

Databehandleravtale «FHI-NCD studien» (avtalen)

Databehandleravtale knyttet til «FHI-NCD studien» (avtalen)

Inngås mellom
Folkehelseinstituttet
Org. Nr. 983 744 516
Lovisenberggata 8
0456 OSLO
Norge
(behandlingsansvarlig)
Og
Navn på fastlege
(databehandler)

om behandling av personopplysninger («Avtalen») som databehandler skal foreta for
behandlingsansvarlig som følge av at behandlingsansvarlig deltar i PraksisNett.

Databehandleravtale må inngås når FHI ber andre parter om å behandle data på sine vegne. I FHI-NCD studien gjelder dette registrering av målinger av risikofaktorer i Nettskjema og håndtering av blodprøver og blodprøvesvar. Det er ment for å beskytte personopplysninger til deltagere.

Innledning (avtalens hensikt)

Avtalevilkårene i denne databehandleravtalen (avtalen) regulerer rettigheter og plikter for behandlingsansvarlig og databehandler, når det behandles personopplysninger på vegne av den behandlingsansvarlige i Nettskjema (som brukes til å registrere måleresultat i FHI-NCD studien) og rekvirering av blodprøver og mottak av blodprøvesvar.

Formålet med behandlingen, varigheten av behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte følger av vedlegg til Avtalen (Vedlegg A).

Avtalevilkårene er utformet for å sikre Partenes overholdelse av artikkel 28 nr. 3 i Europaparlaments- og rådsforordning (EU) 2016/679 vedtatt 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (GDPR) og Lov om behandling av personopplysninger av 15. juni 2018 nr.38 og tilhørende forskrifter (heretter Personvernregelverket). Der Avtalevilkårene inneholder ord og begreper som er definert i GDPR, har de samme betydning som i forordningen.

I forbindelse med aktivitet som beskrevet i Vedlegg A vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Avtalevilkårene.

Ved motstrid mellom Avtalevilkårene og de rammer som følger av Personvernregelverket eller annen relevant lovgivning, viker Avtalevilkårene.

Behandlingsansvarliges rettigheter og plikter

Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger utføres i samsvar med Personvernregelverket, relevant helselovgivning og Avtalevilkårene.

Den behandlingsansvarlige bestemmer formålet med og rammene for behandlingen av personopplysningene.

Den behandlingsansvarlige er ansvarlig for at det foreligger lovlig behandlingsgrunnlag for personopplysningene som databehandler behandler på vegne av behandlingsansvarlig.



Databehandleren skal følge behandlingsansvarliges instruks

Databehandleren skal kun behandle personopplysninger på instruks fra den behandlingsansvarlige. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at instruksen gitt av den behandlingsansvarlige er i strid med Personvernregelverket. Dersom databehandler overtrer bestemmelsene i Personvernregelverket ved selv å fastsette formålene med og midlene for behandlingen, skal databehandleren anses for å være behandlingsansvarlig med hensyn til nevnte behandling i henhold til GDPR artikkel 28 nr. 10. I tilfelle databehandleren behandler personopplysninger for egne formål (i kraft av å være lege) for å etterleve plikter som følger av ufravikelig lov, anses ikke slik behandling som brudd på denne Databehandleravtalen. Databehandler skal ikke behandle personopplysninger Databehandleren får tilgang til på annen måte enn det som er nødvendig for å utføre de oppdrag som Databehandler har for den Behandlingsansvarlige. Databehandleroppdraget er nærmere beskrevet under vedlegg A. Personopplysninger skal kun behandles i Nettskjema (som automatisk overføres til TSD). Databehandler skal ikke ha tilgang til TSD.

Konfidensialitet

Databehandlerer forpliktet til konfidensialitet. Det er kun databehandler som har tilgang til, og skal sende inn Nettskjema med personopplysninger m.m. Databehandleren skal på anmodning fra den behandlingsansvarlige dokumentere at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte forpliktelser.

