postmottak@ehelse.no.

Deres ref:	Vår ref:	Saksbehandler:	Dato:
23/687	2023/5900-4	Heidi Elisabeth Robertsen	22.09.2023

Innspill til Retningslinje for bruk av reelle journalopplysninger for utvikling og test i lukkede miljøer

Innspill fra personvernombudet

Vi viser til Direktoratet for e-helses høringsbrev av 23.06.2023, Ref. 23/687, om utkast til retningslinje for bruk av direkte identifiserbare helseopplysninger til utvikling og testing av behandlingsrettede helseregistre.

Under følger høringsuttalelse fra personvernombudet ved UNN

Innledning

Retningslinjen er ment å gi veiledning knyttet til praktiseringen av en ny bestemmelse i pasientjournalloven § 11 annet ledd, som gir hjemmel for å benytte direkte identifiserbare helseopplysninger til slike formål.

Personvernombudet har tatt utgangspunkt i direktoratets spørsmålsstilling om endringer i innhold og språkbruk som kan gjøre utkastet mest mulig relevant og tilgjengelig for målgruppen. Videre har vi naturlig nok sett på spørsmål som går på ivaretakelsen av personvernregelverket og de registrertes rettigheter og friheter.

Når det gjelder spørsmålet om forslag til praktiske eksempler som kan berike retningslinjen, er ikke vi nok «hands-on» til å foreslå nye eksempler, men vi har knyttet enkelte kommentarer til eksisterende eksempler som kan bidra til at disse blir presise nok, og slik at de i alle fall ikke gir vilkårene et annet innhold enn hva loven legger opp til. Vi anmoder direktoratet om å vurdere alle innspill til eksempler ut fra risikoen for at målgruppen «legger for mye i» eksemplene. Det vil være uheldig om veldig konkrete eksempler tas til inntekt for mer eller mindre bruk av reelle pasientopplysninger enn hva loven legger opp til.

Høringsinnspillene er bygget opp i tråd med veilederens nummerering/rekkefølge.

Om bestemmelsens rekkevidde – snever unntaksbestemmelse – veilederen punkt 1

Vi vil innledningsvis peke på retningslinjens punkt 1.1 andre avsnitt, hvor det presiseres at bestemmelsen er ment å være en snever unntaksbestemmelse. Tilsvarende vil vi peke på siste avsnitt i punkt 1.1, om at virksomheter som ikke velger å følge anbefalingene må basere dette på en konkret og begrunnet vurdering som dokumenteres.

Personvernombudet er naturligvis helt enig i disse utgangspunkter, og mener disse forholdene med fordel kan løftes og tydeliggjøres ytterligere. Det er helt sentrale utgangspunkter, som må følge brukeren og beslutningstakerne hele veien i sine vurderinger. Vi mener punktene derfor gjerne kan gjøres mer konkret i forbindelse med senere redegjørelser for vilkår, tiltak og øvrige forhold som virksomheten må vurdere ifbm. mulig bruk av (direkte) identifiserbare helseopplysninger til testformål. Vår «bekymring» er at enkelte i målgruppen fort vil gå rett på sak på de mer praktiske eksempler og retningslinjer, og da er det en fordel om man søker å gi utgangspunktet mer vekt i selve veilederen.

<u>Punkt 1.2 Om retningslinjen og 1.3 beslutningstakere – involvering av riktig personell i virksomheten</u>

Retningslinjens punkt 1.2 oppsummerer hva retningslinjen skal være, bl.a. at den vil redegjøre for «hvilke vurderinger den dataansvarlige virksomheten må gjøre før helseopplysninger eventuelt benyttes» til test- og utviklingsformål.

For en jurist er denne setningen nokså klar, men for personell med annen fagbakgrunn kan det bli for svevende.

