Direktoratet for e-helse

Sentralt styringsdokument

Steg 2 for digital samhandling

Bilag I1 Overordnet personvernvurdering for målbildet for helhetlig samhandling

IE-1087

Publikasjonens tittel:
Sentralt styringsdokument
Steg 2 for digital samhandling

Bilag I1 Overordnet personvernvurdering
for målbildet for helhetlig samhandling

Rapportnummer
E-1087

Utgitt:
Januar 2022

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

Innhold

Sammendrag

Direktoratet for e-helse har i samarbeid med sektor beskrevet et målbilde for helhetlig samhandling som gir en visjon for fremtiden og som beskriver samhandlingen i helse- og omsorgstjenesten frem mot 2030.

Målbildet skisserer en ny digitalisert måte å samhandle på i helse- og omsorgstjenesten. Dette reiser grunnleggende personvernspørsmål. Det er viktig å utrede disse tidlig for å sikre at samhandlingsløsningene kan etableres i henhold til regelverket og med godt personvern og informasjonssikkerhet.

Direktoratet for e-helse har derfor gjennomført en overordnet personvernvurdering av det skisserte målbildet for helhetlig samhandling (konseptet).

Under følger en oppsummering av direktoratets vurderinger av sentrale krav i regelverket:

- *Ivaretakelse av grunnleggende rettigheter.* Behandlingen av helseopplysninger i nasjonale samhandlingsløsninger vil kunne føles som et inngrep i den enkeltes privatliv. Det er derfor viktig å identifisere og gjennomføre tiltak som reduserer dette. Samtidig er det viktig å veie dette mot den enkeltes krav på tilfredsstillende helsetjenester.
- *Rettsgrunnlag for behandling av helseopplysningene.* Det vil være behov for regelverksutvikling for å sikre rettsgrunnlag for enkelte av tjenestene som er skissert i målbildet for helhetlig samhandling. For behov for regelverksutvikling for tjenester i steg 2 vises det til nærmere omtale i vedlegg G.
- *Formålet med behandlingen av helseopplysningene.* Formålet er å sikre at relevante og nødvendige helseopplysninger om pasienten er tilgjengelige for helsepersonell ved ytelse av helsehjelp, uavhengig av hvor i landet pasienten behandles, samtidig som det er et formål at personvernet til pasientene ivaretas. Pasientjournallovens formål setter rammen for behandlingen av helseopplysningene. Formålet er knyttet til helsehjelp og deling av helseopplysninger i samhandlingsløsninger.
- *Plasseringen av dataansvaret.* Etablering av samhandlingsløsninger vil kreve en form for sentralisering av dataansvaret. Den enkelte ansvarsmodellen må avklares for de enkelte samhandlingsløsningene.
- *Ivaretakelse av den registrertes rettigheter*. Det er identifisert risiko forbundet med ivaretakelse av den registrertes rettigheter. Det vil imidlertid være mulig å redusere risikoen betydelig ved gjennomføring av ulike skisserte tiltak.

1. Innledning

Målbildet for helhetlig samhandling i helse- og omsorgstjenesten skisserer en ny digitalisert måte å samhandle på i helse- og omsorgstjenesten. Dette reiser grunnleggende personvernspørsmål.

Den sentrale loven som regulerer behandling av personopplysninger generelt sett, er lov 15. juni 2018 om behandling av personopplysninger (personopplysningsloven) som gjennomfører EUs personvernforordning av 27. april 2016. Denne omfatter også behandling av helseopplysninger. Med behandling menes her enhver aktivitet knyttet til opplysningene, som for eksempel innsamling, registrering, lagring, slik det er definert i EUs personvernforordning artikkel 4 nr. 2. Det påhviler den *behandlingsansvarlige* en rekke plikter. Behandlingsansvarlig er, i henhold til personvernforordningen artikkel 4 nr. 7, den virksomheten som faktisk bestemmer formålet med behandlingen av opplysningene og hvilke midler som skal brukes. I henhold til pasientjournalloven § 2 bokstav e skal begrepet forstås synonymt med *dataansvarlig*, som er det begrepet som benyttes i pasientjournalloven. Begrepene *dataansvar* og *dataansvarlig* vil derfor bli benyttet i det videre.

I henhold til forordningen skal personopplysninger behandles i tråd med en rekke prinsipper, og de registrerte har en rekke rettigheter som den dataansvarlige ivareta. Blant annet skal den dataansvarlige 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, tilgjengelighet og robusthet. Den dataansvarlige skal videre anvende prinsippene om innebygd personvern.

Det er viktig å kartlegge og utrede personvernspørsmålene tidlig for å sikre at løsningene kan etableres i henhold til regelverket og med innebygd personvern og tilstrekkelig informasjonssikkerhet. Det ble allerede i utredningen av *Én innbygger - én journal*[1], *Konseptvalgutredning Nasjonal løsning for kommunal helse- og omsorgstjeneste*[2] og *Sentralt styringsdokument Akson: Helhetlig samhandling og felles kommunal journalløsning*[3], gjennomført overordnede personvernvurderinger. Dette dokumentet bygger videre på de tidligere personvernvurderingene og beskriver en vurdering av personvern med fokus på arbeidet i Program digital samhandling (PDS) og det skisserte målbildet for helhetlig samhandling. Vurderingene er på et overordnet nivå og basert på konseptskisser. Den nærmere etterlevelsen av personvernkravene må skje i utviklingen av løsningene.

Vurderingen starter med en kort beskrivelse av målbildet for digital samhandling og deretter vurderes løsningene opp mot følgende sentrale krav i regelverket:

- grunnleggende rettigheter
- personvernprinsippene med særlig fokus på rettsgrunnlag, formålsbegrensning og ansvarlighet (dataansvar)

[1] Helse- og omsorgsdepartementet, *Meld. St. 9 (2012-2013) Én innbygger - én journal*, 2012.
[2] Direktoratet for e-helse, *Konseptvalgutredning Nasjonal løsning for kommunal helse- og omsorgstjeneste*, 2018
[3] Direktoratet for e-helse, *Sentralt styringsdokument Akson: Helhetlig samhandling og felles kommunal journalløsning*, 2020

- den registrertes rettigheter

Krav om sikkerhet i behandlingen av helseopplysningene vil ikke bli behandlet i dette dokumentet. Det er gjort en egen overordnet risiko og sårbarhetsvurdering (ROS) som er beskrevet i bilag J2. Videre vil ikke krav om innebygd personvern bli behandlet i dette dokumentet. Det vises til omtalen av dette i vedlegg I *Strategi for informasjonssikkerhet og personvern* (prinsipp 3).

Denne personvernvurderingen, sammen med den overordnede risiko- og sårbarhetsvurderingen, se bilag J2, er underlag i det videre arbeidet med sikkerhet og personvern knyttet til helhetlig samhandling. Personvernvurderingen vil kunne være et underlag i det videre arbeidet med personvernkonsekvensvurderinger. I EUs personvernvurdering artikkel 35 nr. 1. stilles det krav om at dataansvarlig må gjøre en personvernkonsekvensvurdering (DPIA) ved behandling av personopplysninger som vil medføre en høy risiko for fysiske personers rettigheter og friheter. Det vil trolig i det videre arbeidet med å etablere samhandlingsløsninger behov for å gjennomføre flere DPIA etter EUs personvernforordning blant annet fordi det skal behandles særlig kategorier av personopplysninger (helseopplysninger) og på grunn av omfanget av behandlingen. Det er naturlig at Norsk helsenett SF gjennomfører DPIA i det videre arbeidet med samhandlingsløsningene.

1.1. Forutsetninger og avgrensninger

Det gjøres følgende forutsetninger:

- At vurderingen knyttes til det skisserte målbildet for helhetlig samhandling (omtalt under). Det omfatter nye samhandlingsløsninger, bl.a. ulike typer nye nasjonale informasjonstjenester og komponenter som skal understøtte samhandlingen. Det innebærer at det omfatter både steg 1, steg 2 og fremtidige steg i arbeidet med målbildet om digital samhandling.
- At Helse- og omsorgsdepartementet gjennomfører regelverksarbeid for å sikre nødvendig rettsgrunnlag for behandlingen av helseopplysningene i nye samhandlingsløsninger. Departementet har allerede igangsatt et lovarbeid som er den rettslige oppfølgingen av Én innbygger – én journal.
- At Norsk helsenett tar ansvar for å ivareta personvernet og informasjonssikkerheten i nye samhandlingsløsninger. Det omfatter å gjennomføre personvernkonsekvensvurdering (DPIA) for de enkelte løsningene.

