Felles kommunal journal interim AS

Bilag 5.1:

Overordnet personvernvurdering

Styringsdokument

Felles kommunal journal: Et felles journalløft for kommuner utenfor helseregion i Midt-Norge

Versjon 0.8

18.11.2022

INNHOLDSFORTEGNELSE

1. INNLEDNING

I dette bilaget finner du:

- Vurdering av behandlingens formål og grunnlag
- Vurdering av behandlingens omfang og art
- Vurdering av personvernsprinsipper

Dette bilaget hører til Vedlegg 5. Det kan også leses sammen med Bilag 5.2.

En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Vurderingen skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastsette risikoreduserende tiltak. Prosessen med DPIA skal bidra til å skape og påvise etterlevelse av personvernet til de registrerte. Dette er en plikt regulert gjennompersonvernregelverket[1], som må gjennomføres hvis det er høy risiko for de registrerte.

I prosjektets arbeid er det gjennomført en overordnet vurdering av personvern sett i forhold til den konseptuelle løsningen. Her legges til grunn at leverandørene leverer funksjoner (sluttbrukerløsningene), og informasjonen lagres og tilgjengeliggjøres på en plattform. Vurderingen er gjennomført av kommunale ressurser i prosjektet. Dette har vært viktig for å sikre erfaring og forankring til en kommunal virkelighet og utfordringsbilde.

Det må gjøres nye vurderinger av personvernkonsekvenser ved planlegging av utprøvinger i alle steg, som må oppdateres i løpet av utprøvingene.

1.1. Formål og grunnlag for behandling

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og være forklart på en måte som gjør at alle berørte har samme forståelse av hva opplysningene skal brukes til. For at formålet skal være legitimt, må det i tillegg ha et rettslig grunnlag. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet[2].

Tiltaket skal sørge for sikker og enkel tilgang til relevante helseopplysninger og andre personopplysninger som benyttes i samhandling mellom helsepersonell for å yte, administrere eller kvalitetssikre helsehjelp. Helseopplysningene og andre personopplysninger vil lagres og behandles på en plattform.

Plattformen vil utvikles stegvis og tas i bruk gradvis og det innebærer at informasjonsmengden vil endres over tid. Prosjektet har arbeidet frem en avgrensning av hva et forventet omfang av informasjon kan være, innledningsvis. Det vises til Bilag 2.2 for utfyllende informasjon for beskrivelse av hva disse kategoriene er.

Det betyr at det er følgende formål og grunnlag for behandling som er aktuelle i starten

Formål	Behandlingsgrunnlag
Behandling av helseopplysninger	• Helsepersonelloven §§§ 4, 39, 40 • Pasientjournalloven §§§ 1, 2, 3 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9

[1] Datatilsynet.no

[2] Datatilsynets strategi | Datatilsynet

Kommunikasjon mellom ansatte i samme virksomhet	• Pasientjournalloven § 19, 25 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h
Kommunikasjon mellom ansatte i ulike virksomheter om helseopplysninger	• Pasientjournalloven § 19 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h

Etter hvert vil følgende formål og grunnlag for behandling bli aktuelle:

Formål	Behandlingsgrunnlag
Behandle og besvare søknader om helsetjenester	• Pasientjournalloven §§ 11, 20 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h
Tilgjengeliggjøring av pasientinformasjon for helsepersonell med tjenstlig	• Helsepersonelloven § 45 • Pasientjournalloven §§ 19, 20 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9
Organisering av pasientavtaler og oppdrag	• Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h
Sikre rett egenbetaling fra pasient	• Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h
IPLOS data som rapportering til helsemyndigheter KPR (Kommunalt pasient- og brukerregister)	• Pasientjournalloven §§ 20 • Helseregisterloven § 11 bokstav j • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9, nr. 2, bokstav h
Behandling av helseopplysninger for forskningsformål uten den registrertes samtykke	• Helsepersonelloven § 37 • Pasientjournalloven § 20 • Personvernforordningen Artikkel 6, nr. 1, bokstav c • Personvernforordningen Artikkel 9

2. BEHANDLINGENS OMFANG OG ART

2.1. Omfanget av informasjon

Omfanget for en plattform er innledningsvis avgrenset til å omfatte relevant pasientinformasjon (for mer informasjon om avgrensninger som er gjort se Vedlegg 4, samt Bilag 2.1). Pasientinformasjon er kategorisert som *særlige kategorier av personopplysninger*[3]. Dette stiller ekstra høye krav til

[3] Eksempler på sensitive personopplysninger er behandling av genetiske og biometriske opplysninger, helseopplysninger, opplysninger om en fysisk persons seksuelle forhold, eller seksuelle orientering mm

etterfølgelse av personvern og informasjonssikkerhet. Tiltak for å imøtekomme dette blir beskrevet senere i bilaget, samt i Bilag 5.2.