Sikkerhet ved behandlingen

Den behandlingsansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til vurdert risiko i henhold til GDPR artikkel 32. I henhold til GDPR artikkel 32, skal databehandleren – uavhengig av den behandlingsansvarlige – vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandlingen og implementere tiltak for å redusere risikoen. For dette formål skal den behandlingsansvarlige på forespørsel gi databehandleren all informasjon som er nødvendig for å identifisere og vurdere slik risiko.

Videre skal databehandleren bistå den behandlingsansvarlige i å sikre overholdelse av den behandlingsansvarliges plikter etter GDPR artikkel 32-36.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Foreligger det godkjente adferdsnormer etter personvernforordningens artikkel 40 eller godkjent sertifiseringsordning etter artikkel 42, som Databehandleren har påtatt seg å overholde eller være sertifisert etter, plikter Databehandleren å etterkomme slike adferdsnormer eller sertifiseringskrav.

Tilgang til data for tredjepart

Dersom databehandler har behov for at tredjeparter skal ha tilgang til data må dette avklares og skriftlig avtales særskilt med behandlingsansvarlig.

Bistand til den behandlingsansvarlige

1. Databehandleren skal, i den grad det er mulig, bistå den behandlingsansvarlige med å oppfylle den behandlingsansvarliges plikt til å svare på henvendelser fra forskningsdeltakeren/ den registrerte med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel III. Databehandleren underretter straks den behandlingsansvarlige om enhver henvendelse fra de registrerte. Databehandleren skal ikke selv besvare henvendelser, med mindre den behandlingsansvarlige har gitt tillatelse til dette.

2. Databehandleren skal bistå den behandlingsansvarlige med overholdelse av:

- a. den behandlingsansvarliges plikt til å uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde brudd på personopplysnings-sikkerheten til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter,
- b. den behandlingsansvarliges plikt til å underrette om brudd på personopplysnings-sikkerheten til den registrerte, dersom det er sannsynlig at bruddet på person-opplysnings-sikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter,
- c. den behandlingsansvarliges plikt til å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet (en vurdering av personvernkonsekvenser - DPIA) i henhold til GDPR artikkel 35,
- d. den behandlingsansvarliges plikt til å rådføre seg med Datatilsynet (forhåndsdrøftinger) i henhold til GDPR artikkel 36.
- e. forpliktelsen til å sikre at personopplysningene er korrekte og oppdaterte, ved straks å underrette behandlingsansvarlig dersom databehandleren blir oppmerksom på at personopplysningene som behandles er ukorrekte eller er blitt foreldet.

Melding om brudd på personopplysningssikkerheten (info om personvern på FHI)

1. I tilfelle brudd på personopplysningssikkerheten, skal databehandleren underrette den behandlingsansvarlige uten ubegrunnet opphold.
2. Brudd på personopplysningssikkerheten vil si et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller til personopplysninger som er overført, lagret eller på annen måte behandlet, jf. GDPR artikkel 4 nr. 12. Dette kan for eksempel være datainnbrudd og omfattende forsøk på datainnbrudd, distribusjon av personopplysninger til uautoriserte mottakere, tyveri og annet tap av lagringsmedier (uavhengig av om disse er kryptert eller ikke).
3. Databehandleren skal bistå den behandlingsansvarlige i å melde brudd på personopplysningssikkerheten til Datatilsynet, hvilket omfatter at databehandleren skal bistå i å innhente informasjon i henhold til GDPR artikkel 33 nr. 3.
4. Brudd på personopplysningssikkerheten skal varsles til kontaktperson som angitt i Vedlegg A, både per e-post og telefon, med kopi til;
folkehelseinstituttet@fhi.no/folkehelseinstituttet@fhi.no. Behandlingsansvarliges personvernombud skal også varsles; Personvernombud@fhi.no.

Opphør av tilgang til personopplysninger (som del av studien)

Når behandling av personopplysninger ikke lenger er nødvendig for å oppfylle formålet med aktivitetene som fremgår av Vedlegg A, er databehandleren forpliktet til å opphøre all behandling av personopplysninger på vegne av Behandlingsansvarlig.

Når enkeltbrukere hos databehandler ikke lenger har behov for tilgang til Nettskjema, skal databehandler underrette behandlingsansvarlig slik at behandlingsansvarlig evt. kan fjerne tilgangen.