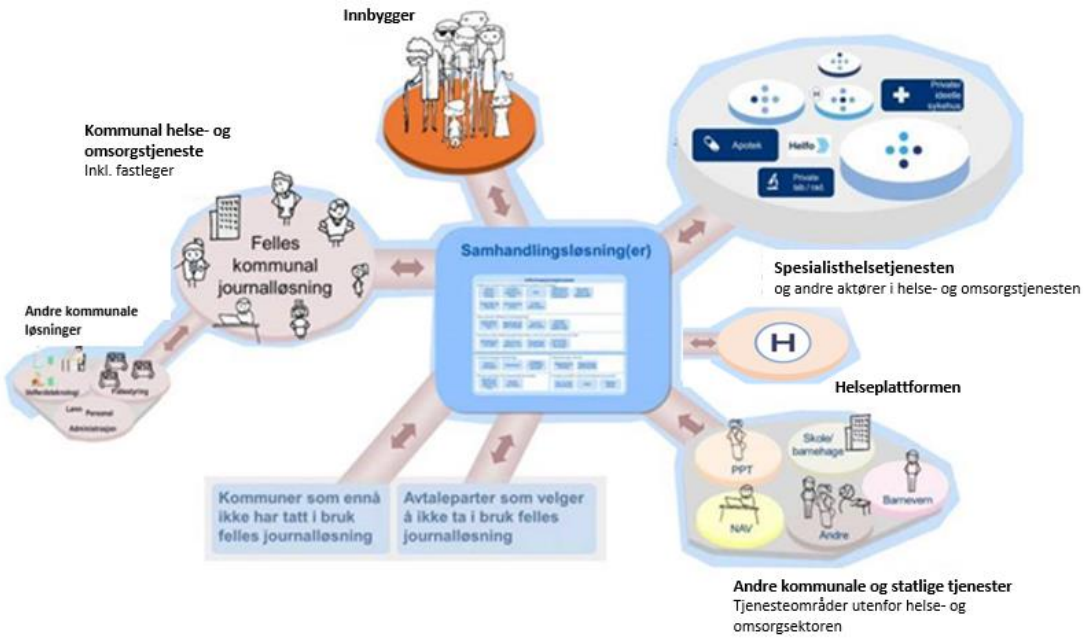
Det gjøres følgende avgrensinger:

- Vurderingen omhandler ikke Felles kommunal journal.
- Vurderingen omhandler ikke eksisterende nasjonale samhandlingsløsninger fordi det legges til grunn at personvernspørsmål allerede er utredet. Dette gjelder e-reseptkjeden, kjernejournal, Helsenorge og helsenettet.
- Vurderingen er ikke en fullverdig personvernkonsekvensvurdering etter EUs personvernforordning (DPIA). Det vil være behov for at Norsk helsenett gjennomfører DPIA knyttet til de enkelte løsningene så snart informasjonsgrunnlaget er tilstrekkelig.

1.2. Konseptbeskrivelse

Direktoratet for e-helse har i samarbeid med sektor beskrevet et målbilde for helhetlig samhandling som gir en visjon for fremtiden, og som beskriver samhandlingen i helse- og omsorgstjenesten frem mot 2030. Program digital samhandling bruker målbildet som styringsverktøy for å vise retningen. Målbildet består av ulike løsninger som muliggjør samhandling, som programmet tar sikte på å realisere innen 2030 for å understøtte ytelse av helse- og omsorgshjelp. Dette inkluderer å sikre kontinuitet i direkte helsehjelp, for eksempel når innbygger beveger seg mellom ulike virksomheter eller skrives ut fra sykehus, og å sikre samhandling med responssenter med velferdsteknologiske utstyr og digital hjemmeoppfølging.

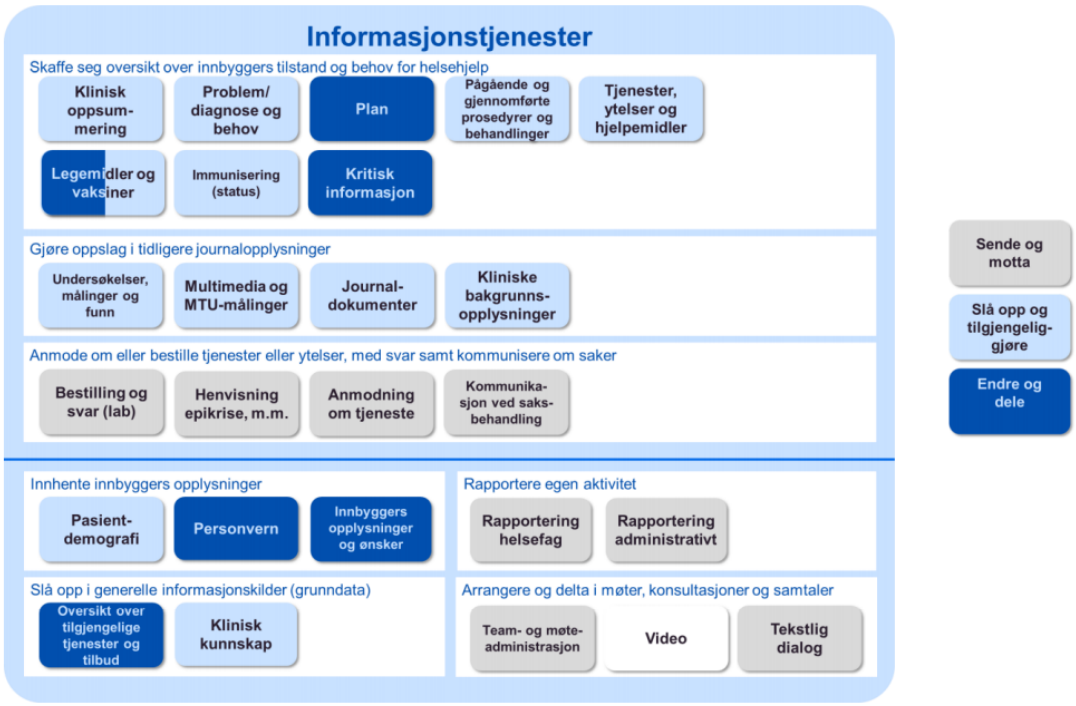
Målbildet for helhetlig samhandling er å etablere en helhetlig samhandlingsløsning som sikrer samhandling på tvers av ulike aktører, og er bygget opp av 26 informasjonstjenester som representerer et sett av informasjonsbehov som ikke er tilstrekkelig dekket i dagens nasjonale e-helseløsninger for samhandling. Hver informasjonstjeneste gir mulighet for å utveksle eller dele helseinformasjon mellom ulike aktører. Målbildet for helhetlig samhandling ble utarbeidet i forprosjektet til helhetlig samhandling. Nærmere informasjon om prosessen og resultatet finnes i bilag G2 *Helhetlig samhandling* til S*entralt styringsdokument– helhetlig samhandling og felles kommunal journalløsning.*



Figur 1 Aktører som samhandler gjennom felles løsninger når målbildet er realisert

En informasjonstjeneste definerer et utvalg av informasjon som kan deles. Informasjonen kan deles ved hjelp av de ulike organisatoriske samhandlingsformene "sende og motta", "slå opp og tilgjengeliggjøre" og "endre og dele". Disse beskrives nærmere senere i kapittelet. Informasjonstjeneste og samhandlingsform er vist i figuren nedenfor. Informasjonsinnhold for

hver informasjonstjeneste må defineres med utgangspunkt i internasjonale standarder, terminologi og kodeverk, med tilhørende tekniske grensesnitt (API).



Figur 2 Informasjonstjenester for helhetlig samhandling

Aktivitetene som vises i målbildet gjenspeiler aktivitetene helsepersonell gjennomfører når de tar mot, gjennomfører behandling, planlegger videre behandling og oppsummerer behandlingen. Informasjonstjenestene understøtter aktivitetenes behov for informasjon:

- **Skaffe seg oversikt over innbyggers tilstand og behov for helsehjelp:** Informasjonstjenestene i denne kategorien benytter helsearbeiderne til å få oversikt over hvem innbyggeren er og kritisk informasjon om innbyggerens helse. Eks. på dette er å få oversikt over evt. legemiddelallergier.
- **Gjøre oppslag i tidligere journalopplysninger:** Informasjonstjenesten gir helsepersonell muligheten til å grave seg dypere ned i innbyggerens sykdoms- og undersøkelseshistorikk fra tidligere besøk i helsetjenesten. Eks. hvis fastende langtidsblodsukker blir målt kan helsepersonell gå inn å journalen og få resultater fra tidligere tester som dagens resultater kan sammenlignes med.
- **Anmode om eller bestille tjenester eller ytelser, med svar samt kommunisere om saker:** Informasjonstjenestene tilrettelegger for samhandling innad i helsetjenesten og med aktører utenfor. Det kan være bestilling av nye prøver eller svar på prøver som er gjennomført, eller anmodning om tjenester fra evt. andre aktører som f.eks. samhandling med nav når innbygger skal sykemeldes. sykemelding til NAV.
- **Innhente innbyggers opplysninger:** Informasjonstjenestene tilbyr informasjon om innbyggeren som f.eks. foreldreansvar og behov for tolk som helsepersonell kan bruke i samhandling med andre aktører for å dekke innbyggernes behov best mulig.