For å definere hvilken *relevant* pasientinformasjon en felles i plattform må bestå av, må vi blant annet se til Forskrift om pasientjournal (Pasientjournalforskriften)[4] som sier at en pasientjournal skal inneholde opplysninger som er *relevante og nødvendig for å yte helsehjelp til den enkelte pasient*, jf. helsepersonelloven § 40. Dette inkluderer opplysninger for å kunne identifisere og kontakte pasienten og virksomheten der helsehjelpen gis. Journalen skal gi en oversiktlig og samlet fremstilling av pasientens helsetilstand slik at det er lett for helsepersonell å sette seg inn i pasientens helsetilstand og eventuelt videre planlagt helsehjelp.

Behandling av informasjon i en plattform vil innebære behandling av ulike typer sensitive personopplysninger. Prosjektet har arbeidet frem en avgrensning av hva et forventet omfang av informasjon kan være innledningsvis. Det vises til Bilag 2.2 for utfyllende informasjon for beskrivelse av hva disse kategoriene er.

Etter hvert som plattformen utvikles stegvis og åpner for ny informasjon må protokoll over behandlingsaktiviteter og personvernkonsekvensvurderingen oppdateres med hvilke typer og kategorier av personopplysninger som benyttes.

2.2. Vurdering av behandlingens formål

«EHDS (European Health Data Space) er et forslag til nytt rammeverk for deling av helsedata lagt frem av Europakommisjonen. Det nye regelverket skal gi enkeltpersoner direkte tilgang til egne helsedata, og gi mulighet til å dele helsedata med helsepersonell i hele EU. Pasientjournaler, resepter o.l. skal utstedes i et felles EU-format. I tillegg skal det etableres et rettslig rammeverk for gjenbruk av helsedata til forskning, innovasjon (industri) og politikkutforming. Kommisjonen ser for seg at helsedataområdet er operativt i 2025.»

(https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en)

Plattformen skal lagre og kan sammenstille informasjon, også som grunnlag for nye tjenester vi ikke kjenner i dag. Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål for behandling av personopplysninger skal identifiseres og være forklart på en måte som gjør at alle berørte har samme forståelse av hva opplysningene skal brukes til[5]. I planlegging og realisering av nye tjenester (eks nye informasjonstjenester) må det avklares hvorvidt formålet er nytt, samt om det er vanskelig for en innbygger å forestille seg hva formålet med behandlingen er. For å sikre innbyggerens personvern er det derfor viktig at vi etablerer en tydelig forståelse av hvordan informasjonen skal brukes, altså formålet med informasjonen, og er klar over hvilke plikter og rettigheter som inntreffer dersom et formål endres.

Behandlingen av personopplysninger på en plattform er nødvendig for å sikre forsvarlige og gode helsetjenester i form av tilgang til nødvendige oppdaterte helseopplysninger om pasienten.

Andre vurderinger det blir sentralt å gjøre ved implementering av nye tjenester i en stegvis utvikling er vurderinger av hvorvidt informasjonen predikterer adferd eller profilerer innbygger, eller om behandlingen kan føre til automatiserte beslutninger som får effekt for den registrertes rettigheter. Det er også viktig å vurdere om behandlingen av informasjonen kan innebære systematisk overvåkning av innbygger eller de ansatte.

[4] Forskrift om pasientjournal (pasientjournalforskriften) - Lovdata

[5] Forskrift om pasientjournal (pasientjournalforskriften) - Lovdata

2.3. Behandling i stor skala og ulike kategorier innbyggere

I et målbilde innebærer det behandling av informasjon i stor skala. Det involverer et høyt antall registrerte (basert på innbyggere i 291 kommuner), dekker et stort geografisk område (alle kommuner utenfor Midt-Norge) og mange ulike typer personopplysninger. For å oppfylle kravene kommunene har til behandling og arkivering av informasjon vil behandling også skje over lengre tid[6]. Behandlingen av særlige kategorier personopplysninger, som helseopplysninger er, vil omfatte mange ulike kategorier innbyggere og til dels sårbare grupper. Informasjon skal også utveksles og sammenstilles med informasjon fra nasjonale løsninger, eksempelvis informasjon om innbyggere i Midt-Norge.

