DEN NORSKE LEGEFORENING

Sendt kun per e-post.

Deres ref.: Vår ref: HSAK202500559 Dato: 17-10-2025

Høring - Oversikt over kriterier til sikre analyserom for sekundærbruk av helsedata i Norge – i forberedelse til kommende krav i EHDS

Innledning

Legeforeningen har fra Helsedirektoratet mottatt til høring – Oversikt over kriterier til sikre analyserom for sekundærbruk av helsedata i Norge. Arbeidet er en del av prosjektet FAIR Secure Provision and Use of Health data in Norway (SPUHiN) – et samarbeid mellom Helsedirektoratet, Folkehelseinstituttet og flere av de mest brukte sikre analyserom i Norge (NORTRE).

Høringen har vært sendt ut til Legeforeningens foreningsledd og har blitt behandlet i foreningens sentralstyre.

Helt overordnet er det avgjørende at sikre analyserom etableres med høy standard for informasjonssikkerhet, personvern og transparens, for å ivareta pasientens tillit til helsetjenesten.

Nedenfor følger våre merknader.

Konkretisering av roller og ansvar

Norge har ennå ikke utnevnt en koordinerende "Health Data Access Body" (HDAB) som det kreves av EHDS artikkel 55-59.

HDAB skal vurdere og godkjenne forespørsler om tilgang til helsedata til sekundære formål, tilgjengeliggjøre data og iverksette nødvendige tiltak for å beskytte sensitive data. Det kan utpekes flere HDAB-er som ivaretar rollen og ansvarsområdene som beskrevet i EHDS-forordningen, men det *må* utpekes en koordinerende HDAB med kontaktflate med aktørene i inn- og utland. Helsedirektoratet skriver at kravet til koordinerende HDAB kun er delvis oppfylt:

> "FHI/Helsedataservice (HDS) oppfyller mange av kravene til en koordinerende HDAB i dag. Det er behov for å tydeliggjøre rollen og videreutvikle funksjoner, kompetanse, kapasitet og tekniske løsninger for at Helsedataservice skal kunne oppfylle kravene i henhold til EHDS.

Det må vurderes om det skal utpekes flere HDAB'er."[2]

Det forutsettes at dette arbeides med.

Videre nevner kriterielisten at formålet med kriterielisten er å fungere som "et verktøy for selverkæring for tilbydere av sikre analyserom", men det gis ingen konkrete retningslinjer for hvordan denne prosessen skal gjennomføres.

Tekniske spesifikasjoner

Kriterielisten krever at kryptering skal skje i tråd med gjeldende krypteringsstandarder, men konkrete algoritmer blir ikke spesifisert.

Videre nevens behov for maskin-til-maskin dataoverføring uten å gi tekniske spesifikasjoner for API-design.

For at kriterielisten skal fungere i praksis, bør det gjøres et målrettet arbeid med disse områdene.

Personvern

Det er klart at strenge personvernhensyn gjør seg gjeldende for sekundærbruk av helsedata. Det følger blant annet av fortalen til EHDS at brukere ikke skal forsøke å re-identifisere fysiske personer ut fra datasettet som er gjort tilgjengelig etter forordningen, og at de som gjør det, skal kunne ilegges bøter eller straffereaksjoner hvis hjemlet i nasjonal lovgivning.[3]

Pseudonymisering som standardprinsipp

For å styrke personvernbeskyttelsen og samtidig gi den nødvendige fleksibiliteten for medisinsk forskning og innovasjon, foreslås det at alle helsedata som lagres i SPE-er skal være pseudonymisert *før* de gjøres tilgjengelige for forskere og andre brukere. Dette innebærer:

- Fjerning av direkte identifikatorer: Personnummer, navn, adresser og andre direkte identifiserbare opplysninger fjernes eller erstattes med pseudonymer.
- Teknisk pseudonymisering: Implementering av hash-funksjoner eller kryptografiske teknikker som gjør re-identifikasjon praktisk umulig for SPE-brukere.
- Separasjon av nøkler: Koblingsnøkler mellom pseudonymer og identiteter er ikke tilgjengelige for brukere av SPE-miljøet.