Eks. Identifisere hvorvidt innbyggere som blir akuttinnlagt har foreldreansvar og det er behov for å iverksette tiltak for å ivareta barn.

- **Slå opp i generelle informasjonskilder (grunndata):** Grunndatatjenesten tilbyr informasjon om hvilke tjenester som er tilgjengelig i kommunen innbyggeren bor i samt at den tilbyr klinisk fagkunnskap.
- **Rapportere om aktivitet:** Informasjonstjenestene som benyttes for å rapportere om aktivitet til Helfo for refusjon og rapportering av medisinske data til registre slik at den blir tilgjengelig for bla. Forskning.
- **Arrangere og delta i møter, konsultasjoner og samtaler:** Informasjonstjenestene gir helsepersonell muligheten til å samhandle digitalt for å utveksle informasjon med annet helsepersonell og innbyggere.

Målbildet for helhetlig samhandling er beskrevet nærmere i vedlegg M.

2. Grunnleggende rettigheter

Beskyttelse av personvernet er anerkjent som en menneskerettighet. Dette slås fast både i den europeiske menneskerettskonvensjon artikkel 8 og i Grunnloven § 102.

Etter FNs konvensjon om økonomiske, sosiale og kulturelle rettigheter artikkel 12 er staten samtidig forpliktet til å treffe tiltak for å sørge for at borgernes fysiske og psykiske helsestandard er så høy som mulig.

I fortalen til personvernforordningen i punkt 4 angis følgende:

> "*Behandling av personopplysninger bør ha som formål å tjene menneskeheten. Retten til vern av personopplysninger er ikke en absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet*."

Dette innebærer da at de personvernmessige ulempene ved bruk av helseopplysninger må vurderes opp mot statens plikt til å sikre en god helsestandard. Pasientsikkerhet og kvalitet i pasientbehandlingen forutsetter at helsepersonell (med flere) har anledning til å behandle, og har tilgang til, nødvendige og relevante helseopplysninger. Hensynet til den enkeltes personvern og hensynet til pasientsikkerhet og kvalitet i den helsehjelp som ytes, må derfor veies mot hverandre i samsvar med forholdsmessighetsprinsippet.

En slik avveining er allerede, på et overordnet nivå, foretatt gjennom kravene i personvernforordningen og i helselovgivningen. Personvernforordningen oppstiller en rekke prinsipper som behandling av personopplysninger skal skje i samsvar med. Helseopplysninger omfattes også av disse, for de tilfeller der det er adgang til å behandle helseopplysninger. Prinsippene er basert på tanken om at behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltpersoner. Helselovgivningen oppstiller i tillegg krav som skal ivareta pasientsikkerhet og kvalitet i helsehjelpen som ytes.

Etter EUs personvernforordning er det også krav om at det skal gjøres en vurdering av den registrertes friheter etter europeiske menneskerettskonvensjon, f. eks retten til tanke, tros- og religionsfrihet, retten til ikke å bli diskriminert, ytrings- og informasjonsfrihet og retten til

privatliv og kommunikasjonsvern. Retten til privatliv innebærer blant annet en rett til personopplysningsvern. Den enkelte skal i så stor grad som mulig ha selvbestemmelse og kontroll med egne opplysninger. Det vil samhandlingsløsninger behandles helseopplysninger basert på helselovgivningen, der pasienten har begrenset grad har mulighet til å motsette seg behandlingen. Pasienten kan ikke motsette seg at helsepersonellet fører journal. For å ivareta pasientens mulighet for selvbestemmelse og kontroll er pasienten imidlertid gitt en rekke rettigheter i helselovgivningen, for eksempel rett til å sperre, innsyn, retting, sletting mv.

Det er naturlig å tenke seg at aktive pasienter og brukere som utøver egne rettigheter og har god informasjon om behandlingen som skjer i de nasjonale tjenestene, vil kunne føle at de har større grad av selvbestemmelse og kontroll over deling av egne helseopplysninger. Det skal tilrettelegge for dette, og det er derfor et absolutt krav at personvernet skal styrkes. Det skal identifiseres og gjennomføre tiltak som kan gi pasienten medbestemmelse og kontroll der det er mulig. Videre må det settes inn ulike tiltak for å sikre tillitt til løsningen som sådan, og særlig at sikkerheten er godt ivaretatt. Det må bl.a. være gode mekanismer for identitets- og tilgangsstyring for å sikre at kun helsepersonell med tjenstlig behov og innenfor regler om taushetsplikt får tilgjengeliggjort helseopplysningene. En annen viktig ting er at det skal være enkelt å utøve sine rettigheter som det å sperre mv. Dette skal løses med gode personverntjenester for innbygger og enkel utøvelse av rettigheter for eksempel via helsenorge.no. Blant annet vil pasienten i større grad kunne få en helhetlig oversikt over egne helseopplysninger, noe som vil gi pasienten en større grad av kontroll over hvor deres opplysninger behandles slik at de kan utøve sine rettigheter. De enkelte rettighetene er omtalt nedenfor i kapittel 4.

3. Personvernprinsipper

EUs personvernforordning artikkel 5 oppstiller syv personvernprinsipper. All behandling av personopplysninger må skje i samsvar med disse. Prinsippene er basert på tanken om at behandling av personopplysninger skal skje på en måte som sikrer forutsigbarhet og forholdsmessighet for enkeltpersoner.

I dette kapitlet gjøres en overordnet vurdering av det enkelte prinsipp opp mot det skisserte målbildet for helhetlig samhandling. Vurderingen viser at enkelte av prinsippene vil kunne bli utfordret, men at det er mulig å redusere risikoen betydelig ved ulike tiltak. Begge deler er omtalt under. Det forutsettes imidlertid at det gjennomføres en fullverdig personvernkonsekvensvurdering (DPIA) konkret for den enkelte tjeneste.

3.1. Lovlighet, rettferdighet og åpenhet

Krav til behandlingsgrunnlag

EUs personvernforordning artikkel 5 nr.1 bokstav a stiller krav om at personopplysninger skal behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte.

Målbildet for helhetlig samhandling er beskrevet som nasjonale løsninger for behandling av helseopplysninger ved helsehjelp til den enkelte pasient. Det legges til grunn at behandlingen av helseopplysningene som utgangspunkt omfattes av formålet med pasientjournalloven, jf. § 1. 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.

Dette innebærer at behandling av helseopplysninger i nye samhandlingstjenester må ha et tydelig rettslig grunnlag. Dette må vurderes konkret for hver av samhandlingsløsningene hvorvidt det foreligger et tilstrekkelig rettslig grunnlag. Eksisterende samhandlingsløsninger som reseptformidleren og kjernejournal har allerede rettsgrunnlag.

Kravet til lovlighet innebærer også at alle de øvrige personvernprinsippene er oppfylt, og at behandlingen for øvrig er i tråd med krav etter regelverket.

Gjeldende rett

Den viktigste særloven som regulerer journalopplysninger er pasientjournalloven, som blant annet gir det rettslige behandlingsgrunnlaget for pasientjournaler. I tillegg omfatter helsepersonelloven og pasient- og brukerrettighetsloven bestemmelser knyttet til den enkeltes personvern. Bestemmelsene i særlovgivningen til dels gjentar eller direkte viser til sentrale bestemmelser i forordningen, eller presiserer krav til behandling av helseopplysninger. De generelle reglene i forordningen gjelder dermed så langt ikke annet følger av helselovgivningen.

Formålet med pasientjournalloven er at behandlingen av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet. Dette skal skje ved at relevante og nødvendige opplysninger om pasienten og helsehjelpen nedtegnes/registreres i en journal for den enkelte pasient. Opplysningene skal være tilgjengelige for annet helsepersonell som har behov for dem ved ytelse av helsehjelp til pasienten. Samtidig skal vernet mot at opplysninger gis til uvedkommende ivaretas, jf. rett til vern mot spredning av opplysninger (pasient- og brukerrettighetsloven § 3-6), jf. taushetsplikt (helsepersonelloven § 21 flg.), og forbud mot urettmessig tilegnelse av helseopplysninger (helsepersonelloven § 21 a).

