingen av løsningen.

Det vil for alle konseptene være nødvendig å etablere tekniske, fysiske og organisatoriske tiltak for å redusere personvernulemper. Identifiserte personvernkonsekvenser vil danne grunnlag for å bestemme hvilke tiltak som skal treffes for å redusere risikoen.

3 Prinsipper for behandling av personopplysninger

3.1 Krav om å opptre i samsvar med prinsippene

Reglene for behandling av personopplysninger bygger på flere grunnleggende prinsipper. Disse er nedfelt i EUs personvernforordning art. 5. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene. Alle kravene i personvernforordningen for øvrig vil kunne føres tilbake til et eller flere av personvernprinsippene, og samlet bidra til at prinsippene effektivt kan ivaretas.

Under gjøres en vurdering av personvernprinsippene opp mot konseptene og hvor egnet de er til å ivareta prinsippene. På det overordnede nivået konseptene er på nå, er det vanskelig å utpeke ett konsept som best kan oppfylle prinsippene. Det legges til grunn at alle konseptene vil kunne oppfylle prinsippene.

3.2 Lovlighet, rettferdighet og åpenhet – vurdering av konseptene

Prinsippet om lovlighet innebærer først og fremst at behandlingen av personopplysninger må ha et rettslig grunnlag etter forordningen og eventuelt særlovgivningen. Videre vil prinsippet om lovlighet også innebære en etterlevelse av bestemmelser i forordningen som er aktuelle for behandlingen. En vurdering av dette prinsippet vil dermed også bety en gjennomgang av lovligheten av behandlingen totalt sett.

Prinsippet om rettferdighet innebærer at behandlingen av personopplysninger skal skje på en måte som er rettferdig for den registrerte. Behandlingen skal for eksempel ikke foregå på fordekte eller manipulerende måter. Hvis behandlingen skal oppfylle prinsippet om åpenhet, betyr det at behandlingen må skje på en måte som er oversiktlig og forutsigbar for den registrerte, slik at den registrerte er i stand til å ivareta egne interesser og bruke sine rettigheter.

3.2.1 Vurdering av konseptene

Alle konseptene må ha rettslig grunnlag for behandlingen av helseopplysningene. Krav om rettsgrunnlag er vurdert i kapittel 5. Det fremgår der at alle konseptene, dvs. de nasjonale

løsningene, vil kunne kreve rettslige endringer for å kunne oppfylle prinsippet og kravene i gjeldende rett og forordningen.

Konsept 1, som i stor grad er en videreføring av dagens situasjon, vil delvis kunne realiseres innenfor gjeldende rett. Det å realisere konseptet fullt ut med ny nasjonal samhandlingsløsning vil kunne kreve rettslige endringer. I konsept 4 vil det i tillegg være behov for rettslige endringer for kunne pålegge virksomhetene å ta løsningen i bruk. Konsept 7 vil i tillegg kreve lovendring for å kunne etablere en nasjonal journalløsning.

For å oppfylle kravet om åpenhet vil det i alle konseptene måtte settes inn tiltak for å gi god informasjon til den registrerte. Den registrerte må for eksempel få tydelig informasjon om hvor vedkommende skal henvende seg for å ivareta sine rettigheter. Konsept 7 og eventuelt konsept 4 vil kunne muliggjøre at det gis effektiv og helhetlig informasjon til den registrerte i større grad enn i konsept 1. Det er imidlertid vanskelig å si noe sikkert om konsept 7 og konsept 4 vil kunne ivareta dette på en bedre måte enn konsept 1.

3.3 Formålsbegrensning – vurdering av konseptene

I formålsbegrensning ligger det at personopplysninger bare kan behandles til uttrykkelige, spesifikt angitte og berettigede formål. Det betyr at et hvert formål med behandling av personopplysninger skal identifiseres og være forklart på en tydelig måte. Personopplysninger kan ikke gjenbrukes til formål som er uforenelige med det opprinnelige formålet.

3.3.1 Vurdering av konseptene

Alle konseptene (behandlinger og løsninger) vil kunne skje innenfor formålet som er vurdert i kapittel 5. Det er ingen grunn til å skille på konseptene.

3.4 Dataminimering – vurdering av konseptene

Dataminimeringsprinsippet henger tett sammen med formålsbegrensningsprinsippet. I dataminimeringsprinsippet ligger det at den dataansvarlige skal begrense mengden med personopplysninger til det som er relevant og nødvendig for å oppnå det konkrete formålet med behandlingen.

3.4.1 Vurdering av konseptene

Det må for alle konseptene gjøres en vurdering av hva som er nødvendige og relevante opplysninger for å oppnå formålet som er vurdert i kapittel 5. Alle konseptene vil i større eller mindre grad baseres på strukturert journalføring. Det er ingen grunn til å skille på konseptene.

3.5 Riktighet – vurdering av konseptene

Det er et prinsipp etter EUs personvernforordning at personopplysninger som behandles skal være korrekte, og opplysningene må oppdateres ved behov. Dataansvarlig må sørge for at personopplysninger som er uriktige rettes eller slettes straks/uten ugrunnet opphold.

3.5.1 Vurdering av konseptene

Konsept 7 og konsept 4 vil kunne muliggjøre en helhetlig og mer effektiv håndtering av rettigheter slik at det blir enklere for den registrerte å oppdage om informasjonen er korrekt eller misvisende, og dermed bidra til at opplysningene er korrekte. Den registrerte rettigheter er vurdert i kapittel 8. Utover muligheten for en mer helhetlig håndtering er det imidlertid vanskelig å si sikkert om konsept 7 og konsept 4 vil kunne ivareta dette på en bedre måte enn konsept 1.

3.6 Integritet og konfidensialitet – vurdering av konseptene

Prinsippet om opplysningenes integritet betyr at opplysningene som behandles må være korrekte, gyldige og fullstendige og sikres mot utilsiktet eller uautorisert endring eller sletting. Konfidensialitet handler kort sagt om å sikre at opplysningene bare er tilgjengelig for de som rettmessig skal ha tilgang til dem.

3.6.1 Vurdering av konseptene

Krav om sikkerhet i behandlingen av helseopplysningene (informasjonssikkerhet) vil ikke bli vurdert her, men i en overordnet risiko- og sårbarhetsvurdering (ROS). Denne personvernvurderingen må derfor ses i sammenheng med den overordnede ROS-vurderingen for konseptene. Se vedlegg G "Overordnet risiko- og sårbarhetsvurdering".