Ut fra våre erfaringer knyttet til strukturer og beslutningsprosesser i de ulike (helse)foretakene, mener vi at retningslinjen med fordel kan innta et punkt/huskeliste til brukerne (målgruppen) om at en må ha tydelig for seg hvem som er rette personer å involvere i egen virksomhet i forbindelse med vurderinger og beslutninger om bruk av helseopplysninger til (også) test- og utviklingsformål. Konkret hvem dette er vil naturligvis kunne variere mellom de ulike foretakene, men retningslinjen kan peke på dette som en aktuell problemstilling og løfte det frem for målgruppen.

Dette vil både kunne bidra til en bevisstgjøring for målgruppen med hensyn til å følge interne retningslinjer (fullmaktsmatrise og lignende), men også som et punkt for å sikre at riktige brukere internt i virksomhetene involveres på riktig tid. Enten dette er direktør, klinikksjef, avdelingsledelse osv. for beslutning, ansatte, informasjonssikkerhetsansvarlig, personvernombud, brukerrepresentanter osv. for andre innspill.

Hvilket punkt dette skal fremgå under har vi ikke noen spesiell formening om, men det siterte punktet under 1.2 kan være et startpunkt, og evt. videre i punkt 1.3 om målgruppe, kan dette trekkes noe mer frem.

Om punkt 2 vilkår for bruk av helseopplysninger til utviklings- og testformål

Forslag om endring i rekkefølge på teksten for å synliggjøre hovedreglene

Punkt 2 i veilederen tar for seg vilkårene for bruk av direkte identifiserbare opplysninger til test- og utviklingsformål. I tredje kulepunkt angis vilkåret om at det må være umulig eller uforholdsmessig vanskelig å oppnå formålet ved bruk av «pseudonyme, anonyme eller fiktive opplysninger».

Rekkefølgen for alternativene til bruk av direkte identifiserbare helseopplysninger i det følgende tar utgangspunkt i lovens rekkefølge (som gjengitt ovenfor). Som et generelt innspill, tenker vi at det av pedagogiske/bevisstgjørende grunner kan være en fordel å snu dette på hodet i retningslinjen og starte med minste inngripende testregime.

Personvernprinsippene tilsier at man starter med å vurdere om man kan oppnå formålet uten bruk av personopplysninger, typisk i denne sammenheng at man i stedet tester med fiktive/syntetiske data, evt. anonymiserer data for det konkrete formålet, eller atter alternativt at man ser på bruk av pseudonyme data, slik som også er trukket frem i andre avsnitt punkt 2. Først etter å ha gjennomgått dette, vil det være aktuelt å vurdere bruk av direkte identifiserbare helseopplysninger.

Innspill til punkt 2.1.1 «Umulighetsvilkåret»

Gjennomgangen av vilkåret starter med å konstatere høy terskel, ved at formålet «ikke på noen måte..» kan oppnås med et mindre inngripende alternativ. Det senere eksempelet som gis synes imidlertid å senke denne terskelen veldig mye. Eksempelet er også så rundt formet og lite konkret at noen bevisst eller ubevisst kan komme til å feiltolke vilkåret, og dermed konkludere med at umulighetsvilkåret er anvendelig selv om spørsmålet heller burde vært vurdert etter om det er uforholdsmessig vanskelig. Vi har ikke et godt alternativt forslag til eksempel, men en mulighet er at man her helt dropper eksempler og heller bruker en setning eller to til på å utbrodere selve vilkåret «umulig». EDPBs veileder knyttet til unntak fra informasjonsplikten etter personvernforordningen artikkel 15 nr. 5 bokstav b kan være en relevant inspirasjon.

Terskelen er så høy at man står overfor en svart/hvitt-situasjon. Det er generelt sett ingen grader av umulighet. Enten er noe mulig, eller så er det umulig. Etter vår mening vil derfor, slik også som etter overnevnte bestemmelse i personvernforordningen, umulighetsvilkåret stort sett ikke være anvendelig.