Sikkerhetsrevisjon og inspeksjoner

1. Databehandleren skal på forespørsel gjøre tilgjengelig for den behandlingsansvarlige all



informasjon som er nødvendig for å påvise overholdelse av pliktene som følger av GDPR artikkel 28 og Avtalevilkårene. Databehandler skal tillate og bidra til sikkerhetsrevisjoner, inkludert inspeksjoner, utført av den behandlingsansvarlige eller annen uavhengig tredjepart bemyndiget av den behandlingsansvarlige.

2. Etter relevant lovgivning kan et tilsynsorgan pålegge både behandlingsansvarlig og databehandler å fremlegge informasjon og gi tilgang som er nødvendig for at tilsynet skal kunne utføre sine oppgaver. Datatilsynets tilgang til lokaler og utstyr er hjemlet i GDPR artikkel 58 nr. 1 bokstav f.

Erstatning

1. Partene er ansvarlige overfor hverandre for eventuelle tap, kostnader og skader som oppstår på grunn av Partens unnlatelse av å overholde sine forpliktelser i henhold til denne Databehandleravtalen.
2. Ingen av Partene er ansvarlig for indirekte skade, følgeskade eller lignende skade som en annen Part pådrar seg.

Lovvalg og vernetting

Databehandleravtalen er underlagt norsk rett og Partene velger Oslo tingrett som vernetting. Dette gjelder også etter opphør av Databehandleravtalen.

Avtalens varighet

Denne Databehandleravtalen skal gjelde så lenge databehandler behandler personopplysninger på vegne av den behandlingsansvarlige (se vedlegg A: Behandlingen har følgende varighet).

VEDLEGG A: Instruks vedrørende behandling av personopplysninger

A.1. Bakgrunn og formål med behandlingen

Høyt blodtrykk, kolesterol, blodsukker og overvekt er blant de viktigste risikofaktorene for hjerte- og karsykdom, kreft, diabetes og KOLS. Likevel har vi begrenset kunnskap om forekomsten og utviklingen av disse risikofaktorene i den norske befolkningen.

Målet med denne pilotstudien er å teste en metode for innsamling av på risikofaktorer i primærhelsetjenesten og vurdere om dette kan danne grunnlag for en enkel og effektiv metode for å følge utviklingen av risikofaktorer i befolkningen. I denne sammenheng vil databehandler måle og registrere personopplysninger, slik som blant annet risikofaktorer og fødselsnummer.

A.2. Behandlingsaktiviteter

Databehandleren skal utføre følgende behandlingsaktiviteter på vegne av den behandlingsansvarlige:

- Rekruttere deltakere til studien fra (hver deltagende fastlege) sin pasientliste
- Registrere personopplysninger og verdier av målte risikofaktorer m.m i Nettskjema
- Sende ett Nettskjema per deltager, og med det automatisk oversende personopplysninger og helsedata til TSD for lagring
- Dele resultater om høyde, vekt, midje og hoftemål og blodtrykksnivå med deltakerne



Rekvirere og oversende blodprøver til Fürst for analyse

A.3. Type personopplysninger

Behandlingen omfatter følgende kategorier av personopplysninger om de registrerte:

Direkte identifiserbare personopplysninger

Navn (i forbindelse med rekruttering)

Fødselsnummer/personnummer

Indirekte identifiserbare personopplysninger

Fødselsår

Kjønn

Fastlegekontor

Tid siden sist måltid

Om høyde er selvrapportert (ja/nei)

Helseopplysninger

Høyde

Vekt

Midjemål

Hoftemål

Blodtrykksmålinger

Om pasienten har tatt blodprøve og eventuell begrunnelse hvis ikke

HbA1c

Totalkolesterol

LDL-kolesterol

HDL-kolesterol

Triglyserider

Andre opplysninger avtalen omfatter

Dette er ikke-personopplysninger, men tekniske og administrative studievariabler som inngår i datagrunnlaget.