Det vil for alle konseptene være nødvendig å sette inn robuste tiltak og rutiner som sikrer mot utilsiktet eller uautorisert endring, sletting eller tilgang til helseopplysningene.

3.7 Lagringsbegrensning – vurdering av konseptene

Prinsipp om lagringsbegrensning betyr at personopplysninger skal slettes når formålet de ble samlet inn for er oppnådd.

3.7.1 Vurdering av konseptene

Alle konseptene må sette inn tiltak for å følge til enhver tid gjeldende krav til lagringstid. Regler for lagring og oppbevaring av helseopplysningene i pasientjournalen følger av pasientjournalloven og pasientjournalforskriften. Lagringstiden for helseopplysninger i nasjonale løsninger som Nasjonal kjernejournal, Reseptformidleren mv. er regulert i forskrift. Det er ulike lagringstider for helseopplysninger i de ulike nasjonale løsningene og pasientjournalen. Hvordan dette skal håndteres i nye løsninger må avklares i forprosjektet. Det er ingen grunn til å skille på konseptene.

3.8 Ansvarlighet – vurdering av konseptene

Prinsippet om ansvarlighet understreker at den dataansvarlige er den ansvarlige for at behandlingen oppfyller personvernprinsippene etter forordningen og at den registrertes rettigheter og friheter er ivaretatt. Dette må også kunne dokumenteres.

3.8.1 Vurdering av konseptene

Alle konseptene (løsningene og behandlingene) må ha en ansvarlig for behandlingen av helseopplysningene. Dataansvaret er nærmere omtalt i kapittel 6. Det legges til grunn at alle konseptene vil kunne ivareta prinsippet.

I Konsept 7 legges det opp til at dataansvaret for den nasjonale journalen skal samles hos én virksomhet. Det vil gi grunnlag for en tydelig ansvarsplassering. Den enkelte helsevirksomhet vil fortsatt måtte ha noe selvstendig ansvar for behandlingen av helseopplysningene. I konseptene 1 og 4 vil ansvaret, som i dag, være plassert hos de enkelte helsevirksomhetene. Ansvaret vil da fortsatt være fragmentert, og man har derfor ikke de samme mulighetene til å etablere en helhetlig tilnærming til håndteringen av den registrertes rettigheter. På den annen side vil ansvaret da være plassert hos virksomhetene som utfører helsehjelp, og som også vil være nærmest til å ta stilling til eventuelle krav om innsyn, retting mv. Plassering av dataansvaret for en nasjonal samhandlingsløsning vil måtte avklares.

4 Innebygd personvern

4.1 Krav om innbygd personvern

Innebygd personvern vil bli et krav når EUs personvernforordning art. 25 trer i kraft. Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning fra de første ideene kommer opp til løsningen settes i drift og under videre forvaltning av løsningen. Kravet til innebygd personvern skal sørge for at løsningene som brukes oppfyller personvernprinsipper, ivaretar den registrertes rettigheter og krav til sikkerhet ved behandlingen effektivt oppfylles.

Kravet til innebygd personvern og personvern som standardinnstilling, er et sentralt krav i forordningen. Den dataansvarlige skal følge kravet om innebygd personvern ved utvikling av programvare, og ved bestilling av system, løsninger og tjenester. Kravet bør også inkluderes ved inngåelse av avtaler med leverandører.

4.2 Vurdering av konseptene

Det vil generelt kunne være vanskeligere og mer ressurskrevende å etablere innebygd personvern ved realiseringen av konsept 1, som i stor grad bygger på eksisterende løsninger, enn å legge dette som er forutsetning for utvikling av nye nasjonale løsninger i konsept 4 og konsept 7.

5 Formålsvurdering

5.1 Krav om formålsbestemthet

Et grunnleggende prinsipp er at personopplysninger bare skal behandles til uttrykkelig angitte og berettigede formål. Det er i tillegg et krav om at opplysningene ikke skal behandles til andre formål som er uforenelig med det opprinnelige. I slike tilfeller er det nødvendig med

eget rettsgrunnlag. Dette er prinsippet om «formålsbegrensning», se omtale i punkt 3.3. Det må derfor avklares hvilket formål behandlingen av helseopplysningene i konseptene skal ha og hvilke behov den skal dekke.

Formålet som angis for løsningen vil være førende for hvilke opplysninger som kan samles inn og behandles i løsningen. Dersom det senere skulle oppstå ønske om eller behov for å gjenbruke informasjonen til andre formål, må det gjennomføres en ny vurdering.

5.2 Hva er formålet?

Konseptene skal tjene målbildet som er beskrevet i Meld. St. 9 (2012-2013) Én innbygger – én journal. Helsepersonell skal ha rask og enkel tilgang til nødvendige og oppdaterte helseopplysninger, samtidig som personvernet ivaretas. Dette gjelder gjennom hele behandlingsforløpet uavhengig av hvor i landet pasienten blir syk eller får behandling.

Videre skal konseptene kunne nå målene angitt i prosjektets oppdrag, som er å løse behov knyttet til:

- Klinisk dokumentasjon og pasient- og brukeradministrasjon i kommunal helse- og omsorgstjeneste, inkludert fastlegene
- Samhandling med øvrig helsetjeneste (særlig spesialisthelsetjenesten)
- Samhandling mellom helsetjenesten og andre kommunale og statlige tjenesteområder

Det er videre en rammebetingelse at krav til personvern og informasjonssikkerhet skal ivaretas.

Hovedformålet er å gi pasienter helsehjelp av god kvalitet. Behandlingen av helseopplysningene skal skje på en måte som gjør at relevante og nødvendige helseopplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell for å kunne gi helsehjelp, samtidig som vernet mot at opplysninger gis til uvedkommende ivaretas. At relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonellet, vil fremme god kvalitet i helsehjelpen og pasientsikkerheten. Behandlingen av helseopplysninger skal også skje på en måte som ivaretar pasientens rettigheter.

I tillegg er det et formål å tilrettelegge for bedre elektronisk samhandling mellom helse- og omsorgstjenesten og personell i øvrige kommunale tjenester, for eksempel med barnevernet eller NAV. Det legges til grunn at behandlingen skal skje innenfor gjeldende rett, herunder regler om taushetsplikt.