Innspill til punkt 2.1.2 – uforholdsmessig vanskelig

Første avsnitt i punktet innledes som en glidende overgang fra punktet over. Det gir grei flyt i teksten, men vi mener at man i likhet med punkt 2.1.1 tar utgangspunkt i juridisk metode også her ved at man starter med utgangspunkt i lovens vilkår og hva som kan utledes av den. Deler av første avsnitt kan i stedet flyttes opp til 2.1.1, som en spoiler/videre henvisning til «å se mer i neste punkt».
I avsnittets siste setning henvises det til forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 5(2) som hjemmel for dokumentasjonskravet. Vi er enig i at vurderingen skal

dokumenteres, men er kanskje litt usikker på om forskriftshenvisningen er helt treffende.

I andre avsnitt sies at vilkåret bare er oppfylt dersom bruken av […] vil være «uforholdsmessig». Dette er en unøyaktig gjengivelse av vilkåret «uforholdsmessig *vanskelig*», og bør rettes opp i.

Når det gjelder det øvrige innholdet i andre avsnitt, fremstår det mindre tilgjengelig for målgruppen. For en jurist er en (u)forholdsmessighetsvurdering og den balansetesten som det innebærer nokså klart, men for annet fagpersonell er ikke dette like selvsagt. Slik teksten nå fremstår, forutsetter den at man er kjent med hva dette innebærer, før den direkte går videre på momenter som kan være relevante i en forholdsmessighetsvurdering. Man bør spandere noen setninger på å forklare hva en forholdsmessighetsvurdering er og hvordan den gjennomføres først.

Også i dette avsnittet synes eksempelet å senke terskelen for bruk av direkte identifiserbare helseopplysninger utover hva hovedregelen tilsier. Dette vil også fort kunne bli brukt som en begrunnelse eller legitimering i bruk av pasientopplysninger fremfor syntetiske data i svært mange tilfeller.

<u>Om de opplistede momenter i forholdsmessighetsvurderingen</u>

I punkt 2.1.2 avsnitt tre flg. gjennomgås flere relevante momenter i en forholdsmessighetsvurdering. Selv om listen angis å ikke være uttømmende, mener vi punktene med fordel kan nummeres/settes opp som en sjekkliste for forhold som alltid må vurderes. Dette vil kunne bidra til bedre personopplysningsvern. Man kan gjerne slenge på en «annet» som et siste nummererte punkt i sjekklisten.

Selv om vi er enig i at de opplistede momenter er relevante, synes vi at man skaper en ubalanse ved (først og fremst) å trekke frem momenter som taler *for* bruk av direkte identifiserbare opplysninger.

I den grad det trekkes frem momenter som taler *mot* bruk av direkte identifiserbare opplysninger i test- og utvikling, synes vi veilederen blir litt for vag. Se f.eks. annet avsnitt under punkt «oppfyllelse av pasientrettigheter» hvor manglende mulighet til etterlevelse av den registrertes rettigheter og friheter i et testmiljø trekkes frem som noe som «kan» tilsi at man ikke bruker pasientopplysninger. Etter vår mening er dette helt klart et moment som tilsier at man ikke bør gjennomføre med direkte identifiserbare helseopplysninger. For det tilfelle at man til tross for manglende oppfyllelse av rettighetene, f.eks. fordi man ikke kan oppfylle kravet om informasjon til den registrerte, må man (også) påvise et relevant unntak fra informasjonsplikten. Ved å trekke frem noen av disse forholdene/konsekvensene ved manglende oppfyllelse av personvernregelverket, kan man i større grad tydeliggjøre momentene som taler i mot og det (ekstra)arbeidet det innebærer dersom man går for løsninger som er i strid med det generelle personvernregelverket.