Det er ikke krav om pasientens samtykke for at helsepersonellet kan nedtegne og lagre journalopplysninger. Tvert imot, har helsepersonell som yter helsehjelp plikt til å nedtegne opplysninger som anses som relevante og nødvendige for helsehjelpen til den enkelte pasient, samt opplysninger som er nødvendig for å oppfylle melde- eller opplysningsplikter som er fastsatt i lov, jf. helsepersonelloven §§ 39 og 40. 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 og pasient- og brukerrettighetsloven § 5-3.

Pasientjournalloven pålegger virksomheter som yter helsehjelp å sørge for å ha behandlingsrettede helseregistre for gjennomføring av helsepersonells dokumentasjonsplikt, jf. § 8. Systemene skal innrettes slik at helsepersonell kan utføre sine lovpålagte oppgaver og ansvar overfor pasientene.

Pasientjournalloven gir rettslig grunnlag for etablering av behandlingsrettede helseregistre, jf. § 2. Behandlingsrettede helseregistre har sammenheng med dokumentasjonsplikten og omfatter all behandling av helseopplysninger som er nødvendige for at helsehjelp kan ytes. Behandlingsrettede helseregistre har et utfyllende rettslig grunnlag i pasientjournalloven og andre lover og forskrifter. Bestemmelsene setter strenge vilkår for å samle inn og på annen måte behandle helseopplysninger, samtidig som det er bestemmelser for å ivareta den enkeltes selvbestemmelse og kontroll over egne helseopplysninger og hvordan de behandles. Ved innføring av EUs personvernforordning i norsk rett har Helse- og

omsorgsdepartementet vurdert at det ikke er behov for endringer i helselovgivningen for å oppfylle kravene til rettslig grunnlag for pasientjournaler.

Pasientjournalloven regulerer ulike behandlingsrettede helseregistre. Av § 6 fremgår det at behandlingsrettede helseregistre 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 lette 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 helseregistre, alle systemene som utgjør hele pasientjournalen eller kun registre på bestemte områder. Registre som inngår i samarbeidet, skal komme i stedet for de registrene som virksomhetene bruker internt i virksomheten. 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 pasient og brukere i hele landet og ikke begrenses til en bestemt region. Bestemmelsen gir hjemmel for behandlingsrettede helseregistre på bestemte områder, som for eksempel legemiddelregister eller epikriseregister. Register vedtatt med hjemmel i denne bestemmelsen skal komme i stedet for virksomhetsinterne journaler eller felles journaler basert på samarbeid mellom virksomheter som hjemles i §§ 8 og 9.

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

Videre gir pasientjournalloven rettslig grunnlag for deling av opplysninger med helsepersonell og samarbeidende personell når det er nødvendig for å kunne gi helsehjelp, jf. § 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. Dette kan skje både ved at helsepersonellet gis adgang til å søke opp de aktuelle opplysningene i systemet, eller ved at opplysningene gjøres tilgjengelig ved at de utleveres elektronisk eller på papir. Journalopplysninger kan som hovedregel ikke gjøres tilgjengelig for annet helsepersonell dersom pasienten motsetter seg det, jf. pasientjournalloven § 17. Opplysningene skal gjøres tilgjengelig på en måte som ivaretar informasjonssikkerheten, jf. lovens § 22. Videre stiller pasientjournalforskriften § 13 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 § 12 tredje ledd. Tilgang til helseopplysninger skal bygge bl.a. på autorisasjon, sikker autentisering og etterfølgende kontroll, jf. pasientjournalforskriften §§ 13 og 14.

Behov for regelverksendringer

I konseptvalgsutredningen og sentralt styringsdokument for Akson[4] ble det gjort vurderinger av hvorvidt det forelå rettslig grunnlag for felles kommunal journal og samhandlingsløsninger. Pasientjournalloven regulerer ulike behandlingsrettede helseregistre og samhandlingsformer. På bakgrunn av beskrivelsene som forelå på det tidspunktet ble det vurdert at det totale konseptet ville kreve endringer i pasientjournalloven.

Det legges derfor til grunn at det må påregnes at det vil være nødvendig å gjøre endringer i regelverket for å kunne realisere målbildet for helthetlig samhandling. Eksisterende nasjonale e-helseløsninger, og det rettslige grunnlaget disse bygger på, vil neppe være tilstrekkelig for å oppnå hele dette målbildet. Realiseringen av målbildet innebærer trolig at det må etableres både spesifikke tjenester og felleskomponenter, som gjør det mulig å tilgjengeliggjøre og sammenstille relevante helseopplysninger, utover det som det er rom for i dagens nasjonale e-helseløsninger. Dette vil trolig kreve lovendring. Det må blant annet legges til grunn at tjenester som skal basere seg på sentral lagring av kopisett, vil kreve særskilt rettsgrunnlag.

Ved utvikling av regelverket bør informasjonstjenestene, infrastrukturen og verktøyene som må til for å realisere målbildet, sees i sammenheng, fremfor at enkelttjenester og verktøy reguleres hver for seg. For å ivareta helheten er det en fordel om fremtidige lovbestemmelser som skal etablere det rettslige grunnlaget for målbildet helhetlig digital samhandling kan utformes som funksjonsorienterte og teknologinøytrale rammebestemmelser som tar høyde for fremtidig utvikling. Slike rammebestemmelser vil kunne være digitaliseringsvennlige og fullt ut forsvarlig, forutsatt at de er godt utredet, slik at det sikrer den nødvendige forutberegnelighet for lovgiver. Dette vil skape den nødvendige fleksibilitet for en smidig tilnærming ved utvikling av de løsninger som er nødvendige for å nå målbildet.

Helse- og omsorgsdepartementet har hatt på høring forslag til endringer i pasientjournalloven, som blant annet har til formål å etablere det rettslige grunnlaget for visjonen om *Én innbygger – én journal*[5]. Det legges for øvrig til grunn at Helse- og omsorgsdepartementet vil vurdere behovet for ytterligere endringer blant annet på grunnlag av innspill fra Direktoratet for e-helse.

3.2. Åpen og rettferdig behandling

Hvis behandlingen skal være åpen og rettferdig, betyr det at behandlingen skal skje på en måte som er oversiktlig og forutsigbar for den registrerte, slik at den registrerte er i stand til å ivareta sine egne interesser og utøve sine rettigheter. Kompleksiteten i målbildet for digital samhandling kan gjøre at prinsippet om åpenhet og rettferdighet utfordres. Samhandlingsløsningene består av mange ulike informasjonstjenester, med ulike

[4] Direktoratet for e-helse, *Konseptvalgutredning Nasjonal løsning for kommunal helse- og omsorgstjeneste*, 2018

[5] Helse- og omsorgsdepartementet, *Meld. St. 9 (2012-2013) Én innbygger - én journal*, 2012.

samhandlingsformer og komponenter, som skal understøtte samhandlingen. Det kan derfor være krevende og uforutsigbart for innbygger å forstå hvordan helseopplysningene tilgjengeliggjøres eller hvordan egne rettigheter skal ivaretas på tvers av disse løsningene. På den annen gir samhandlingsløsninger og målbildet mulighet for en mer helhetlig og effektiv håndtering av rettigheter, herunder å gi pasienten individuelt innsyn, enn dagens desentraliserte journalløsninger.

For å ivareta prinsippet om åpen og rettferdig behandling, vil det blant annet være viktig med en god kommunikasjonsstrategi for å gi pasienter og brukere informasjon om løsningene, hvordan behandlingen av helseopplysninger foregår og om ivaretakelse av egne rettigheter.

Det forutsettes at det etableres gode og lett tilgjengelige innbyggertjenester som gjør det enkelt for pasient og bruker å ta kontakt for å få mer informasjon, innsyn i egne helseopplysninger og utøve sine øvrige rettigheter.

3.3. Formålsbegrensning

All behandling av personopplysninger skal skje innenfor et formål. Et grunnleggende prinsipp som følger av EUs personvernforordning artikkel 5 nr.1 bokstav b, er at personopplysninger bare skal behandles til spesifikke, uttrykkelig angitte og berettigede formål, dvs. prinsippet om formålsbegrensning. 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.

Det må avklares hvilket formål behandlingen av helseopplysningene i målbildet for digital samhandling skal ha og hvilke behov det skal dekke. Formålet som angis for behandlingen av person- og helseopplysninger i samhandlingsløsninger vil dermed være førende for hvilke opplysninger som kan samles inn og behandles.