5.3 Vurdering av konseptene

Det legges til grunn at alle konseptene (løsninger og behandlinger) vil kunne realiseres innenfor målene som er beskrevet i Meld. St. 9 (2012-2013) Én innbygger – én journal og i oppdraget med å løse behov knyttet til en nasjonal løsning for kommunal helse- og omsorgstjeneste. Konseptene vil imidlertid i ulik grad oppnå målene. Konsept 7 har høyere måloppnåelse enn konseptene 1 og 4. Se eksempelvis vurdering av krav i Vedlegg B Mulighetsstudie og vurdering av nytte i Vedlegg D Kost- og nyttevurdering.

Det bør være bevissthet rundt at konsept 7 (og eventuelt konsept 4) vil kunne medføre at vi får et økt press på å bruke helseopplysningene til andre formål. Slik endret bruk vil i så fall kreve en ny vurdering og evt. rettslige endringer.

6 Rettslig grunnlag

6.1 Krav om rettslig grunnlag for behandling av helseopplysninger

Alle konseptene har løsninger som er beskrevet som løsninger for dokumentasjon av helsehjelp og samhandling i forbindelse med ytelse av helsehjelp til den enkelte pasient. Disse må kunne sies å være behandlingsrettede helseregistre, jf. definisjonen i pasientjournalloven § 2 d.

For å behandle helseopplysninger til dette formålet krever EUs personvernforordning og pasientjournalloven at det skal foreligge et rettslig grunnlag for behandlingen av helseopplysningene. Dette er også omtalt under prinsippet om lovlighet i kapittel 3.2. Det er derfor behov for å avklare om det foreligger slikt rettslig grunnlag for å kunne etablere løsningene og behandlingene som er beskrevet i de tre konseptene.

I dette kapittelet vurderes rettsgrunnlaget for det som er nytt sammenlignet med dagens situasjon, dvs. de nasjonale løsningene. I kapittel 6.3 vurderes rettsgrunnlaget for én nasjonal journalløsning i konsept 7 og i kapittel 6.4 vurderes rettsgrunnlaget for en nasjonal samhandlingsløsning i konseptene 1, 4 og 7. Det legges til grunn at behandlingen av helseopplysninger som skjer i dag har gyldig rettsgrunnlag.

6.2 Pasientjournalloven

Pasientjournalloven regulerer «behandlingsrettede helseregistre» uavhengig av i hvilket system opplysningene registreres. I § 2 bokstav d) er behandlingsrettet helseregister definert som *"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* enkeltperson."

Behandlingsrettede helseregistre er knyttet til dokumentasjonsplikten og skal omfatte all behandling av helseopplysninger som er nødvendige for at helsehjelp kan ytes. Helsepersonell som yter helsehjelp har plikt til å nedtegne opplysninger som anses som relevante og nødvendige for helsehjelpen til den enkelte pasient, samt opplysninger som er nødvendige for å oppfylle melde- eller opplysningsplikter som er fastsatt i lov, jf. helsepersonelloven §§ 39, 40. Det er ikke krav om pasientens samtykke for at helsepersonellet kan nedtegne og lagre journalopplysninger. Pasienten har imidlertid rett til å motsette seg at helseopplysninger i behandlingsrettet helseregister gjøres tilgjengelig for annet helsepersonell, jf. pasientjournalloven § 17, helsepersonelloven §§ 25 og 45, pasient- og brukerrettighetsloven § 5-3.

Pasientjournalloven regulerer ulike behandlingsrettede helseregistre. Av § 6 fremgår det at behandlingsrettede helseregister skal ha hjemmel i lov. Det følger av § 8 at virksomheter som yter helsehjelp har plikt til å sørge for behandlingsrettede helseregistre. Av pasientjournalloven § 7 om krav til behandlingsrettede helseregistre følger at behandlingsrettede helseregistre skal understøtte pasientforløp i klinisk praksis og være lett å bruke og å finne frem i. De skal også være utformet og organisert slik at krav fastsatt i eller i medhold av lov kan oppfylles.

Pasientjournalloven § 9 gir hjemmelsgrunnlag for at flere virksomheter kan samarbeide om behandlingsrettede helseregister. Samarbeidet kan omfatte privateide så vel som offentlige virksomheter, alle typer behandlingsrettede helseregister, alle systemene som utgjør hele pasientjournalen eller kun registre på bestemte områder. Bestemmelsen krever at det inngås en skriftlig samarbeidsavtale og setter krav til innholdet i avtalen. Det følger av andre ledd at departementet i forskrift eller enkeltvedtak kan gi nærmere vilkår for samarbeid om behandlingsrettede helseregistre etter første ledd.

Pasientjournalloven § 10 gir hjemmel til, i forskrift, å etablere nasjonale behandlingsrettede helseregistre. Med nasjonale registre menes registre som kan gjelde pasienter og brukere i hele landet (landsomfattende) og som ikke er begrenset til for eksempel regioner. Bestemmelsen gir hjemmel for behandlingsrettede helseregistre på bestemte områder, som for eksempel legemiddelregister eller epikriseregister.

Reseptformidleren og Nasjonal kjernejournal er regulert særskilt i pasientjournalloven §§ 12 og 13.

6.3 Vurdering av konseptene

6.3.1 Rettsgrunnlag - nasjonal journalløsing

Konsept 7 innebærer at det etableres én felles nasjonal journalløsning for dokumentasjon av helsehjelp og samhandling i kommunal helse- og omsorgstjeneste. Løsningen skal etableres og forvaltes i et samarbeid mellom nasjonale myndigheter og virksomheter og kommunesektoren. Virksomheter i kommunal helse- og omsorgstjeneste skal pålegges å bruke løsningen for å gjennomføre dokumentasjonsplikten.

Pasientjournalloven § 9 åpner for at to eller flere virksomheter kan samarbeide om behandlingsrettede helseregistre. Bestemmelsen er svært vid. Bestemmelsen omfatter alle typer virksomheter, slik at både private fastleger, offentlige fastleger og andre virksomheter i kommunal helse- og omsorgstjeneste vil kunne omfattes. Videre omfatter den alle typer behandlingsrettede helseregistre, og også samarbeid om hele journalen. Det er ikke satt noen klar grense for hvor omfattende samarbeidet kan være. Dette taler for at den kan gi hjemmel for store, omfattende samarbeid både med tanke på antall virksomheter og omfanget av helseopplysninger. For å tydeliggjøre ansvaret for personvernet og hvordan kompliserte spørsmål skal avklares kan det for store og komplekse samarbeid være aktuelt å fastsette sentrale krav og/eller utpeke dataansvarlig i forskrift eller enkeltvedtak, jf. § 9 siste ledd.