Om punkt 3 – lukkede testmiljøer

Punktet er nokså teknisk, både i innhold og språk. Vi mener det her kan være greit å si noe mer om hva et lukket testmiljø er. Vi erfarer at begrepet brukes noe ulikt også innad i klinikker og IKT-

miljøer, og helt sikkert også på tvers av slike miljøer. Forhåpentligvis kommer det innspill knyttet til forståelsen av begrepene fra miljøene, men hvis ikke kan dette være noe å undersøke nærmere eller klarere definere.

I punkt 3.1 «utvikling, testing og prøvedrift», tredje avsnitt, utleder direktoratet fra departementets forarbeidsuttalelse i Prop. 91 L (2021-2022) en aksept for at prøvedrift *utenfor* lukkede testmiljøer kan skje, ettersom departementet har uttalt at «prøvedrift i denne sammenheng vil være omfattet av begrepet test». Personvernombudet stiller spørsmålstegn ved dette. Selv om man ved prøvedrift generelt sett vil forutsette at systemet tas i bruk i mer eller mindre vanlig klinisk praksis, er det etter vår mening ikke gitt at departementet har hatt dette klart for seg i sin vurdering. Vi viser her til de senere avsnittene i nevnte forarbeid, hvor det i avsnitt om benyttelse av unntaksadgangen til bruk av reelle data presiseres fra departementet at det stilles særlig krav til sikring av opplysningene, og videre fremgår at departementet «fastholder derfor at arbeidet skal utføres i lukkede utviklings- og testmiljøer».

Dette er en viktig avklaring, da det potensielt vil kunne få følgefeil i veilederen, se punkt 3.2 i veilederen hvor det sies at det så langt det er mulig skal etableres «separate miljøer […], adskilt fra produksjonsmiljøene». Vi ser imidlertid også at lovgiver kunne vært tydeligere i bestemmelsens ordlyd omkring dette.

Punkt 3.9 – logging

Punktet angir at det skal loggføres tilganger og hendelser i det lukkede testmiljøet, og går nærmere inn på formålet med dette og lagringstid for slike logger. Etter vår mening kan man her i stedet angi at loggingen i testdatabasen/det lukkede miljøet skal være lik og oppfylle de samme krav og formål som for pasientjournalsystemer generelt. Siste punkt om lagringstid kan også misforstås til at loggen kan slettes etter formålet med testingen/utviklingen er oppfylt. Det kan ikke være riktig. Også denne loggen må lagres etter samme vilkår som pasientjournalen generelt. Hvis ikke vil ikke formålene med loggingen kunne oppfylles, og den registrertes rettigheter uthules.

Om punkt 4 – øvrige forhold helsevirksomheten må vurdere

Annet avsnitt i punkt 4.1 kan gjerne utdypes og eksemplifiseres. Vi er kjent med at det er en bevisst eller ubevisst oppfatning om at etablerte leverandører av pasientjournalsystemer som allerede har avtaler med leveranse av journalsystemer til foretaket på eget initiativ kan ta tilgang eller i alle fall be om tilgang til pasientdata i forbindelse med utvikling av moduler o.l. som de (presumtivt) ønsker å selge til helseforetakene i neste omgang.

Punkt 4.4 – behov for mer informasjon om innebygd personvern

Kravet om innebygd personvern er et av de viktigste, om ikke også *det viktigste*, kravet i personopplysningsloven og personvernforordningen, ved at det inkluderer ivaretakelse av alle personvernprinsippene og den registrertes rettigheter og friheter på en god måte i behandlingen av personopplysninger. Det er imidlertid et punkt som mange ikke forstår innholdet og rekkevidden av, med mindre de er jurister og/eller daglig jobber med personvern.

Etter vår mening bør man derfor si noe mer om dette i veilederen, og kanskje også gi noen eksempler, fremfor bare å henvise til eksterne kilder. Ettersom veilederen ellers er nokså detaljert og god, er det fort for den uinnvidde leseren og ta «for lett» på dette kravet sånn som det nå står. Det blir mest bare en apropos.