Samhandlingsløsningene som utgjør målbildet for helhetlig samhandling, skal bidra til å realisere målbildet som er beskrevet i Meld. St. 9 (2012-2013) *Én innbygger – én journal*[6]. 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.

Formålet med samhandlingsløsningene er knyttet til helsehjelp og dreier seg om å sikre at relevante og nødvendig helseopplysninger er tilgjengelig for helsepersonell ifm. helsehjelp, uavhengig hvor pasienten behandles. Gjennom tilgang til tjenester, komponenter og infrastruktur hvor pasientopplysninger kan deles i sanntid skal det legges til rette for effektiv samhandling mellom privat, statlig og kommunal helse- og omsorgstjeneste. Med samhandling menes all form for kontakt, samarbeid, informasjonsutveksling i en virksomhet eller mellom virksomheter, som inngår i eller støtter opp under oppfølging av en pasient i et behandlingsforløp. Hensikten er at helsehjelpen kan ytes effektivt og med god kvalitet når flere aktører er involvert, ved at informasjonen følger pasienten ved kontakt mellom ulike aktører i tjenesten.

Programmet legger til grunn at behandling av helseopplysninger i samhandlingsløsninger vil ha/få rettsgrunnlag innenfor pasientjournalloven. Pasientjournallovens formål og saklige

[6] Helse- og omsorgsdepartementet, *Meld. St. 9 (2012-2013) Én innbygger - én journal*, 2012.

virkeområde setter rammen for behandlingen av helseopplysninger. Det konkrete formålet med de enkelte løsningene vil fremgå av rettsgrunnlaget til den enkelte løsningen.

Formålet med behandling av helseopplysninger i nye samhandlingsløsninger vil i hovedsak være forankret i helselovgivningen. En rettslig forankring i form av lovhjemmel og forskrift vil redusere risikoen for at det blir tvil om hva helseopplysningene skal kunne brukes til. Pasientjournalloven vil sette en ytre ramme for behandlingen av helseopplysningene, mens en ny lovhjemmel og tilhørende forskrifter vil kunne sette en enda mer konkret ramme for hvordan helseopplysningene skal behandles. Det skal kunne meldes opplysninger fra virksomhetene via samhandlingsløsninger til sekundærformål. Regelverket må tilrettelegge for dette.

Det må videre sørges for at helseopplysningene i samhandlingsløsninger faktisk og i praksis ikke brukes til andre formål enn det regelverket forutsetter. Det kan ved etablering av nye samhandlingsløsninger være behov for mer informasjon om bruken av opplysningene og formålet med disse, og at samhandlingen skal skje innenfor rammen av taushetsplikten og tjenstlig behov. Når det samles store mengder helseopplysninger vil det kunne oppstå press på å bruke opplysningene til andre formål som fører til en risiko for formålsutglidning. Dersom helseopplysningene skal brukes til andre formål uforenlig med opprinnelige formål vil det kreve rettslig endringer. Kontinuerlig bevissthet rundt, og opplæringstiltak om, kravet til formålsbegrensning er nødvendig for å bidra til å hindre formålsutglidning.

3.4. Dataminimering

EUs personvernforordning artikkel 5 nr.1 bokstav c stiller krav til at personopplysningene som skal behandles skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for. 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.

Det legges til grunn at behandlingen av helseopplysningene i nye samhandlingsløsninger reguleres i lov og forskrift. Dagens samhandlingsløsninger og bruken av helseopplysningene er regulert blant annet i pasientjournalloven §§ 12 og 13 om reseptformidleren og kjernejournal. For deling av helseopplysninger vil pasientjournalloven § 19 og helsepersonelloven blant annet §§ 25 og 45 sette rammer for hva det kan samhandles om. Dette bidrar til at prinsippet om dataminimering vil bli ivaretatt.

Videre krever det at dataansvarlig, virksomheter og helsepersonell har kunnskap om regelverkets rammer for hvilke opplysninger felles journalløsning og samhandlingsløsningene kan inneholde. Det kreves helsefaglig kompetanse å vurdere hvilke opplysninger som er relevante og nødvendige for helsehjelpen til den enkelte pasient og for at deling av helseopplysninger er i henhold til regelverket om taushetsplikt.

Der løsninger kan utformes på flere forskjellige måter, bør det tilstrebes å etablere løsninger som ikke innebærer unødig behandling av helseopplysninger og andre personopplysninger. Eksempelvis bør løsninger som innebærer tilgjengeliggjøring av opplysninger direkte fra kilden velges, fremfor mellomlagring av kopier, dersom dette kar seg gjøre uten å være uforholdsmessig krevende.

3.5. Riktighet

EUs personvernforordning artikkel 5 nr.1 bokstav d stiller krav til at personopplysninger som behandles skal være korrekte og om nødvendig oppdaterte, og at det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes.

Det er risiko for at prosessen med å få rettet og slettet helseopplysninger som lagres/behandles i felles nasjonale samhandlingstjenester kan ta tid. Dette fordi både en sentral aktør som behandler opplysningene og virksomhetene vil kunne måtte involveres. Virksomhetene er nærmest til å vurdere riktigheten av helseopplysningene, eksempelvis ved å gjøre faglige vurderinger knyttet til journalføring og krav om retting og sletting av helseopplysninger. Mens selve rettingen vil måtte skje hos den sentrale aktøren. Dette gjøres i dag for retting og sletting av helseopplysninger i kjernejournal. Dersom en slik prosess tar lang tid, vil det kunne utfordre prinsippet om riktighet.

Det må etableres gode saksbehandlingsrutiner mellom den sentrale aktøren og virksomhetene slik at kravet kan ivaretas på en god måte. Videre må det etableres gode og lett tilgjengelige innbyggertjenester som gjør det enkelt for pasient og bruker å ta kontakt for å få mer informasjon, innsyn i egne helseopplysninger og utøve sine øvrige rettigheter.

3.6. Lagringsbegrensning

EUs personvernforordning artikkel 5 nr.1 bokstav e stiller krav om at personopplysninger skal lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for. Det innebærer at opplysningene må slettes når formålet de ble samlet inn for er nådd.

Lagringstiden for helseopplysningene er og vil i stor grad være regulert. Lagringstid for helseopplysninger i journal vil, som i dag, bl.a. være forankret i pasientjournalloven og pasientjournalforskriften. Dette reduserer risikoen for at helseopplysningene brukes eller oppbevares etter at formålet er nådd. Det må sørges for at helseopplysningene faktisk og i praksis slettes når formålet er nådd.

Lagringstiden for helseopplysninger i dagens samhandlingsløsninger som f.eks. kjernejournal og reseptformidleren er regulert konkret i egne forskrifter. Det vil behov for å vurdere hvilken lagringstid som skal gjelde for behandlingen av helseopplysningene i nye samhandlingsløsninger, slik at opplysningene ikke lagres lenger enn det som er nødvendig for å ivareta formålet.

Det må derfor bygges inn slettefunksjoner i løsningene slik at helseopplysningene i størst mulig grad kan slettes automatisk når formålet er nådd. Det er i dag slike slettemekanismer i kjernejournal og reseptformidleren.

3.7. Integritet og konfidensialitet

EUs personvernforordning artikkel 5 nr.1 bokstav f stiller krav om at personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder

vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.

Kompleksiteten i målbildet om helhetlig samhandling gjør at krav om integritet og konfidensialitet vil kunne utfordres. Nye samhandlingsløsninger samler og deler stor mengde helseopplysninger og involverer mange og ulike typer helsepersonell. På den ene siden skal helsepersonellet effektivt kunne får tilgjengeliggjort helseopplysningene, mens det på den andre siden skal sikres av konfidensialiteten ivaretas. Dette vil stille store krav til identitets- og tilgangsstyring.

Det er utarbeidet en egen overordnet risiko- og sårbarhetsvurdering for programmet, se bilag J2.

Arbeidet med å vurdere prinsipper og krav til identitets- og tilgangsstyring ved deling av helseopplysninger mellom virksomheter i nye samhandlingsløsninger bør derfor starte tidlig. Det er viktig å videreutvikle tillitstjenester herunder HelseID og personverntjenester som vil bidra til å sikre tillitten mellom virksomheten som skal dele helseopplysningene. Det bør konkret vurderes om helseopplysninger og opplysninger om personidentifikasjon, som navn og personnummer, kan lagres i separate databaser.

3.8. Ansvarlighet

EUs personvernforordning artikkel 5 nr. 2 fastsetter at den dataansvarlige er ansvarlig for at personvernprinsippene overholdes, og skal kunne dokumentere dette.