Pasientjournalloven § 9 regulerer imidlertid de frivillige samarbeidene der initiativet normalt kommer fra virksomhetene selv. Den gir heller ikke hjemmel for å kunne pålegge virksomhetene å ta i bruk en felles løsning.

Det legges derfor til grunn at én nasjonal løsning for kommunal helse- og omsorgstjeneste i konsept 7 ikke kan etableres med hjemmel i pasientjournalloven § 9.

Et annet spørsmål er om pasientjournalloven § 9 kan gi hjemmel for en pilot under utviklingen av den nasjonale løsningen. Det er et spørsmål som må vurderes konkret, dersom det er aktuelt.

Pasientjournalloven § 10 gir hjemmel for å i forskrift etablere nasjonale behandlingsrettede helseregistre. Bestemmelsen kan brukes for å etablere nasjonale løsninger som ledd i å realisere det endelige målet om "Én innbygger - én journal". Videre gir den hjemmel for å kunne pålegge virksomheter å ta en slik nasjonal løsning i bruk.

Bestemmelsen er imidlertid avgrenset til journalløsninger på «nærmere bestemte områder». I forarbeidene nevnes løsninger på begrensede områder, som for eksempel; legemiddelregister, svangerskapsjournal, laboratorie- og radiologisystem og epikriseregister. Bestemmelsen er ikke ment å gi rettsgrunnlag for en løsning som dekker alt, dvs. en samlet journalløsning der alle eller mange opplysninger om pasienter samles i samme register. Dette er omtalt i forarbeidene: *«Et nasjonalt journalsystem med en felles totalløsning for alle aktørene innen helse- og omsorgssektoren, bør etter departementets vurdering legges frem for Stortinget og besluttes i lovvedtak.» «Etablering av omfattende helhetlige nasjonale journalløsninger krever dermed lovvedtak.» 2*

Den nasjonale journalløsningen skal dekke tilnærmet hele journalen for aktører innen kommunal helse- og omsorgstjeneste. Den skal ikke kun dekke deler av fastlegens eller kommunens journal, f. eks. kun legemidler. Løsningen vil, for disse aktørene, være ett behandlingsrettet helseregister hvor alle eller mange opplysninger om pasienter samles i en felles løsning. Videre må det ut fra eksemplene i forarbeidene være klart at det med «bestemte områder» er ment ulike fagdeler av en journal. Virkeområdet er ikke avgrenset slik at det gjelder for bestemte «grupper mennesker» eller «grupper virksomheter» som skal ta løsningen i bruk. Det kan derfor ikke være relevant i denne vurderingen at løsningen etableres på området «kommunal helse- og omsorgstjeneste».

På denne bakgrunnen vil en nasjonal journalløsning for kommunal helse- og omsorgstjeneste og konsept 7 heller ikke kunne etableres i forskrift med hjemmel i pasientjournalloven § 10.

Det betyr at realisering av en nasjonal journalløsning i konsept 7 vil kunne kreve lovendring, eksempelvis endringer i pasientjournalloven.

6.3.2 Rettsgrunnlag – nasjonal samhandlingsløsning

Alle konseptene innebærer at det skal etableres en nasjonal samhandlingsløsning for sikker og effektiv tilgjengeliggjøring av helseopplysninger mellom helsepersonell i ulike virksomheter og nivåer når de yter helsehjelp. Endelig omfang av samhandlingsløsningen er ikke definert i denne fasen av arbeidet.

[2] Prop. 72 L (2013-2014) Pasientjournalloven og helseregisterloven

En mulighet er at den nasjonale samhandlingsløsningen kun skal "formidle" helseopplysninger på vegne av virksomhetene, uten et selvstendig formål med behandlingen. Helseopplysningene lagres da i en begrenset periode ifm med tilgjengeliggjøringen og behandles kun for dette formålet og på bakgrunn av oppdraget fra virksomheten. Det kan vurderes om dette kan baseres på databehandleravtale med den enkelte virksomhet og den ansvarlige for samhandlingsløsningen. Men dette forutsetter bl.a. at det er logiske skiller mellom helseopplysninger fra ulike virksomheter/samarbeid.

Det kan imidlertid være behov for at den nasjonale samhandlingsløsningen også skal legge til rette for "dokumentdelingen", dvs. slik at helseopplysninger (dokumenter) kan deles mellom helsepersonell som etterspør informasjon på et senere tidspunkt. Det vil kreve at samhandlingsløsningen inneholder en nasjonal (permanent eller tidsbegrenset) oversikt over hvor det finnes helseopplysninger (journaldokumenter) om enkeltpasienter. Denne oversikten må være tilgjengelig for helsepersonell. Mens den enkelte virksomhet må vurdere hvilke journaldokumenter som kan være aktuelle å dele og gjøres tilgjengelig i løsningen. Dette er behandling av helseopplysninger i samhandlingsløsningen ut over ren formidling, som vil kreve et eget rettslig grunnlag. Det kan vurderes om forskrift om nasjonal kjernejournal § 4 punkt 7 sammenholdt med helsepersonelloven §§ 25 og 45 vil kunne være tilstrekkelig rettslig grunnlag for en nasjonal oversikt og dokumentdeling mellom helsepersonell i ulike virksomheter. Dersom dette er aktuelt må det vurderes om en nasjonal oversikt, jf. kjernejournalforskriften, vil kunne dekke formålet med konseptene. Dette bl.a. fordi innbygger kan reservere seg mot kjernejournal, og en slik nasjonal oversikt dermed ikke vil være komplett.

Videre kan det tenkes at samhandlingsløsningen på bestemte områder etablerer nye nasjonale journalløsninger. Pasientjournalloven § 10 åpner for at det i forskrift kan etableres nasjonale behandlingsrettede helseregistre på bestemte områder. Det vil evt. være behov for å etablere rettslig grunnlag i form av forskrift etter § 10.

I tillegg til å gi rettsgrunnlag for en nasjonal samhandlingsløsning vil en rettslig regulering kunne være hensiktsmessig for å etablere klare ansvarsforhold, rammer for behandlingen, forutsigbarhet mv. for en nasjonal samhandlingsløsning. Dette må vurderes nærmere i det videre arbeidet.