DEN NORSKE LEGEFORENING

Endring av filuttrekksrestriksjoner

I stedet for å fokusere primært på å begrense uttrekk av "identifiserbare data" som beskrevet i gjeldende krav (P19-P25), bør fokuset være på strukturell personvernsikring gjennom design:

- Data som er tilgjengelige i SPE er allerede pseudonymisert og derfor ikke-personlige for brukerne.
- Uttrekksrestriksjoner kan fokusere på å forhindre re-identifikasjon gjennom statistiske avsløringsteknikker.

Fleksibelt datauttrekk for forskning og innovasjon

Med pseudonymiserte data som grunnlag, kan SPE-er tillate mer fleksible uttrekk av:

- Individnivå datasett som er nødvendige for maskinlæring og KI-utvikling.
- Komplette pasientforløp for utvikling av kliniske beslutningsstøtte-systemer.
- Detaljerte kliniske mønstre for medisinsk produktutvikling.

Alt dette med begrenset risiko for re-identifikasjon av enkeltpersoner.

Kobling til nye data gjennom kontrollerte prosesser

Koblingsnøkler bør tillate:

- Tilkobling av nye data fra dataeierne til eksisterende pseudonymiserte datasett.
- Longitudinale studier hvor samme pasienter følges over tid.
- Kobling mellom registre for mer omfattende forskningsdatasett.

Slike koblinger skal kun utføres av dataeierne eller godkjente mellomaktører som har tilgang til identitetsnøklene.

Foreslåtte endringer i SPE-anbefalingene

Endring av P25 (Review of file extraction):

Nåværende tekst fokuserer på: "review the data in the files that have been extracted, until the review has been performed by the SPE user organisation"

Foreslått endring: SPE skal implementere tekniske kontroller som sikrer at uttrekk ikke kan re-identifisere pseudonymiserte data gjennom statistisk avsløring eller kobling med eksterne datasett. Manuell gjennomgang skal primært fokusere på å forhindre statistisk reidentifikasjon.

DEN NORSKE LEGEFORENING

Nytt krav: Pseudonymiseringsstandard (P-NY1):

Krav: *Alle helsedata som gjøres tilgjengelige i SPE skal være pseudonymisert i henhold til gjeldende tekniske standarder, slik at re-identifikasjon er praktisk umulig for SPE-brukere.*

Nytt krav: Koblingsnøkkel-administrasjon (P-NY2):

Krav: *SPE-provider skal implementere sikre prosedyrer for administrasjon av koblingsnøkler som tillater autoriserte dataeieres å knytte nye data til eksisterende pseudonymiserte datasett.*

Fordeler ved denne tilnærmingen

Fordeler ved denne tilnærmingen er for det første juridisk sikkerhet. Pseudonymisering er bla. etter personvernforordningen artikkel 32 oppgitt som et tiltak for oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen ved behandling av personopplysninger.

I sak C-413/23 P ble det vurdert at pseudonymiserte data kan falle utenfor definisjonen av personopplysninger etter Regulation 2018/1725 artikkel 3 nr. 6, gitt at det er praktisk umulig for mottaker av dataene å identifisere noen registrerte personer fra dataene. Denne forordningen er ikke gjennomført i norsk rett,[4] men det følger bla. av forordningens fortalepunkt 5 at den skal tolkes homogent med personvernforordningen (GDPR).

Det bemerkes at dommen står i kontrast til European Data Protection Board (EDPB) sin veileder om pseudonymisering, hvor det fastslås at pseudonymiserte data regnes som personopplysninger.

Dersom pseudonymiserte data ikke regnes som personopplysninger fordi mottaker ikke har noen mulighet til å identifisere fysiske personer, vil dette lette adgangen til forskning. Tilnærmingen er dermed forsknings- og innovasjonsvennlig. Det vil tillate arbeid med individnivå-data uten personvernrisiko, støtte utvikling av KI og maskinlærings-applikasjoner, og muliggjøre validering av medisinske algoritmer på realistiske datasett.

At helsedata som *lagres* i SPE-er er pseudonymisert, kan videre forhindre muligheten for re-identifikasjon – som vil innebære brudd med regelverket i både EHDS og flere nasjonale lovkrav, herunder kunne medføre sanksjoner.

En slik løsning vil bidra til å oppfylle personvernforordningens krav om innebygget personvern.