Blodtrykksapparat brukt

Mansjettstørrelse brukt

Kalibreringsstatus for blodtrykksapparat

Om høyde og vekt ble målt etter protokoll (ja/nei)

Om midje og hofte ble målt etter protokoll (ja/nei)

Om blodtrykk ble målt etter protokoll (ja/nei)

MA

A.4. Behandlingen omfatter følgende kategorier av registrerte

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig omfatter følgende kategorier av registrerte:

Gruppen personer opplysningene gjelder er pasienter til utvalgte fastleger som er tilfeldig trukket ut fra pasientlister, er i alderen 18–70 år uten langtkommen demens og terminal sykdom (eksklusjonskriterier) og samtykket til deltakelse i Prosjektet. Behandlingen omfatter personopplysninger om ca. 300 deltagende pasienter fordelt på omtrent 20 fastlegekontor.

A.5. Behandlingen har følgende varighet

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig varer frem til databehandler har utført oppdraget og uansett ikke lengre enn endelig sluttdato, 30.11.2027. Om endelig sluttdato inntreffer før Databehandleren har utført oppdraget sitt må all databehandling på vegne av Behandlingsansvarlig opphøre umiddelbart, med mindre annet er skriftlig avtalt.

A.6. Behandlingssted

Databehandlers behandling av personopplysninger i henhold til denne databehandleravtalen skal kun foregå på Nettskjema. Dette innebærer at databehandler ikke skal ta skjermbilde, laste ned data eller på annen måte eksportere data, med unntak av resultatmål (høyde, vekt, midje og hoftemål og blodtrykksnivå).

Disse opplysningene skal printes ut og deles med deltager og ikke tas vare på med mindre ufravikelig lovgivning pålegger fastlege å beholde opplysningene for andre formål. Denne behandlingen er da ikke en del av databehandleroppdraget som gjøres på vegne av FHI.

Prosjektnummer TSD: p3660, FHI-NCD studien.

A.7. Instruks for behandling av personopplysninger i tredjestat eller hos internasjonal organisasjon

Personopplysninger skal ikke overføres til tredjestater eller internasjonale organisasjoner.

A.8. Den Behandlingsansvarliges kontaktopplysninger

Prosjektleder FHI-NCD:

Karianne Svendsen

E-postadresse: karianne.svendsen@fhi.no

Telefon: 950 26 445

Personvernombud:

Kjersti Haugan

E-postadresse: Personvernombud@fhi.no

Telefon: 951 07 312

Informasjonssikkerhetsansvarlig:

Pål Jakob Solerød

E-postadresse: ciso@fhi.no

Telefon: 911 77 265

A.8 Kontaktopplysninger databehandler

Navn på legekantor

Adresse til legekantor

Telefonnummer legekantor

Signer for å godkjenne databehandlingsavtalen

Følgende informasjon om deg er hentet automatisk fra BankID for å kunne knytte samtykket til deg:

Navn

Ditt fødselsnummer

Lest og godkjenner databehandlingsavtalen

Ja

Nei, jeg ønsker ikke å delta

Kopi av digitalt signert avtale leveres til den digitale postkassen til den som signerer, og lagres i en egen mappe i TSD prosjektet tilknyttet FHI-NCD prosjektet.

Signering med BankID

For å gi et signert samtykke, blir du videresendt til Postens signeringstjeneste. Her kan du evt. lese gjennom samtykket på nytt og kan signere dette digitalt med BankID.

Etter signering blir det sendt en kopi av samtykket til din digitale postkasse.

For å endre dette samtykket, kan du logge inn i samtykkeportalen:

<https://consent-portal.tsd.usit.no>

FHI (behandlingsansvarlig)

Behandlingsansvarlig bekrefter at denne avtalen er gjennomgått og godkjent på vegne av Folkehelseinstituttet v/Avdelingsdirektør Avdeling for kroniske sykdommer, Marte Handal. Avtalen anses bindene og trer i kraft når databehandler har signert.

MHandal
MARTE HANDAL
AVD. DIR AVDELING FOR KRONISKE SYKDOMMER
FHI

Generert: 2026-01-05 13:38:09.

MH