6.3.3 Oppsummering

Alle konseptene vil trolig behøve rettslig endringer for å etablere rettsgrunnlag for nye nasjonale journal- og samhandlingsløsninger. Det må gjøres en grundigere og endelig vurdering av rettsgrunnlaget for valgt konsept i forprosjektet.

Konsept 7 vil trolig kreve lovendring for å etablere en nasjonal journalløsning for kommunal helse- og omsorgstjeneste. Den kan neppe etableres med hjemmel i eksisterende bestemmelser i pasientjournalloven. Det vil kunne være aktuelt å etablere løsningen som en ny lovbestemmelse i pasientjournalloven med tilhørende forskriftshjemler for å kunne gi nærmere bestemmelser om ansvar, hvordan opplysningene skal behandles, mv. I tillegg vil det kunne være behov for rettslig endringer for å etablere rettsgrunnlag for etablering av en nasjonal samhandlingsløsning.

Konseptene 1 og 4 vil delvis kunne realiseres innenfor gjeldende rett. Men for å realisere konseptene fullt ut er foreløpig konklusjon at det vil det kunne være behov for lov- eller forskriftsendringer for å etablere rettsgrunnlag for en nasjonal samhandlingsløsning.

For konseptene 4 og 7 vil det i tillegg måtte vurderes om det vil kreve endringer i lov eller forskrift for eventuelt å pålegge bruk av løsninger. For alle konseptene kan det vurderes tilsvarende for en samhandlingsløsning. Dette er del av det videre arbeid med vurdering av behov for rettslige endringer, se kapittel 9.

7 Ansvar

7.1 Krav om plassering av ansvar

EUs personvernforordning opererer med rollene behandlingsansvarlig (i helselovgivningen betegnet som dataansvarlig) og databehandler. Hovedansvaret for behandling av helseopplysninger ligger hos den dataansvarlige. Dataansvaret handler om plasseringen av ansvaret for etterlevelse av personvernregler og ansvaret ved brudd på regelverket. Prinsippet om ansvarlighet er omtalt i punkt 3.8.

I dette kapittelet gjøres en vurdering av ansvar for behandlingen av helseopplysninger ved etablering av nye nasjonale løsninger. Konseptene 1 og 4 viderefører for øvrig i stor grad dagens ansvarsforhold.

7.2 Aktører og ansvar

7.2.1 Dataansvarlig

Begrepet behandlingsansvarlig er i EUs personvernforordningen artikkel 4 nr. 7 definert som:

> "en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatens nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriterier for utpeking av vedkommende fastsettes i unionsretten eller i medlemsstatenes nasjonale rett."

I helselovgivningen er behandlingsansvarlig omtalt som dataansvarlig, jf. endringer i pasientjournalloven ifm tilpasning til EUs personvernforordning. Begrepene skal forstås på samme måte.

Dette er en funksjonell definisjon som plasserer ansvaret hos den som har den faktiske kontrollen med behandlingen av helseopplysningene og som bestemmer formål og virkemidler.

Lovverket gir imidlertid også mulighet til å utpeke dataansvarlig i lov eller forskrift. Det er flere eksempler på dette i helse- og omsorgssektoren. F.eks. er Direktoratet for e-helse utpekt som dataansvarlig i forskrift for Reseptformidleren og Nasjonal kjernejournal.

I helse- og omsorgssektoren er dataansvarlig en juridisk person, dvs. en virksomhet, fordi det i praksis vil være virksomhetene som har søksmålskompetanse. Det daglige ansvaret utøves imidlertid av en eller flere fysiske personer.

EUs personvernforordning pålegger plikter for den dataansvarlige. Brudd på reglene er sanksjonert med bl.a. overtredelsesgebyr. De sentrale pliktene for den dataansvarlige er bl.a. å:

- sikre rettslig grunnlag (lovligheten av å behandle helseopplysninger) *
- ha oversikt over behandlingen av helseopplysningene
- inngå databehandleravtale når databehandling tjenesteutsettes
- bruke databehandler som gir tilstrekkelig garanti for ivaretakelse av personvernet
- etablere internkontroll
- sikre personopplysningssikkerhet, herunder at krav til konfidensialitet, integritet og tilgjengelighet blir ivaretatt
- etablere tilgangsstyring og etterfølgende kontroll, herunder sørge for at helsepersonells taushetsplikt og retten til å motsette seg utlevering av helseopplysninger ivaretas
- underrette Datatilsynet ved brudd på personopplysningssikkerheten (avviksmelding)
- melde til den registrerte om brudd på personopplysningssikkerheten der dette er pålagt
- ha løsninger med innebygd personvern og personvern som standardinnstilling*
- gjennomføre personvernkonsekvensvurderinger for nye løsninger*
- ha forhåndsdrøftinger med Datatilsynet for nye løsninger som innebærer høy risiko*
- sørge for at den registrerte rettighet blir ivaretatt, bl.a.:
    - gi den registrerte innsyn
    - gi informasjon og veiledning til den registrerte
    - sørge for rutiner for sletting og retting

*Det må vurderes om enkelte av disse pliktene vil kunne ivaretas i et lovarbeid, bl.a. det å gjennomføre personvernkonsekvensvurderinger og forhåndsdrøftinger med Datatilsynet. Ansvaret ligger da til lovendringsprosessen.

EUs personvernforordning åpner for ulike måter å organisere dataansvaret på, enten selvstendig dataansvar eller felles dataansvar. Personvernet kan ivaretas på begge måtene.

En virksomhet som alene bestemmer formålet og virkemidlene har et selvstendig dataansvar for behandlingen av helseopplysningene. I helse- og omsorgstjenesten vil de fleste virksomhetene per i dag ha et selvstendig dataansvar. Ofte vil to eller flere virksomheter samarbeide ved at de utveksler helseopplysninger seg imellom, mens de hver for seg har bestemt formål og virkemidler. Dette vil ikke utgjøre et felles dataansvar. Et eksempel på dette er utveksling av pasientopplysninger mellom sykehus og fastlege. Begge virksomhetene vil da være dataansvarlig for sin EPJ-løsning og behandlingen av helseopplysninger i den.