Til sist har det en betydning for den praktiske implementeringen. Det vil redusere behovet for en omfattende manuell gjennomgang av alle datauttrekk, og automatisere personvernbeskyttelse gjennom tekniske tiltak.

REK

Legeforeningen mener det bør vurderes hvordan kriterielisten og søknadsprosessen for utlevering av helsedata kan kobles tettere til REK-prosessen, slik at bruk av helsedata skjer både sikkert og etisk forsvarlig. En slik felles informasjonsbase kan bidra til å effektivisere saksbehandlingen, redusere dobbeltarbeid for søker, og sikre bedre konsistens mellom de etiske og tekniske vurderingene før data tas i bruk.

Det foreslås en tilnærming hvor HDAB og REK behandler søknadene parallelt, med et felles innsendingspunkt og med en mekanisme som sikrer at utlevering av data ikke skjer før REK har gitt godkjenning, eller det er konkludert med at REK-godkjenning ikke er nødvendig.

For at en slik tilnærming skal være mulig, bør søkeren – i sin forespørsel om bruk av helsedata til sekundærformål – oppgi:

- Prosjektbeskrivelse og metadata, inkludert tittel, formål, prosjektleder/SPE-owner, organisasjon, varighet, samarbeidspartnere (med rolle og behandlingsgrunnlag), lagringsperiode og plan for sletting.
- Juridisk grunnlag for innhenting og utlevering av data
- Beskrivelse av datagrunnlaget, herunder inklusjons- og eksklusjonskriterier, planlagte koblinger og variabelliste.
- Beskrivelse av hvordan personopplysningene skal håndteres (SPE)

Finansiering

Mange av dagens dataansvarlige og forvaltere av helsedata mangler kapasitet og kompetanse til å imøtekomme kravene i EHDS-forordningen. I denne forbindelse bør det sikres forutsigbar finansering og nasjonal regulering av kostander for å sikre at datainnehaverne gjøres i stand til å overholde sine plikter.

Etter EHDS artikkel 50 nr. 2 skal det i nasjonal lovgivning bestemmes om aktører i artikkel 50 nr. 1, herunder *micro enterprises*, skal omfattes av plikten til å avlevere data etter artikkel 60.

Legeforeningen mener at slike virksomheter skal være unntatt avleveringsplikten, da dette vil være enda en administrativ oppgave som må prioriteres i mindre virksomheter som allerede er presset. For det tilfelle at det i nasjonal lovgivning besluttes at slike virksomheter skal være omfattet, må dette finansieres.

DEN NORSKE LEGEFORENING

Avsluttende kommentarer

Legeforeningen støtter intensjonen bak kriterielisten. Listen kan bli et verdifullt verktøy for å sikre trygg og ansvarlig sekundærbruk av helsedata i Norge, samtidig som den forbereder norske aktører på kommende EHDS-krav. Samtidig er det viktig at løsningen er praktisk anvendelig, og ivaretar krav til personvern. Det må arbeides med å konkretisere de tekniske spesifikasjonene, og fordelingen av roller og ansvar.

Med hilsen
Den norske legeforening
Jus- og arbeidsliv

Siri Skumlien
generalsekretær

Lars Duvaland
direktør, Jus og arbeidsliv

Saksbehandler: Mathias Gravdehaug, rådgiver/advokat

[1] Rettsakten er tidligere vurdert til å ikke være EØS-relevant og er derfor ikke tatt inn i EØS-avtalen. Forordningen gjelder beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer og byråer, og om fri utveksling av slike opplysninger.

[2] https://www.helsedirektoratet.no/rapporter/ehds-konsekvensvurdering--gapanalyse-pr.11.april-2025/styring-og-organisering, siste faglig endring 19. mai 2025.

DEN NORSKE LEGEFORENING

[3] EHDS fortalepunkt 72
[4] Rettsakten er tidligere vurdert til å ikke være EØS-relevant og er derfor ikke tatt inn i EØS-avtalen. Forordningen gjelder beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer og byråer, og om fri utveksling av slike opplysninger.
[5] EHDS artikkel 50 nr. 1 bokstav b
[6] EHDS artikkel 50 nr. 2

Dokumentet er godkjent elektronisk