Ved enhver virksomhet i helse- og omsorgstjenesten skal ansvar og oppgaver være tydelig avklart. Det er særlig tre former for ansvar som er relevant;

- Helsepersonellets individansvar etter helsepersonelloven
- Virksomhetsansvar etter spesialisthelsetjenesteloven og helse- og omsorgstjenesteloven
- Dataansvar etter personvernlovgivningen

Ved digitalisering og utvikling av målbildet for helhetlig samhandling har håndteringen av ansvaret og samspillet mellom disse ulike rollene betydning. Kompleksiteten vil kunne utfordre ansvarlighetsprinsippet og medføre risiko for uklare ansvarsforhold. Det er en omfattende løsning og den involverer svært mange og ulike typer virksomheter. Dette vil kreve at det gjøres ny vurdering av roller og ansvar ved etablering av samhandlingsløsninger. Det er sentralt at dataansvar og plikter er klart plassert, og på en måte som sikrer at informasjonssikkerheten og personvernet blir ivaretatt.

For eksisterende nasjonale samhandlingsløsninger, for eksempel kjernejournal og reseptformidleren, er dataansvaret allerede plassert.

Helsepersonellets individansvar

Det enkelte helsepersonell har ansvar for å opptre i samsvar med lovpålagte krav, først og fremst å yte forsvarlige helsetjenester jf. helsepersonelloven § 4 (forsvarlighetskravet). Arbeidsgiver har på sin side plikt til å organisere virksomheten på en måte som tilrettelegger for at helsepersonellet kan overholde sine lovpålagte plikter, jf. helsepersonelloven § 16. De lovpålagte kravene er plikter som følgelig samtidig setter rammer for arbeidsgivers

styringsrett. Kravene har derfor betydning for både utøvelse av virksomhetsansvaret og dataansvaret.

Det medisinske behandlingstilbudet er avansert og spesialisert, og det er stor grad av funksjonsdeling av oppgaver. Forsvarlighetskravet er en rettslig standard. Innholdet i normen vil blant annet være avhengig av den enkeltes faglige tilhørighet, formelle og reelle kvalifikasjoner, variasjoner i personlig erfaring og kompetanse. Krav til forsvarlighet innebærer at helsepersonellet må innrette seg etter sine faglige kvalifikasjoner og respektere begrensninger i egen kompetanse, jf. § 4 andre ledd. Det fremgår uttrykkelig av bestemmelsen at helsepersonell skal innhente bistand eller henvise pasienter videre der dette er nødvendig og mulig. Plikten til å samarbeide og samhandle med annet kvalifisert personell dersom pasientens behov tilsier dette, understrekes også. Det følger av forsvarlighetskravet at personellet har en plikt til å innhente nødvendig informasjon om pasienten før helsehjelp gis. Det må innhentes tilstrekkelig informasjon til at beslutning om og gjennomføring av hjelp etter loven kan gjøres forsvarlig.

Helsepersonells individansvar omfatter blant annet lovpålagt taushetsplikt, journalføringsplikt, plikt til å gi innsyn i journal til de som har krav på det, rett og plikt til å dele opplysninger med annet helsepersonell "når dette er nødvendig for å kunne gi forsvarlig helsehjelp", jf. helsepersonelloven §§ 39, 40, 25 og 45.

Etablering av nye pasientjournalløsninger og samhandlingstjenester vil ikke endre på plikten til forsvarlig yrkesutøvelse. Helsepersonell som yter helsehjelp, vil fortsatt ha et selvstendig ansvar for å yte forsvarlig helsehjelp.

Virksomhetsansvar

Eiere og ledere i helsetjenesten har et generelt ansvar for at tjenestenes drift gjennomføres innen lovfastsatte rammer, herunder legge til rette for at personell som utfører tjenestene blir i stand til å overholde sine lovpålagte plikter. Det vises særlig til helsepersonelloven § 16, spesialisthelsetjenesteloven § 2-2, jf. §§ 2-1e, 3-4a og 3-2, og 40 helse- og omsorgstjenesteloven § 4-1, jf. § 5-10. Virksomhetsansvaret favner videre enn dataansvaret som kun gjelder behandling av person- eller helseopplysninger.

Det følger videre av pasientjournalloven § 19, at den dataansvarlige skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Dette er et virksomhetsansvar. Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp, jf. helsepersonelloven § 25. Det er den dataansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Det er imidlertid en forutsetning at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten. Hvordan opplysninger kan gjøres tilgjengelige er altså avhengig av kvaliteten og mulighetene i ikt-systemene hos både arbeidsgiver og mottaker. Videre følger det av spesialisthelsetjenesteloven § 3-2 at helseforetak og andre helseinstitusjoner skal sørge for at journal- og informasjonssystemene ved institusjonen er forsvarlige. Tilsvarende plikt er også pålagt kommunen og virksomhet som har avtale med kommunen om å yte helse- og omsorgstjenester, jf. helse- og omsorgstjenesteloven § 5-10. Av forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten følger at den som har det

overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter, jf. forskriftens § 3.

Dataansvar

Behandling av helseopplysninger i journal må knyttes til en dataansvarlig. Dataansvaret er, som omtalt ovenfor, definert ved at ansvaret plasseres hos den virksomheten som faktisk bestemmer formålet med behandlingen av opplysningene og hvilke midler som skal brukes. Når formålet med og midlene for behandlingen er fastsatt i nasjonal rett, kan den dataansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i nasjonal rett.

Det er knyttet en rekke oppgaver og plikter til dataansvaret og det legges opp til sanksjoner når pliktene ikke overholdes. Sentrale plikter for den dataansvarlige er blant annet å sikre og dokumentere at behandlingen av opplysningene utføres i samsvar med personvernprinsippene, sikre gyldig rettsgrunnlag, etablere tekniske og organisatoriske tiltak, lage protokoll for all behandlingen av opplysningene, gjennomføre DPIA, sikre personopplysningssikkerhet, håndtere brudd på personopplysningssikkerheten og ivareta den registrertes rettigheter. Oppgavene kan delegeres, men ikke selve dataansvaret. En databehandler utfører oppgaver på vegne av og etter instruks fra dataansvarlig.

En praktisk utfordring er at mange av pliktene og rettighetene som påligger den dataansvarlige også er plikter som direkte knytter seg til selve ytelsen av helsehjelp og dokumentasjonsplikten, og som gir pasienten rettigheter knyttet til helseopplysninger om dem selv. Hvordan pliktene og rettighetene etter helselovgivningen skal ivaretas følger blant annet av helsepersonelloven og pasient- og brukerrettighetsloven. De er knyttet opp mot helsehjelpen og innebærer ofte konkrete vurderinger som gjøres av behandlende helsepersonell. Helsepersonell må for eksempel foreta en helsefaglig vurdering av om den enkelte har rett til å få rettet eller slettet opplysninger i henhold til helsepersonelloven §§ 42 og 43. Tilsvarende må det i noen særlige tilfeller gjøres helsefaglige vurderinger ved forespørsel om individuelt innsyn i helseopplysninger. Virksomheten har på sin side plikt til å sørge for å ha behandlingsrettede helseregistre for gjennomføring av helsepersonells dokumentasjonsplikt, jf. pasientjournalloven § 8.

EUs personvernforordning legger opp til ulike dataansvarsmodeller, både selvstendig dataansvar og åpner for felles dataansvar. Dataansvaret kan altså ligge til en virksomhet alene eller sammen med andre.