Felles dataansvar oppstår der to eller flere virksomheter bestemmer seg for å opprette og føre én felles journal for all behandling av et bestemt sett av helseopplysninger. Gjennom dette bestemmer de at formålet er å dokumentere helsehjelp i felles journal og at den felles

journalen er virkemidlet for å få gjennomført dette. I en slik situasjon vil alle ha det samme ansvaret for behandlingen av helseopplysningene i journalen. Felles dataansvar innebærer ikke en deling av selve ansvaret, men at det blir flere dataansvarlige for den samme behandlingen der hver og en har en selvstendig plikt til å oppfylle kravene i personvernregelverket. Det ligger med andre ord ingen ansvarsbegrensning i dette. De praktiske oppgavene som er knyttet til dataansvaret kan imidlertid fordeles mellom avtalepartene.

7.2.2 Databehandler

Det daglige forvaltningsansvaret og drift kan legges til en databehandler. Begrepet databehandler er i EUs personvernforordning artikkel 4 nr. 8 definert som "en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige."

Databehandler har ingen selvstendig råderett over helseopplysningene, og kan bare behandle opplysningene innenfor rammen av en klar avtale med den databehandlingsansvarlige. Rollen vil både være aktuell om man setter ut drift av løsningen til en kommersiell virksomhet eller om man oppretter en uavhengig, spesialisert driftsenhet.

En dataansvarlig vil selv normalt bestemme om driften skal ivaretas internt eller om driftsoppgavene skal ivaretas eksternt, og i så fall hvem som får oppdraget om å være databehandler for den dataansvarlige. Databehandler utpekes normalt ikke i lov eller forskrift fordi det kan føre til at forvaltningen av løsningen da vil bli mindre fleksibel og den dataansvarliges handlingsrom vil minske.

7.3 Virksomhetenes ansvar

Konsept 7 legger opp til at dataansvaret for en nasjonal journal for kommunal helse- og omsorgstjeneste skal samles hos en aktør, separat fra virksomhetene som registrerer helseopplysningene i løsningen. Dette vil reise spørsmål om hvilket ansvar og forpliktelser som dermed overføres til denne aktøren og hva som fortsatt må ligge igjen hos de enkelte helsevirksomhetene. I dag har helsevirksomhetene ansvar for å yte helsehjelp, dokumentere helsehjelp, sørge for behandlingsrettede helseregister/journalløsninger og de er dataansvarlige for helseopplysningene. Dette spørsmålet vil være aktuelt for alle konseptene ved etablering av en nasjonal samhandlingsløsning.

En utfordring ved en slik grenseoppgang er at mange av pliktene og rettighetene som påligger den dataansvarlige er også plikter som direkte knytter seg til helsehjelpsytelsen og dokumentasjonsplikten, og som gir pasienten rettigheter knyttet til helseopplysninger om dem selv, jf. journalforskriften § 4, spesialisthelsetjenesteloven § 3-2, helse- og omsorgstjenesteloven § 5-10 og tannhelsetjenesteloven § 1-3a, helsepersonelloven § 16.

Hvordan pliktene og rettighetene etter helselovgivningen skal ivaretas følger av helsepersonelloven og pasient- og brukerrettighetsloven. De er knyttet opp mot helsehjelpen og innebærer ofte konkrete vurderinger som gjøres av behandlende helsepersonell. For å finne ut om pasienten har rett til for eksempel å få rettet eller slettet opplysninger i henhold til helsepersonelloven §§ 42 og 43, vil helsepersonell måtte foreta en helsefaglig vurdering. Tilsvarende må det gjøres helsefaglige vurderinger mht. individuelt innsyn i egne helseopplysninger.

Dette er plikter som det ikke er sikkert at kan ivaretas av en virksomhet som utpekes som dataansvarlig for en nasjonal journalløsning, fordi den ikke også vil være ansvarlig for pasientbehandlingen og dermed ikke ha faglig grunnlag for å gjøre slike vurderinger. Hvordan rettigheter etter de to regelsettene skal innfris må organiseres på en hensiktsmessig måte mellom dataansvarlig og helsevirksomhet. Behandling av pasientrettigheter etter henholdsvis personvernregelverk og helselovgivning kan derfor vurderes løst ved en to-delt håndtering. Den dataansvarlige må legge praktisk til rette for at for eksempel retting og sletting kan skje, mens det er helsepersonellet som gjør den helsefaglige vurderingen av om vilkårene for retting eller sletting er oppfylt. Dersom det ikke legges til rette for at helsepersonellet selv skal rette og slette etter å ha vurdert spørsmålet, må helsepersonellet gi den dataansvarlige beskjed om hvordan retting eller sletting skal skje. Eventuelle endringer må altså gjøres i den enkelte helsevirksomhet av ansvarlig helsepersonell, i henhold til reglene som gjelder for retting og sletting etter helselovgivningen. Den som blir dataansvarlig vil imidlertid være ansvarlig for at pasientens rettigheter kan ivaretas i den nasjonale journalløsningen. Dette er tilsvarende vurdering som ble gjort knyttet til Nasjonal kjernejournal.

De enkelte helsevirksomhetene vil fortsatt måtte ha et selvstendig ansvar knyttet til behandling av helseopplysningene. Hva dette omfatter og hvordan dette skal håndteres må vurderes i det videre arbeidet. Etablering av én nasjonal løsning innebærer at det må gjøres et tydeligere skille mellom på den ene siden ansvaret for den nasjonale journalløsningen som kan ligge på nasjonalt nivå og de rettigheter som knytter seg direkte til behandlingen av helseopplysningene iht. personvernregelverket, og på den andre siden de plikter og rettigheter som knytter seg til det helsefaglige arbeidet som utøves hos den enkelte virksomhet som yter helsehjelp.

7.4 Vurdering av konseptene

Alle konseptene vil, men i ulik grad, kunne ha konsekvenser for dagens ansvar for behandlingen av helseopplysninger.

Konsept 7 legger opp til at dataansvaret for en nasjonal journalløsning for kommunal helse- og omsorgstjeneste skal samles hos en aktør, separat fra virksomhetene som registrerer helseopplysningene i løsningen. Dataansvaret flyttes da fra de enkelte helsevirksomhetene til denne ene virksomheten som "utpekes" som dataansvarlig i lov eller forskrift. Det vil måtte avklares hvem som skal være dataansvarlig for journalløsningen. Aktøren som utpekes må faktisk være i stand til/kapabel til å ta dette ansvaret og ha oversikt og kontroll med løsningen. De enkelte helsevirksomhetene vil fortsatt måtte ha et selvstendig ansvar knyttet til behandling av helseopplysningene. Det må avklares hva dataansvaret skal omfatte konkret for den nasjonale journalløsningen, og hva som ikke omfattes og som dermed må ligge igjen hos virksomhetene.