2.4. Vurderinger av ny bruk av opplysninger

Målbildet åpner for innovasjon og næringsutvikling i betydelig grad. Det vil også omfatte tjenester og muligheter vi ikke kjenner innhold i eller rekkevidden av i dag. Det kan innebære ny bruk av personopplysninger eller teknologiske/organisatoriske løsninger der risiko enda ikke er kjent. Eksempler er nye apper, velferdsteknologi, IoT eller kunstig intelligens (AI), herunder beslutningsstøtte og læringssystem. Behovet for gode tiltak som ivaretar fortløpende vurderinger av nye mulighets- og bruksområder blir derfor helt sentralt, og må etableres i videre arbeid.

2.5. Innsamling av informasjon

Personopplysningene samles stort sett inn via helsepersonell som gjennom dokumentasjonsplikt (Helsepersonelloven §39) nedtegner sentral og viktig dokumentasjon. Det kan skje i direkte samtale med pasienten eller brukeren, eller det kan være dokumentasjon av gjennomført behandling, tiltak eller vurdering. Det gjøres først og fremst i arbeidsverktøyene (for eksempel eksisterende journalløsninger), og vil lagres på plattformen kontinuerlig for å oppnå målet om relevant og oppdatert informasjon.

[6] *Normen, Faktaark 25 – Lagringstid og sletting, Versjon 3.0 Desember 2021*

2.6. Behandlingsansvar

I dagens situasjon lagres personopplysninger i det enkelte journalsystem, gjerne lokalt i hver kommune. I målbildet finnes det en felles plattform hvor informasjon vil bli lagret og sammenstilt. Behandlingsansvaret må fortsatt være som det er i dag. Den enkelte virksomhet (eksempelvis kommune) er dataansvarlig[7] for informasjonen som produseres og dokumenteres. Dette begrunnes også i Lov om kommunale helse- og omsorgstjenester, §3-1 (kommunenes sørge for ansvar). Den ansvarlige er også overordnet ansvarlig for å overholde personvernprinsippene[8]. Dette ansvaret endres ikke med bruk, og det en absolutt forutsetning at pasientinformasjon som deles, kun kan leses og gjenbrukes, men ikke endres. Drifts- og forvaltningsorgan vil være databehandler[9] av informasjon i en felles plattform fordi de behandler personopplysningene på vegne av andre (behandlingsansvarlig). Dette må være regulert gjennom databehandleravtaler, og det vil derfor foreligge et tydelig behov for godt definerte avtaler i et målbilde. Tilsvarende vil konsumenter av informasjonen være ansvarlig for sin bruk og håndtering av informasjonen.

I dag er Helsenettet et økosystem som omfatter tilnærmet alle leverandører av helsetjenester i Norge, inklusive alle kommuner og fylkeskommuner. Helsenettet er primært en avtalebasert juridisk konstruksjon (tillitsmodell) hvor Norsk helsenett SF (NHN) har rollen som tillitsanker. Ettersom alle medlemmer av helsenettet inngår samme avtale med NHN sikres også at alle tilfredsstiller Normens krav til informasjonssikkerhet. Dermed kan alle medlemmene utveksle pasientinformasjon uten å inngå selvstendige avtaler, men i stedet hvile på sine respektive avtaler med NHN.

Gjennom tilpasning til GDPR, hvor også transport av informasjon betraktes som behandling, ble det også inngått databehandleravtale mellom NHN og samtlige (ca. 6 000) medlemmer av Helsenettet. Dermed kan også NHN opptre som databehandler uten ytterligere avtaler.

2.7. Tilgang til informasjonen

Helsepersonell vil få tilgang til informasjonen som finnes i plattformen med grunnlag i tjenstlig behov. Innbygger skal gjennom sine rettigheter i personvernforordningen, samt annet lovverk, få innsyn i egen informasjon. Det er også naturlig å anta at relevante IT-operatører eller annet teknisk personell vil ha tilgang til plattformen i forbindelse med feilretting, drift og forvaltning, men de har ikke tjenstlig behov for å ha tilgang til informasjonen på plattformen. Tilsvarende vil leverandører også få tilgang til at deres systemer skriver til og leser informasjon fra plattformen som presenteres i leverandørens applikasjon. Det blir viktig med gode databehandleravtaler som styrer dette, samt gode løsninger for sporing og logging.