Helse- og omsorgsdepartementet omtaler dataansvar i høringsnotat om endringer i pasientjournalloven § 10 om nasjonal digital samhandling til beste for pasient og bruker[7]. Departementet vurderer det slik at etablering av ulike løsninger som inngår i en nasjonal datainfrastruktur tilsier at det bør gis en hjemmel til å plassere og nærmere regulere dataansvar i forskrift, herunder åpne for at dataansvaret sentraliseres til forvaltningsorganisasjoner. Samhandling mellom de ulike aktørene og komponentene, og ansvarsforholdene i samhandlingen vil da kunne reguleres. Direktoratet for e-helse deler departementets vurdering. Slike forvaltningsorganisasjoner, som departementet viser til i høringsnotatet, som har de nødvendige ressurser og spesialkompetanse innen personvern og informasjonssikkerhet, vil trolig ha de beste forutsetninger for å forvalte et dataansvar. Samme effekt vil neppe oppnås dersom slike forvaltningsorganisasjoner utelukkende opptrer

[7] Helse- og omsorgsdepartementet, *Høring om endringer i pasientjournalloven mv. - nasjonal digital samhandling til beste for pasienter og brukere*, 2021

som databehandlere uten dataansvar. I en kompleks infrastruktur vil en slik plassering av dataansvar kunne motvirke en opplevelse av ansvarspulverisering. Etter direktoratets vurdering er ansvarsplasseringen i samhandlingen i utgangspunktet klar, men erfaring viser at de ulike aktørene kan oppleve usikkerhet om ansvarsforholdene. Det kan derfor være hensiktsmessig om dataansvaret for den behandling som skjer i samhandlingen plasseres hos en sentral aktør. En slik klar ansvarsplassering vil kunne gjøre det mer forutsigbart for virksomhetene å ta i bruk samhandlingsløsningene. Direktoratet for e-helse anser det videre som viktig at det er en tydelig grense mellom dataansvaret, der dette plasseres hos en «forvaltningsorganisasjon» og det eventuelle «restansvaret» som ikke vil omfattes av dette, men forblir hos de enkelte virksomhetene. Plasseringen av dataansvaret bør vurderes konkret for den enkelte samhandlingsløsningen.

4. Ivaretakelse av personvernrettigheter

EUs personvernforordning kapittel III oppstiller alle de rettigheter den registrerte har etter personvernregelverket når personopplysninger samles inn og behandles om enkeltpersoner. 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 pasient eller bruker, som den samhandlingsløsninger inneholder helseopplysninger om. Helsepersonell som dokumenterer og deler helseopplysninger kan også i enkelte tilfeller være den registrerte, men opplysningene er da å betrakte som personopplysninger. Dette vurderes ikke nærmere her.

Dataansvarlig har plikt til å legge til rette for at pasient og brukere får oppfylt rettighetene sine på en enkel måte.

I dette kapitelet gjøres en vurdering av den registrertes rettigheter. Vurderingen viser at enkelte av prinsippene vil kunne bli utfordret, men at det er mulig å redusere risikoen betydelig ved ulike tiltak.

4.1. Rett til informasjon

EUs personvernforordning artikkel 12 til14 gir den registrerte rett til informasjon om hvordan person- og helseopplysningene behandles. Den registrerte har rett på generell informasjon om hvem som behandler helseopplysninger, hvilke opplysninger det gjelder og hvordan de behandles, jf. forordningen artikkel 13 og artikkel14. Personopplysningsloven og helselovene gir særregler som innebærer enkelte begrensninger i forordningens bestemmelser, blant annet gjelder ikke artikkel 14.

Informasjon om behandlingen er en grunnleggende forutsetning for at den registrerte skal kunne ivareta sine øvrige rettigheter og interesser. Uten at retten til informasjon blir oppfylt på en god måte, vil det være vanskelig for den registrerte å utøve sine øvrige personvernrettigheter. Målbildet om helhetlig samhandling består av flere løsninger. Behandling av helseopplysning i ulike felles nasjonale tjenester fremstår som komplekst på grunn av stort omfang helseopplysninger og mange involverte virksomheter og helsepersonell. Det er viktig at den registrerte har mulighet til å forstå helheten og hvordan løsningene henger sammen.

Det vil være av vesentlig betydning å ha en strategi for hvordan informere innbyggerne om løsningene, hvordan behandlingen av helseopplysninger foregår der, hvordan ansvarsforholdene er, og spesielt hvor de kan utøve sine rettigheter som innsyn, retting, sletting, sperre mv.

Det må etableres enkle og brukervennlige innbyggertjenester som gjør det enkelt for pasienten å få informasjon, innsyn og oversikt over egne helseopplysninger, logg som viser bruken av helseopplysningene og for å kunne utøve sine øvrige rettigheter.

4.2. Rett til innsyn

EUs personvernforordning art. 15 gir den registrerte rett til innsyn. Innsynsretten er en helt grunnleggende personvernrettighet som må ivaretas i arbeidet med felles journalløsning og samhandlingsløsningene. Innsynsretten gjør det lettere for den registrerte å ivareta sine øvrige rettigheter, f. eks er det ofte gjennom innsyn at den registrerte kan oppdage at det er registrert feil informasjon som videre kan føre til et krav om sletting.

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.

Innsyn i egne helseopplysninger og delingen av disse er en grunnleggende forutsetning for at den registrerte skal kunne ivareta sine øvrige rettigheter og interesser. Uten at retten til individuelt innsyn blir oppfylt på en god måte, vil det være vanskelig for den registrerte å utøve sine øvrige personvernrettigheter.

Felles samhandlingsløsninger, vil i kraft av å være mer samlende løsninger, gjerne med kun én dataansvarlig, kunne bidra til å ivareta retten på en bedre måte enn i dag, fordi den muliggjør en mer helhetlig og effektiv håndtering av rettigheter. Eksempelvis helhetlig innsyn i all deling som skjer i samhandlingsløsninger.

Det må være klart for den registrerte hvor en forespørsel om innsyn i egne helseopplysninger og logg skal rettes. Den registrerte skal også kunne få informasjon om hvem det er utlevert opplysninger til. Dette betyr at det må finnes en oppdatert oversikt over hvem det er utlevert (tilgjengeliggjort) opplysninger til. Det er antagelig ikke tilstrekkelig med en brukslogg med hvem som har hatt tilgang til opplysningene, men at det må gis nok informasjon om mottaker slik at den registrerte selv kan vurdere om de ønsker å utøve andre rettigheter de har, for eksempel sperre. Det må iverksettes tekniske tiltak som sørger for at det til enhver tid finnes en slik oversikt over hvem det er tilgjengeliggjort opplysninger til.

Videre er det et mål om at pasienten skal få en helhetlig oversikt over helseopplysninger som er registrert i ulike pasientjournaler, nye tjenester inkludert opplysninger som er delt med

annet helsepersonell. En samlet oversikt over helseopplysninger vil gi innbygger større grad av kontroll over egne opplysninger enn hva som er tilfelle i dag. I dag er gis det i hovedsak innsyn per virksomhet eller tjeneste og i hovedsak på papir.

Det kan vurderes å etablere en forvaltningsorganisasjon knyttet til samhandlingsløsninger med kompetanse, kapasitet og myndighet til å legge til rette for at enkeltpersoner får oppfylt rettighetene sine på en enkel måte. Det må legges til rette for gode saksbehandlingsrutiner mellom samhandlingsløsningene og virksomhetene som skal bruke løsningen. Dette skal som hovedregel gjøres uten kostnad for den registrerte og innen 30 dager.

Det bør etableres en strategi for å gi pasient og bruker informasjon om løsningene, hvordan behandlingen av helseopplysninger foregår, hvordan ansvarsforholdene er og spesielt hvor de kan utøve sine rettigheter som innsyn, retting, sletting, sperre mv.

Det må forutsettes at det etableres enkle og brukervennlige innbyggertjenester som gjør det enkelt for pasient og bruker å få informasjon, innsyn og helhetlig oversikt over egne helseopplysninger og logg, for å kunne utøve sine øvrige rettigheter.

4.3. Rett til retting

Etter EUs personvernforordning artikkel 16 har den registrerte krav på å få uriktige opplysninger om seg selv rettet eller komplettert. Det finnes særlovgivning på helseområdet som kan begrense den registrertes rett til retting og sletting.

Pasienten har rett til å kreve retting i pasientjournalen, jf. pasient- og brukerrettighetsloven § 5-2. Helsepersonellet som har ført journalen skal vurdere kravet konkret, jf.

helsepersonelloven §§ 43 og 44, og slette opplysninger dersom vilkårene for dette er til stede.

Når det gjelder nye tjenester som lagrer helseopplysninger (originalopplysning, kopi eller metadata) bør det etableres en forvaltning som etablerer rutiner for å sikre at kravet om retting når frem til virksomhetene som skal behandle det. Det må legges opp til rutiner der kravet om retting sendes til virksomhetene/helsepersonellet som har registrert opplysningene. Gitt fristen om ugrunnet opphold, vil det kunne være utfordrende å sikre gode nok rutiner eller andre tiltak som sørger for å oppfylle at retting skjer innen fristen. Denne rettigheten kan bli utfordret fordi rettingen må skje i virksomheten der opplysningene ble registrert f. eks på et fastlegekontor. Det er derfor flere ledd som må involveres, og det vil kunne være utfordrende å automatisere deler eller hele prosessen med retting, som igjen kan det utfordrende å ivareta fristen for saksbehandling. Det bør etableres funksjonalitet som gjør at opplysninger kan "feilmerkes" i påvente av at retting skjer.

Den samme prosessen for retting er lagt til grunn i eksisterende nasjonale samhandlingsløsninger. Dette er for eksempel gjort for kjernejournal.

Retten til retting gir også den registrerte en rett til å komme med supplerende opplysninger. Her vil den samme utfordringen med saksbehandlingskjeden med flere kilder bakover fra felles nasjonale tjenester oppstå. Det vil også kunne være flere kilder der de supplerende opplysningene skal registreres, og dette må ivaretas med tekniske eller organisatoriske tiltak.

Det bør vurderes å etablere en forvaltningsorganisasjon knyttet til samhandlingsløsninger med kompetanse, kapasitet og myndighet til å legge til rette for at enkeltpersoner får oppfylt

rettighetene sine på en enkel måte. Det må legges til rette for gode saksbehandlingsrutiner mellom samhandlingsløsningen og virksomhetene som skal bruke løsningen.

Det må etableres gode saksbehandlingsrutiner mellom den sentrale aktøren og virksomhetene, slik at kravet kan ivaretas på en god måte. Selv om retting og sletting skal skje hos virksomhetene, vil samhandlingsløsninger måtte kunne motta krav fra den registrerte, og må derfor sørge for saksbehandlingsrutiner som gjør at kravet kan oppfylles. Det kan tenkes samme type saksbehandlingsrutiner er etablert for kjernejournal.

Det bør etableres funksjonalitet som gjør at opplysninger kan "feilmerkes" i påvente av at retting skjer.

Det bør etableres en strategi for å gi innbygger informasjon om løsningene, hvordan behandlingen av helseopplysninger foregår og om ivaretakelse av egne rettigheter.

Det forutsettes at det etableres enkle og brukervennlige innbyggertjenester hvor pasient og bruker kan få ivaretatt retten til å kreve retting og sletting.

4.4. Rett til sletting

EUs personvernforordning artikkel 17 medfører at den registrerte i visse tilfeller kan kreve å få opplysninger om seg slettet. Denne retten til å bli glemt, i form av at behandlingsansvarlig skal slette informasjon om den registrerte, gjelder ikke for behandlingsrettede helseregistre, jf. artikkel 17 nr. 3 bokstav b. Retten vil styres av helselovgivningens regler om retting og sletting.

Pasienten har rett til å kreve sletting i pasientjournalen, jf. pasient- og brukerrettighetsloven § 5-2. Helsepersonellet som har ført journalen skal vurdere kravet konkret, jf. helsepersonelloven §§ 43 og 44, og slette opplysninger dersom vilkårene for dette er til stede.

For retten til sletting gjelder mange av de samme utfordringene som ved retting.

Som beskrevet under retting, må det derfor etableres gode samarbeidsrutiner og saksbehandlingsrutiner som sikrer at retten til sletting blir fulgt opp hvis den registrerte anmoder om det.

Det bør etableres en forvaltningsorganisasjon med kompetanse, kapasitet og myndighet til å legge til rette for at enkeltpersoner får oppfylt rettighetene sine på en enkel måte.

Det må på plass gode saksbehandlingsrutiner mellom den sentrale aktøren og virksomhetene, slik at krav kan ivaretas på en god måte. Selv om vurderingen av retting og sletting skal skje hos virksomhetene, vil samhandlingsløsninger måtte kunne motta krav fra den registrerte, og må derfor sørge for saksbehandlingsrutiner som gjør at kravet kan oppfylles.

Det bør etableres funksjonalitet som gjør at opplysninger kan "feilmerkes" i påvente av at sletting skjer.

Det må plass en kommunikasjonsstrategi for å gi pasient og bruker informasjon om løsningene, hvordan behandlingen av helseopplysninger foregår og ivaretakelse av rettigheter.

Det må etableres enkle og brukervennlige innbyggertjenester hvor pasient og bruker kan få ivaretatt retten til å kreve retting og sletting.

4.5. Rett til å motsette seg

Det følger av pasientjournalloven § 17 at pasienten har en rett til å motsette seg at helseopplysninger gis videre til annet personell. Opplysningene kan heller ikke tilgjengeliggjøres eller utleveres dersom det er grunn til å tro at pasienten ville motsette seg det ved forespørsel. Enkelte opplysninger anses som påtrengende nødvendig for helsepersonell å ha kunnskap om for å yte helsehjelp av god kvalitet. Det må derfor fremgå av journalløsninger at det er registrert opplysninger som er sperret. Disse kan som utgangspunkt ikke deles via samhandlingsløsninger. Helseopplysninger kan behandles i journalen uten samtykke fra pasienten. Taushetsplikten setter imidlertid strenge rammer for tilgjengeliggjøringen av helseopplysningene.

Med samhandlingsløsningene vil et større antall helsepersonell potensielt kunne få tilgjengeliggjort helseopplysningene. Dette er nettopp formålet med å få tilgjengeliggjort opplysningene. Samtidig er det sentralt at pasientens personvern ivaretas. Det er derfor helt avgjørende å få på plass god tilgangsstyring som ivaretar pasientens rett til å motsette seg at opplysninger deles.

Det må kunne ivaretas 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. Samhandlingsløsninger må kunne ivareta at pasienten kan sperre for at helseopplysninger blir tilgjengeliggjort for både helsepersonell og virksomheter som ber om å få tilgjengeliggjort opplysninger i nye samhandlingsløsninger.

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.

Dette, i tillegg til andre mekanismer, er med på å gi pasienten kontroll med behandlingen av helseopplysningene i pasientjournalen sin. Pasienten har rett til å sperre deler av eller hele journalen og til å sperre for innsyn for helsepersonell eller virksomheter.

Det bør vurderes å etablere en forvaltningsorganisasjon med kompetanse, kapasitet og myndighet til å legge til rette for at enkeltpersoner får oppfylt rettighetene sine på en enkel måte.

Det må bygges inn sperrefunksjonalitet i system for tilgangsstyring i samhandlingsløsninger.

Det bør etableres en strategi for å gi innbygger informasjon om retten til å sperre og hva den innebærer.

Det forutsettes at det etableres enkle og brukervennlige innbyggertjenester hvor innbygger blant annet kan få informasjon om hva retten til å sperre innebærer og kan få utøvd retten til sperre digitalt.

4.6. Rett til begrensning av behandling

EUs personvernforordning artikkel 18 innebærer at den registrerte i noen tilfeller har rett til at behandlingen av deres opplysninger begrenses. I slike tilfeller skal opplysningene kun lagres, og ikke behandles på annen måte uten den registrertes samtykke.

For samhandlingsløsningene kan dette gjelde når den registrerte har anmodet om sperring.

Retten til begrensning vil måtte ivaretas og dette vil vurderes nærmere i det videre arbeidet.

4.7. Rett til dataportabilitet

EUs personvernforordning artikkel 20 oppstiller retten til dataportabilitet. Denne rettigheten er begrenset til å gjelde tilfeller der den registrerte selv har gitt den dataansvarlige egne personopplysninger. I tillegg gjelder det kun tilfeller der rettsgrunnlaget for behandlingen er enten samtykke i henhold til artikkel 6 nr.1 bokstav a eller artikkel 9 nr. 2 bokstav a eller en avtale etter artikkel 9 nr. 2 bokstav a.

Behandling av helseopplysninger i samhandlingsløsningene vil i all hovedsak være hjemlet i lov eller forskrift. Dette betyr at for nesten all behandling av helseopplysninger i disse løsningene vil ikke dataportabilitet være relevant. Det vil finnes noen tilfeller der dataportabilitet blir aktuelt, f. eks hvis det skal behandles innbyggerdata på samhandlingsløsninger.

Dataportabilitet vil derfor ikke behandles ytterligere i denne vurderingen.

4.8. Rett til å protestere

EUs personvernforordning artikkel 21 innebærer at den registrerte noen tilfeller kan ha rett til å protestere mot behandlingen. Dette gjelder når behandlingsgrunnlaget er personvernforordningen artikkel 6 nr.1 bokstav e allmennhetens interesse eller bokstav f berettiget interesse.

Behandling av helseopplysninger i samhandlingsløsningene vil i all hovedsak være hjemlet i lov eller forskrift. Retten til å protestere vil derfor ikke behandles videre i denne vurderingen.

4.9. Automatiserte individuelle avgjørelser/profilering

EUs personvernforordning artikkel 22 forbyr i visse tilfeller automatiserte individuelle avgjørelser.

Vi ser ikke på nåværende tidspunkt at automatiserte individuelle avgjørelser, herunder

profilering, blir aktuelt knyttet til samhandlingsløsningene. Denne rettigheten blir derfor ikke vurdert nærmere.