Fordelen med å samle ansvaret er at man vil kunne få én aktør med tydelig ansvar for forvaltning, internkontroll og etterlevelse av sikkerhetskrav, ett sted hvor sanksjoner kan gjøres gjeldende etc. Dette vil kunne sikre etterlevelse av personvernregelverk, gi muligheter for styring og for å sikre at det blir en sikker og god løsning. Videre vil et slikt "samlet" dataansvar kunne gjøre behandlingen av helseopplysningene mer tydelig og oversiktlig for den registrerte. På den andre siden vil dataansvaret da være bli plassert lenger fra der

helsehjelpen og mye av behandlingen av helseopplysningene skjer. Et eksempel vil være der det blir behov for å håndtere krav fra den registrerte som krever helsefaglig kompetanse. Dette er en utfordring som vil måtte håndteres i løsningen. Tilsvarende utfordring er håndtert for Nasjonal kjernejournal.

I konseptene 1 og 4 vil ansvaret hovedsakelig, som i dag, være plassert hos virksomhetene. Ansvaret vil da fortsatt være fragmentert, og man har derfor ikke samme muligheter for å gjøre en helhetlig tilnærming til bl.a. sikkerhet, innbyggers rettigheter mv. På den andre siden vil ansvaret da være plassert i nærhet til virksomheten som behandler helseopplysningene, og som f.eks. kan vurdere krav om rettigheter.

Plassering av dataansvaret for en nasjonal samhandlingsløsning er ikke definert i denne fasen av arbeidet, og vil derfor måtte vurdere senere.

8 Den registrertes rettigheter

8.1 Krav om at løsningen skal ivareta rettigheter

Den registrertes rettigheter står sentralt i forordningen, og en av hovedbegrunnelsene for reguleringen er å sikre at den enkelte får bedre kontroll med behandlingen av opplysninger om seg selv. Den "registrerte" vil i dette tilfellet primært være pasienten, som løsningen inneholder helseopplysninger om. Helsepersonell som dokumenterer og har tilgang til helseopplysninger om pasienten kan også i enkelte tilfeller være den "registrerte", men opplysningene er da å betrakte som personopplysninger. Uavhengig av konsept må det legges til rette for å ha gode rutiner for å oppfylle den registrertes rettigheter.

I dette kapittelet vurderes noen av de mest sentrale rettighetene som må ivaretas i alle konseptene. Den registrerte er imidlertid gitt flere rettigheter etter EUs personvernforordning som vi vil se nærmere på i det videre arbeidet med valgte konseptet, eksempelvis retten til begrensning av behandling, rett til ikke å bli utsatt for automatiserte individuelle avgjørelser, herunder profilering.

8.2 Rett til informasjon, individuelt innsyn, retting, sletting og mulighet til å sperre

Informasjon
Den registrerte har rett på generell informasjon om hvem som behandler helseopplysninger, hvilke opplysninger det gjelder og hvordan de behandles, jf. forordningen art. 13 og art. 14. Informasjon er en grunnleggende rettighet for den registrerte. Informasjon som gis skal gjøre den registrerte i stand til å forstå om og hvordan egne person/helseopplysninger blir behandlet og hvilke konsekvenser det har. Dersom den registrerte ikke får nok informasjon vil det ikke være mulig å ivareta egne interesser og andre rettigheter. Det er et krav etter forordningen at informasjonen skal være skriftlig og helst elektronisk og i et klart språk tilpasset målgruppen.

Individuelt innsyn

Videre har den registrerte også en rett til individuelt innsyn i opplysninger som er registrert om dem selv og dette er regulert generelt i forordningen art. 15.

At pasienten har rett til informasjon og innsyn i egne helseopplysninger og hvem som har hatt tilgang til opplysningene, er også spesialregulert, jf. pasientjournalloven § 18. Retten til innsyn bygger her på innsyn i pasient- og brukerrettighetsloven og helsepersonelloven, og gir grunnlag for å helt eller delvis avvise kravet om innsyn ut fra faglige vurderinger. Løsningen må derfor ivareta muligheten til å nekte innsyn i opplysninger i journalen dersom dette er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står vedkommende nær. Pasienten har også rett til informasjon og innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer. Innsynsretten gjelder alle tilfeller der noen har lest, søkt eller på annen måte tilegnet seg, brukt eller besittet helseopplysninger fra behandlingsrettede helseregistre, enten dette er rettmessig eller ikke.

Rett til retting/korrigering
Den registrerte har rett til å få uriktige opplysninger om seg korrigert så snart som mulig/uten ugrunnet opphold, jf. EUs personvernforordning art 16.

Etter helselovgivningen har pasienten rett til å kreve retting i pasientjournalen, jf. pasient- og brukerrettighetsloven § 5-3. Helsepersonellet som har ført journalen skal vurdere kravet konkret, jf. helsepersonelloven § 42 og § 43, og skal rette eller slette opplysninger dersom vilkårene for dette er til stede. I distribuerte løsninger må dette gjøres i den enkelte løsning som inneholder informasjon, og det må også gjøres i de systemene som kan ha mottatt kopier av denne informasjonen.

Rett til sletting
Den registrerte har i visse tilfeller rett til å få opplysninger om seg selv slettet. I EUs personvernforordning art 17 omtales dette som "retten til å bli glemt", og oppstiller i hvilke tilfeller det er aktuelt.

Pasienten har rett til å kreve sletting i pasientjournalen, jf. pasient- og brukerrettighetsloven § 5-3. Helsepersonellet som har ført journalen skal vurdere kravet konkret, jf. helsepersonelloven § 42 og § 43, og skal rette eller slette opplysninger dersom vilkårene for dette er til stede. I distribuerte løsninger må dette gjøres i den enkelte løsning som inneholder informasjon, og det må også gjøres i de systemene som kan ha mottatt kopier av denne informasjonen.

Retten til å bli glemt, i form av at behandlingsansvarlig skal slette informasjon om den registrerte, vil ikke gjøre seg gjeldende som sådan, men vil styres av helselovgivningens regler som omtalt ovenfor.