Punkt 4.5 Dataminimering

Siste setning i annet avsnitt kan med fordel skrives fullt ut. Angivelsen «dette» kan i stedet angis til «enn hva som er nødvendig for å oppnå formålet», slik som vilkåret er.

Overnevnte kan også tas som en generell kommentar. Det genererer noen flere ord i veilederen, men det kan være nyttig og nødvendig å skrive ut setningene i tekster som dette. En veileder leses kanskje eller kanskje ikke fra A til Å en gang, men underveis i arbeidet så blir det gjerne et oppslagsverk. Da kan fullstendige setninger, gjentakelser og krysshenvisninger til andre steder i teksten være nyttige hjelpemidler for å bedre tilgjengeligheten og brukervennligheten til veilederen.

Man bør se nærmere på eksempelet som er benyttet i siste avsnitt. «Nok» data er veldig upresist.

Om punkt 5 – sentrale begreper i retningslinjen

Punktet er generelt bra og nødvendig i veilederen.
Under punkt 5.4 bør man se på om man kan redegjøre i korthet om skillet mellom «ordinære» og «særlige kategorier» personopplysninger. Men en annen ting er at det kan argumenteres for at enhver opplysning om identifiserbare personer i et pasientjournalsystem vil være særlige kategorier personopplysninger. Unntak kan nok være opplysninger om ansatte.

Rekkefølge på punkter

Tilsvarende som tidligere kommentar, kan man kanskje også her ta utgangspunkt i rekkefølgen fiktive, anonyme, pseudonyme og avslutte med direkte identifiserbare helseopplysninger i gjennomgangen. Akkurat her er det kanskje dog mer en smakssak.

Punkt 5.5 direkte identifiserbare opplysninger

Andre setning i avsnittet synes å legge til grunn at det er et vilkår for at noe er direkte identifiserbare opplysninger at de ikke er omfattet av tekniske tiltak slik som kryptering. Dette mener vi er feil og et for snevert synspunkt. Opplysninger i et system kan, i alle fall i dagligtale, være direkte identifiserbare selv om de er krypterte. En kryptering «låser» en database for uvedkommende, men for en «vedkommende» som har tilgang til nøkkelen (omså bare en kode til databasen) vil opplysningene straks være direkte identifiserbare. Det er sånn sett et informasjonssikkerhetstiltak, og ikke noe som nødvendigvis virker inn på lovens definisjon av direkte identifiserbar.

Punkt 5.8 Fiktive opplysninger / syntetiske data

Siste avsnitt i punktet slår fast at det ikke medfører noen risiko knyttet til ivaretakelse av personvernreglene ved bruk av fiktive opplysningen. Slik vi forstår det, innebærer dette en forutsetning om at disse opplysningene under ingen omstendigheter kan «overføres» til reelle pasienter/personer. Vi forstår det slik at det har vært tilfeller ved testing med fiktive data knyttet til f.eks. medisinsk teknisk utstyr, hvor de fiktive testdataene har blitt «overført» til en reell pasient som følge av tett sammenkobling mellom MTU og pasientjournalsystemer. Det vil åpenbart være en relevant risiko.

Punkt 5.11 Lukket utviklings- og testmiljø og generelle bemerkninger

Overordnet synes vi veilederen er bra. Vi savner litt mer utfyllende beskrivelser av enkelte begreper, som f.eks. lukkede testmiljøer, og også en større fremheving av ansvarslinjer. Videre mener vi det vil være en styrke om man trekker frem flere momenter *mot* bruk av direkte identifiserbare data i test- og utvikling. Dette vil kunne styrke virksomhetenes evne til å gjennomføre en god balansetest.

Vennlig hilsen
for personvernombudet på UNN

Karl-Petter Simonsen
personvernrådgiver

Dokumentet er elektronisk godkjent og kan derfor være uten signatur.

Kopi til:
HELSE NORD RHF