3. INNBYGGERS RETTIGHETER

Bruk av personopplysninger skal være oversiktlig og forutsigbar for de opplysningene gjelder. Å sikre transparens bidrar til å skape tillitt og setter innbygger i stand til å ivareta sine interesser[10]. I det

[7] Ansvarlig for behandling av helseopplysninger etter personvernforordningen artikkel 4 nr. 7. Pasientjournalloven, §2 (e)

[8] Personvernprinsippene | Datatilsynet

[9] Databehandler behandler personopplysninger **på vegne av andre**. Databehandleren behandler alltid personopplysningene etter instruks fra en annen virksomhet og kan derfor ikke bestemme formål og andre avgjørende elementer ved behandlingen. Behandlingsansvarlig og databehandler | Datatilsynet

[10] Datatilsynets strategi | Datatilsynet

perspektivet er ikke bare informasjonen i seg selv og bruken av den viktig, men også i hvilken sammenheng (kontekst) den benyttes.

Innbyggere må forventes å ha kjennskap til at det nedtegnes informasjon i pasientjournaler hos ulike tjenester i primærhelsetjenesten. Samtidig omfatter innbyggere også sårbare individer som kan ha begrenset evne til å forstå betydning og eventuell konsekvens, og som dermed ikke har mulighet til å motsette seg uønsket bruk. I dag forundres også mange innbyggere over hvor lite informasjon helsepersonell har tilgang til og i hvilken grad de har mulighet til å samhandle. Innbygger blir i stor grad bærer av egen informasjon. Det vises til Vedlegg 2 for mer utfyllende informasjon om innbyggers behov og utfordringsbilde i dag, samt hvilken virkning et tiltak som dette kan ha.

Et viktig element i den konseptuelle løsningen er deling av informasjon mellom helsepersonell som har tjenstlig behov, noe som vil være et aktuelt tema å diskutere som et ledd i en vurdering av konsekvenser for personvern (DPIA). I helsepersonelloven §45 heter det «Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient etter denne lov, gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.»

For mange pasienter er det i dag en utfordring å måtte fortelle sin sykehistorie om igjen til helsepersonell både i samme virksomhet og i andre virksomheter, og for pasientsikkerheten kan dette være en utfordring hvis pasienten ikke evner å fortelle eller glemmer av vesentlig informasjon. Mange pasienter tror i dag at helsepersonell allerede har tilgang til relevant informasjon om seg selv. I forbindelse med DPIA sammen med representanter for de registrerte må det gjøres en forholdsmessig vurdering i forhold til deling av informasjon ved hjelp av plattformen.

Pasientinformasjon som deles må være relevant og oppdatert. Pasientinformasjon kan spille en sentral rolle i akutte og kritiske situasjoner der det står om liv og helse. Det kan også inngå i et vurderingsgrunnlag for tiltak eller behandling, ny medikamentforordning, eller som en del av en evaluering. Både innbygger og helsepersonell vil derfor ha en særskilt forventing om at informasjonen er korrekt. For å sikre at informasjonen er korrekt kommer det også et krav om at den må være oppdatert til enhver tid. Innbygger skal også være trygg på at informasjonen som deles på tvers av flere behandlere er nødvendig. Det blir derfor viktig å sikre at vurderingen av relevant pasientinformasjon gjøres fortløpende i en stegvis utvikling.

Det blir veldig viktig at den enkelte virksomhet gir innbygger informasjon om hvilken informasjon som nå blir tilgjengelig for annet helsepersonell, som har tjenstlig behov. Det blir også viktig å informere innbygger om deres rettigheter (innsyn, sletting mm), samt hvilke verktøy man har for å utøve disse rettighetene. Tilsvarende må virksomheten ha god kjennskap til innbyggers rettigheter til å utøve medbestemmelse over hvordan den enkelte informasjon håndteres, eksempelvis om det er enkelt informasjon man ikke ønsker å tilgjengeliggjøre for andre (jf. Pasient- og brukerrettighetsloven §5-3).

Mulighetsrommet som kan foreligge i et målbilde, og ettersom mer og mer informasjon gjøres tilgjengelig som grunnlag for nye tjenester eller løsninger, er svært utfordrende å si noe om på nåværende tidspunkt. Hvorvidt behandling vil innebære ny bruk av teknologi eller organisatoriske verktøy som for eksempel nye apper, velferdsteknologi, kunstig intelligens mm er vanskelig å si på nåværende tidspunkt, men må forventes i en fremtidig utvikling. Derfor er det helt nødvendig å gjennomføre grundige DPIA og risikovurderinger for hver ny tjeneste som tas i bruk. Dette vil også være viktig knyttet til fortløpende vurderinger av om det matches eller sammenstilles flere datasett, og om dette nå brukes til nye formål eller hensikter som er vanskelig for innbygger å se for seg.

4. VURDERING AV PERSONVERNPRINSIPPENE

I det videre vurderes personvernprinsippene og i hvilken grad disse påvirkes.

4.1. Formålsbegrensning

Personopplysninger skal kun behandles for spesifikke, uttrykkelig angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og være forklart på en måte som gjør at alle berørte har samme forståelse av hva opplysningene skal brukes til. For at formålet skal være legitimt, må det i tillegg ha et rettslig grunnlag som er i samsvar med etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet[11].

Tiltakets formål er å sørge for sikker og enkel tilgang til relevante helseopplysninger og andre personopplysninger som benyttes i samhandling mellom helsepersonell for å yte, administrere eller kvalitetssikre helsehjelp. Alle behandlinger som gjøres har formål som beskrevet i avsnittet Formål og grunnlag for behandling.

Hjemmel for tiltaket bygger på §19 i pasientjournalloven. Pasientjournalloven §19 fastslår at innenfor rammen av taushetsplikt skal den dataansvarlige 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. Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten. Dette fastslås også i lov om helsepersonell mv (helsepersonelloven) §25 som sier at med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp.

Det er naturlig å anta at innbygger har kunnskap om at den som yter helsehjelp skal nedtegne eller registrere opplysninger som omfatter pasienten og helsehjelpen, samt opplysninger nødvendig for å oppfylle meldeplikt eller opplysningsplikt i en journal for den enkelte pasient (Helsepersonelloven §§29 og 40). Det er derimot ikke like naturlig å anta at innbygger skal forstå at informasjonen nedtegnet hos en virksomhet skal være tilgjengelig for andre virksomheter med tjenstlig behov.

4.2. Dataminimering

Prinsippet om *dataminimering* innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. Dersom personopplysningene ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn.[12]

En felles plattform skal kun inneholde det som er *relevant pasientinformasjon* for å oppnå formålet. Behandlingen av informasjon i relasjon mellom behandler og pasient skjer fortsatt i helsepersonellets sluttbrukerløsninger, og dermed hos den enkelte behandler. Når ny informasjon skal lagres og tilgjengeliggjøres gjennom plattform som ledd i en stegvis utvikling, blir det svært viktig å vurdere at informasjonen man lagrer og tilgjengeliggjør faktisk er relevant for å oppnå formålet.

Det bør foreligge grundige vurderinger hvorvidt det skal være mulig å begrense innsamlingen av personopplysninger. Store variasjoner, lokalt eller individuelt, kan øke risikoen for feil behandling eller vurderinger når helseopplysninger deles på tvers av virksomheter.

[11] Datatilsynets strategi | Datatilsynet

[12] Datatilsynets strategi | Datatilsynet

4.3. Integritet

Personopplysninger som behandles skal være korrekte, og skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for å straks slette eller rette personopplysninger som er uriktige[13]. Det er den som har dokumentert personopplysningen som har ansvar for å rette opp feilaktig informasjon.

En felles plattform vil kreve at informasjonen fortløpende oppdateres av aktørene som samhandler. Noe av informasjonen vil hentes fra nasjonale løsninger og felles registre. Behandlingsansvaret endres ikke med bruk, og det forutsettes derfor at pasientinformasjon som deles, kun kan leses og gjenbrukes, men ikke endres. Ved endringer overføres derfor oppdatert informasjon til plattform.

Relevant pasientinformasjon brukes i vurderinger som kan omfatte forskjellen på liv og død. Det må foreligge en helt klar føring om at informasjon ikke bare skal være relevant, men også korrekt og oppdatert. Dette fordrer en kontinuerlig lagring til plattform når det oppstår hendelser/endringer hos en virksomhet.

Innbyggers rettigheter knyttet til innsyn i journal må opprettholdes, også ift. en plattform. Lov om pasient- og brukerrettigheter fastslår i §3-2 at pasient og bruker har rett til informasjon som er nødvendig for å få innsikt i sin helsetilstand og innholdet i helsehjelpen. §5-1 sier at pasient og bruker har rett til innsyn i journalen sin med bilag og har etter særskilt forespørsel rett til kopi, jf. personvernforordningen artikkel 15. §5-2 fastslår at pasient, bruker eller den som opplysningene gjelder kan også kreve at opplysningene i journalen rettes eller slettes etter reglene i helsepersonelloven §42 til §44. Pasienten og brukeren har også rett til å motsette seg overføring og tilgjengeliggjøring av journal eller opplysninger i journal §5-3. Dette vil også være svært relevant å ivareta muligheter, samt informasjon til innbygger om, i samtale med behandler.

> *«Helse- og personopplysninger fra helse- og omsorgstjenesten skal som regel ikke arkiveres før etter at pasienten er død. På dette tidspunktet gjelder ikke personvernforordningens bestemmelser om behandling av personopplysninger da personvernforordningen ikke omfatter døde personer. Særlovgivningen for helse- og omsorgssektoren og arkivlovgivningen har imidlertid bestemmelser som gjelder avdøde personer.*
>
> *Formålet med behandlingen av helse- og personopplysninger er styrende for hvor lenge virksomheten kan lagre opplysningene. Når virksomheten oppnår formålet med behandlingen, så må helse- og personopplysningene i utgangspunktet slettes eller anonymiseres.»*
>
> Normen, Faktaark 25 – Lagringstid og sletting, Versjon 3.0, desember 2021

4.4. Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for[14]. Helse- og personopplysninger i pasientjournaler skal oppbevares i minst 10 år etter siste innføring i journalen. Imidlertid er det viktig at det i hvert enkelt tilfelle, med bakgrunn i en faglig vurdering, avgjøres om når formålet med behandlingen av helse- og personopplysninger er oppfylt. Dette kan representere vanskelige avveininger når det gjelder pasientinformasjon. Noen av årsakene til dette er:

- Helseopplysninger som kan være nødvendig for å yte helsehjelp til pasienten skal ikke slettes, men behovet må heller ikke fremstå som for hypotetisk. Hvilke helseopplysninger som vil være nødvendig må vurderes konkret i hver enkelt sak.

[13] Datatilsynets strategi | Datatilsynet

[14] Datatilsynets strategi | Datatilsynet

- Ved vurdering av oppbevaringstid må virksomheten også vurdere hensynene bak dokumentasjonsplikten, herunder hensynet til at det skal være mulig å føre kontroll med virksomheten i ettertid og hensynet til pasientens mulighet til å fremme erstatningskrav ved skade. På bakgrunn av disse hensynene vil det ofte være grunnlag for å lagre helseopplysninger i behandlingsrettet helseregister over lang tid

- Virksomheten skal fortsette å lagre helse- og personopplysninger etter at formålet er oppnådd dersom opplysningene er underlagt arkivplikt

Enkelte tjenester i den kommunale og fylkeskommunale helse- og omsorgstjenesten skal arkivere og bevare sine pasient- og journalopplysninger. Dette gjelder helsestasjonstjenester, skolehelsetjenesten og tannhelsetjenesten, samt tjenester innen rusomsorg og psykososial omsorg. Arkivene skal avleveres til kommunalt depot. Med pasient- og journalopplysninger menes all individbasert dokumentasjon som skapes av kommunale og fylkeskommunale tjenester som yter helsehjelp. Andre tjenester i den kommunale eller fylkeskommune helse- og omsorgstjenesten kan kassere sine pasient- og journalopplysninger minimum 20 år etter pasientens død, alternativt 120 år etter pasientens fødsel. Dersom virksomheten ikke har grunnlag for å oppbevare helse- og personopplysninger etter at formålet er oppnådd, så skal de slettes. Slettingen skal gjøres på en forsvarlig måte. Det skal brukes en metode som gjør at det ikke er mulig å rekonstruere opplysningene[15].

Det er for tidlig å fastslå hvordan dette kan ivaretas i en felles plattform, også opp mot informasjon som finnes i behandlernes system. Det må foreligge tiltak som følger Normens anbefalinger, samt relevante lovverk som personvernforordningen, pasientjournalloven, pasientjournalforskrift, helsepersonelloven og arkivloven. Det blir viktig i det videre arbeidet å etablere god forståelse for oppgave- og ansvarsforhold, samt hva som kreves i plattform og i sluttbrukerløsninger.

5. VURDERING AV DEN REGISTRERTES RETTIGHETER OG FRIHETER

I det følgende vurderes hvorvidt den registreres rettigheter og friheter ivaretas av tiltaket. Vurderingene er basert på informasjonen som finnes i arbeidet pr nå.

5.1. Den registreres rettigheter

Virksomhetene har plikt til å behandle personopplysninger på en åpen måte. Det betyr blant annet at de må gi en kort og forståelig informasjon om hvordan de behandler personopplysningene[16].

Det er for tidlig å si hvordan dette skal ivaretas, Men vi kan anta at forvalter av plattformen må utarbeide skriftlig informasjon som gir enkel og klar forståelse av hvordan pasientinformasjonen håndteres. Informasjonen må være lett tilgjengelig og forståelig for mottagerne, samt gi konkret informasjon om hva pasientinformasjon brukes til.

5.2. Innsyn i egne personopplysninger

Innbygger har innsynsrett og kan spørre en virksomhet om hvordan opplysningene behandles, samt hvilke opplysninger de har lagret[17]. Innbygger må på samme måte som tidligere kunne utøve sin rett til journalinnsyn etter §5-1 i pasient- og brukerrettighetsloven.

---

[15] *Normen, Faktaark 25 – Lagringstid og sletting, Versjon 3.0 desember 2021*

[16] Rett til informasjon | Datatilsynet

[17] Rett til innsyn | Datatilsynet

Innbyggeren vil få innsyn i egne opplysninger via helsenorge.no eller egne innsynsløsninger. I det videre arbeidet må det avklares hvordan oppgaver for å ivareta rettigheten fordeles mellom behandlingsansvarlige (virksomhetene) og plattformforvalter. Tilsvarende må det avklares om innsyn avgjøres og gjennomføres direkte fra en behandler i deres sluttbrukerløsning, eller om plattformforvalter vil bidra med informasjon ved ønske om innsyn. Det blir viktig å finne frem til en rutine som gjør det enkelt for innbygger å utøve sin rettighet. Det blir også helt sentralt at plattformen har funksjonalitet som kan sikre at innbyggers rettighet blir ivaretatt.

5.3. Korrigering av egne personopplysninger

Som innbygger skal man sikres mulighet til å kreve retting av opplysninger som er uriktige (jf.personvernforordningen artikkel 16)[18], samt jf. Pasient- og brukerrettighetsloven §5-2. På samme måte som med innsyn i egen journal, beskrevet i forrige avsnitt, må det i det videre arbeidet avklares arbeids- og ansvarsfordeling mellom de ulike samarbeidende aktører, også basert på hvor informasjonen som skal korrigeres er lagret (autorativ kilde). Det blir viktig å finne frem til en rutine som gjør det enkelt for innbygger å utøve sin rettighet. Det blir også helt sentralt at plattformen har funksjonalitet som kan sikre at innbyggers rettighet blir ivaretatt.

5.4. Sletting av egne personopplysninger

Basert på pasient- og brukerrettighetsloven §5-2 har pasient, bruker eller den opplysningene gjelder, rett til å kreve sletting av opplysninger i journalen etter reglene i helsepersonelloven §42 til §44.

På samme måte som med innsyn i egen journal og korrigering av journal beskrevet i foregående avsnitt, må det i det videre arbeidet avklares arbeids- og ansvarsfordeling mellom de ulike samarbeidende aktører, også basert på hvor informasjonen som skal korrigeres er lagret (autorativ kilde). Det blir viktig å finne frem til en rutine som gjør det enkelt å utøve innbyggerens rettighet. Det blir også helt sentralt at plattformen har funksjonalitet som kan sikre at innbyggers rettighet blir ivaretatt.

Innbygger vil kunne utøve denne rettigheten uavhengig av formål og behandlingsgrunnlag i plattformen. Innbyggers rettigheter er hjemlet i loven.

5.5. Begrensning av behandling av personopplysninger

Dette området ansees som mindre relevant i dette tiltaket der hjemmelen for behandling av informasjon er lovfestet. For innbygger vil det tilsvarende være pasient- og brukerrettighetslovens kap. 5 som vil komme til anvendelse i forhold til å endre eller regulere bruk av informasjon i en journal.

5.6. Dataportabilitet

Innbygger kan utøve retten til dataportabilitet. Dette innebærer å få utlevert personopplysninger og gjenbruke disse på tvers av ulike systemer og tjenester. Dette skal gjøre det lettere å bytte tjenesteleverandør (for eksempel overgang til annen (eksmpelvis privat) helseaktør), og skal gjøre det enklere å kunne ta med opplysningene til ønsket leverandør[19].

Retten til dataportabilitet gjelder kun hvis opplysningene som ønskes utlevert er samlet inn på bakgrunn av samtykke eller kontrakt. I plattformen er informasjonen og formålet med informasjonen hjemlet i loven. Dette vil også være informasjon som er nødvendig for å ivareta lovkrav som for

[18] Rett til retting | Datatilsynet

[19] Rett til dataportabilitet | Datatilsynet

eksempel dokumentasjonsplikt for helsepersonell og virksomhetene. Det må derfor avklares nærmere hvordan innbygger skal kunne utøve sin rettighet.

Etter pasient- og brukerrettighetsloven §5-3 kan innbygger overføre og tilgjengeliggjøre journal eller opplysninger i journal, men da i henhold til bestemmelsene i lov om helsepersonell.

Dersom innbygger ønsker utlevert sine opplysninger må de leveres i et maskinlesbart eller vanlig brukt filformat.

5.7. Innsigelse mot behandlingen

Retten til å protestere på behandlingen av informasjonen gjelder ikke i tilfeller der virksomhetene er pålagt i lov å behandle personopplysningene. Dette vil være tilfelle med plattformen og tiltaket. For innbygger vil derfor innsigelse mot behandling av informasjon følge regler for innsyn og tiltak i journal som finnes i pasient- og brukerrettghetsloven §5-1 til §5-3, samt helsepersonelloven. På bakgrunn av dette beskrives ikke denne rettigheten ytterligere.

5.8. Automatiserte avgjørelser og profilering

Som innbygger skal man ikke oppleve at et dataprogram tar store og viktige avgjørelser på egne vegne. Det slår personvernforordningen fast i artikkel 22. Personvernforordningen forbyr automatiserte individuelle avgjørelser som både er helautomatiske (at et menneske ikke har reell innvirkning på dette), eller som har rettsvirkning for innbygger eller i tilsvarende grad påvirker innbygger[20].

Behandling av informasjon i en felles plattform er ikke tenkt å ta beslutninger (automatiserte avgjørelser eller profilering) for innbygger. Innledningsvis er omfanget avgrenset til relevant pasientinformasjon, og det er identifisert spesfikke kategorier av informasjon som et foreslått område for stegvis realisering. Automatiserte beslutninger kan muligens være i større grad aktuelt innenfor saksbehandling, og dette vil ikke være omfattet av plattformen innledningsvis.

Dette er likevel et område som må vurderes jevnlig, også ettersom plattformen får tilgjengelig mer og mer informasjon. Dette vil kunne skape nye muligheter eller endre prosesser som vi ikke kjenner til i dag. Arbeidet med fortløpende risiko- og personvernvurderinger ved tilgjengeliggjøring av ny informasjon, tjenester eller løsninger blir derfor helt avgjørende for å sikre at det gjennomføres grundige vurderinger fortløpende.

I det videre arbeidet, når det blir aktuelt, må det arbeides med å avklare hvordan en innbygger eventuelt skal kunne reservere seg mot en slik behandling.

5.9. Risiko

Vi viser til bilag 5.2. Overordnet risikovurdering for kartlagte risikoer knyttet til personvern. Dette må arbeides videre med i det videre arbeidet med utarbeiding av en personvernkonsekvensutredning (DPIA).

6. VIDERE ARBEID MED PERSONVERN

I forbindelse med planlegging av første utprøving må prosjektet gjennomføre tiltak for å sørge for akseptabel risiko i forhold til personvern. Plattformen vil etter hvert inneholde store mengder helseopplysninger som er regnet som særlige kategorier av opplysninger, samt systematiske og omfattende vurderinger av den registrertes personlige aspekter. I tillegg kan det bli gjenstand for automatisert behandling som danner grunnlag for avgjørelser som i betydelig grad vil påvirke den

[20] Automatiserte avgjerder | Datatilsynet

registrerte (som omtalt i personvernforordningen artikkel 35(3)). Det er derfor helt nødvendig at det gjøres en vurdering av personvernkonsekvensene. Representanter for de registrerte må gi innspill/delta i DPIA. Her kan vi se til allerede etablerte strukturer som bruker- og pasientorganisasjoner (se kap 4 i styringsdokument). Personvernombud fra aktører, helsepersonell, teknisk personell med flere bør også delta i arbeidet.

Det er flere vurderinger og tiltak som må videreutvikles i arbeidet når man har mer konkret kunnskap og avgrensning av endelig løsning, informasjon, informasjonsflyt, berørte aktører mm. Et av tiltakene som må gjøres er protokoll over behandlingsaktiviteter. Etter at en personvernkonsekvensvurdering er gjennomført må deretter ledelsen ta en beslutning i forhold til om:

- risikoen for de registrertes rettigheter og friheter er redusert til et akseptabelt nivå, slik at når tiltak er etablert kan behandlingen av personopplysninger gjennomføres
- risikoen for de registrertes rettigheter og friheter ikke er redusert til et akseptabelt nivå, slik at behandlingen av personopplysninger dermed ikke kan gjennomføres
- risikoen for de registrertes rettigheter og friheter er ikke redusert til et akseptabelt nivå, slik at forhåndsdrøfting med Datatilsynet må gjennomføres før ledelsen tar en beslutning om behandling av personopplysninger