Rett til å motsette seg behandling av helseopplysninger
Pasienten har en rett til å motsette seg at helseopplysninger gis videre til annet personell, jf. pasientjournalloven § 17. Opplysningene kan heller ikke tilgjengeliggjøres eller utleveres dersom det er grunn til å tro at pasienten ville motsette seg det ved forespørsel. Løsningen som velges må kunne ivareta at bestemte deler eller hele journalen enkelt og effektivt kan

gjøres utilgjengelig for enkeltpersoner, grupper av helsepersonell eller helsepersonell i virksomheten der helseopplysningene er nedtegnet i journalen. Det kan være slik at pasienter som har sperret opplysninger, ikke har forutsett alle situasjoner som vil kunne oppstå, eller at årsaken til at de i utgangspunktet ønsket sperring, ikke er der lenger. Løsningen må åpne for at opplysningene allikevel tilgjengeliggjøres dersom tungtveiende private eller offentlige hensyn som fare for liv og helse, gjør det rettmessig å gi opplysningene videre.

8.3 Vurdering av konseptene

Det legges til grunn at alle konseptene vil kunne ivareta den registrertes rettigheter, men at konseptene i ulik grad muliggjør hvor helhetlig og effektivt dette kan håndteres. Hvordan dette skal ivaretas må vurderes nærmere for valgt konsept og ved planlegging og utformingen av løsningene. Det er ikke beskrevet hvordan dette kan håndteres i samhandlingsløsningen.

Konsept 7 innebærer at det etableres en nasjonal journalløsning med en tydelig dataansvarlig. Konseptet vil dermed muliggjøre en helhetlig og effektiv håndtering av rettigheter, herunder retten til individuelt innsyn og retten til å motsette seg behandling av helseopplysninger. På den måten vil den registrerte kunne få bedre muligheter til å gjøre sine rettigheter gjeldende, til medvirkning og til å få kontroll med behandlingen av helseopplysninger i journal. En utfordring med sentral håndtering av rettigheter er å håndtere krav fra den registrerte som krever helsefaglig kompetanse. Det er ikke sikkert at en sentral dataansvarlig har nødvendig kjennskap til faglige grunner for å vurdere dette, da det trolig best kan skje av helsepersonell i virksomheten som behandlet pasienten. Det er derfor trolig behov for en to-delt håndtering av dette, slik at helsepersonellet kan vurdere om innsyn kan gis, og deretter overlate til den sentrale dataansvarlige å tilgjengeliggjøre helseopplysningene for den registrerte. Dette er en utfordring som vil måtte håndteres i løsningen. Tilsvarende utfordring er håndtert for Nasjonal kjernejournal. Dette er nærmere omtalt i kapittel 7.3. Videre vil konsept 7 kunne berøre innbyggers mulighet til å starte med "blanke ark" hos en ny behandler. I dag er det i stor grad opp til pasienten å videreformidle om vedkommende har fått helsehjelp tidligere. I én nasjonal journalløsning vil større antall helsepersonell kunne ha tilgang til helseopplysningene. Dette vil kunne berøre pasientens muligheter til å få ny vurdering uten at helsepersonellet har tilgjengelig tidligere helseopplysninger. Det vil derfor kunne være sentralt at den registrerte på en enkel måte f. eks kan motsette seg behandling av helseopplysninger (sperre).

Konsept 1, som i stor grad viderefører dagens situasjon, gir ikke samme muligheter for helhetlig håndtering av rettigheter. Dette vil kreve koordinering og gode rutiner mellom mange dataansvarlige og samhandlingsløsningen. Det vil trolig både være nødvendig å gi den registrerte informasjon både via en nasjonal samhandlingsløsning og fra den enkelte virksomheten om hvor og hvem som er ansvarlig for behandlingen av helseopplysningene. Det kan eventuelt legges opp til at den nasjonale samhandlingsløsningen kan være en felles inngang for å ta imot innbyggerhenvendelser. Manglende informasjon og individuelt innsyn vil kunne medføre at det er utfordrende for innbygger å få gjort gjeldende sine øvrige rettigheter, f. eks. retten til retting, sletting og til å motsette seg behandling av helseopplysninger. Det blir for eksempel viktig å gi informasjon om hvor og hvordan den registrerte kan henvende seg for å gjøre sine øvrige rettigheter gjeldende all den tid det er

flere virksomheter og dataansvarlige å forholde seg til. Videre vil det kunne være mer krevende å bygge inn den registreres rettigheter i konsept 1, som i motsetning til de øvrige konseptene, innebærer videreutvikling av eksisterende systemer.

Konsept 4 innebærer også en videreføring av dagens ansvarsforhold og lokal/felles journaler, men med den forskjellen at virksomhetene tar i bruk nye journalløsninger. De gamle journalløsningene fases ut. Det innebærer at håndtering av innbyggers personvernrettigheter i større grad kan bygges inn i løsningen og etablere grensesnitt mot helsenorge.no-plattformen. Dette vil igjen kunne medføre at rettighetene blir mer tilgjengelige og kunne håndteres mer effektiv enn i dag, og det som er mulig i konsept 1.

9 Videre arbeid

Konseptet som velges vil måtte realiseres i overensstemmelse med personvernregelverket som gjelder på tidspunktet for realiseringen av tiltaket.

Det vil være nødvendig å utrede nærmere behov for rettslige endringer for å etablere rettsgrunnlag for løsningene/behandlingene i det konseptet som velges. I tillegg vil det være nødvendig å utrede behovet for ytterligere rettslige endringer, blant annet for å kunne pålegge virksomheter å ta i bruk løsningen eller eventuelt å etablere grunnlag for bruk av helseopplysninger til beslutningsstøtte og kvalitetsforbedring. Det vil også måtte avklares hvilken virksomhet som eventuelt skal utpekes som dataansvarlig for nye nasjonale løsninger i lov eller forskrift. Regelverksutvikling må inngå som en del av prosjektgjennomføringen og eventuelt sees som en prosjektrisiko.

Det er grunn til å tro at konseptene vil komme inn under kravet om Data Protection Impact assessment (DPIA) i EUs personvernforordning artikkel 35. Når valg av konsept er gjort, og teknisk løsning er utformet på et tilstrekkelig detaljert nivå, vil det derfor måtte gjennomføres en fullverdig personvernkonsekvensvurdering etter EUs personvernforordning.

Videre vil det måtte gjøres mer inngående juridiske vurderinger i forprosjektet knyttet til bl.a. konkurranseregelverket, sikkerhetsloven og helselovgivningen. Det vil bl.a. måtte gjøres en vurdering av om de nasjonale løsningene er skjermingsverdige informasjonssystemer i henhold til ny sikkerhetslov.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO