UiO : Universitetet i Oslo

AVTALE OM BEHANDLING AV PERSONOPPLYSNINGER

Lagring av forskningsdata i Tjeneste for Sensitive Data

1. Avtalens parter

1.1 Parter

Avtalen inngås mellom databehandlingsansvarlig: (navn på prosjekt) Driving with cerebral palsy – medical and neuropsychological determinants of fitness to drivenavn på prosjekt/Bilkjøring og CP – kritiske faktorer/Sunnaas sykehus HF (Org.nr.: 883 971 752) (heretter kalt behandlingsansvarlig) og databehandler: Tjenester for Sensitive Data ved UiO (Org.nr. 971 035 854) (heretter kalt TSD).

1.2 Kontaktpersoner:

Kontaktperson hos Behandlingsansvarlig:
Sissel Ertenstein, sissel.ertenstein@sunnaas.no / 975 33 905, informasjonssikkerhetsleder.

Kontaktperson hos databehandler: : Gard Thomassen, gardot@usit.uio.no / 93674926, Tjenestegruppeadministrator for TSD. Prøv først tsd-drift@usit.uio.no.

2. Formålet med avtalen

Tjenester for Sensitive Data tilbyr lagringstjeneste til forskere i Norge som forsker på personsensitive data, inkludert helsedata.

Formålet med avtalen er å regulere rettigheter og plikter etter:

- Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (hlsregl.),
- Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (popplyl.), og
- Forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften).

Avtalen regulerer TSDs behandling og sikring av person- og helseopplysninger som er tilgjengeliggjort av behandlingsansvarlig. Det skal fremgå klart dersom TSD kan overlate opplysninger til andre for oppbevaring, bearbeiding eller annen bruk.

Behandlingens formål skal ikke endres av noen av partene uten at ny avtale er signert.

Tittel på prosjektet: Driving with cerebral palsy – medical and neuropsychological determinants of fitness to drive.

3. Partenes ansvarsområde under helseregisterloven og personopplysningsloven med forskrifter

Driving with cerebral palsy – medical and neuropsychological determinants of fitness to drive/Sunnaas sykehus HF er i henhold til lov om helseregistre og behandling av helseopplysninger § 2 nr 8 og personopplysningsloven § 2 nr 4 å anse som Behandlings-ansvarlig.

Den behandlingsansvarlige har ansvar for å påse at krav, herunder krav til sikkerhet, som stilles i helseregisterloven, personopplysningsloven og personopplysningsforskriften er oppfylt. Det innebærer blant annet også at Behandlingsansvarlig har ansvaret for å påse at kravene er

oppfylt i forbindelse med oppbevaring og bruk av helse- og sensitive personopplysningene hos Databehandleren,.

Databehandleren er å anse som databehandler etter helseregistre og behandling av helseopplysninger § 2 nr. 9 og personopplysningsloven § 2 nr. 5, og kan kun behandle helse- og personopplysninger tilgjengeliggjort av Behandlingsansvarlig i henhold til denne avtale. Eventuell annen bruk av helse- og personopplysningene skal i forkant avtales skriftlig med Behandlingsansvarlig.

Databehandleren skal sikre at helse- og personopplysninger tilgjengeliggjort av Behandlingsansvarlig holdes atskilt fra egne og andres opplysninger og tjenester.

4. Beskrivelse av formålet med bruken av databehandler

Databehandleren kan bare behandle personopplysningene i henhold til de formål som er bestemt av den Behandlingsansvarlig og i samsvar med de vilkår som fremgår av denne avtalen.

Deltakerne i studien, dvs. de som svarer på spørsmålene/spørreskjemaene i prosjektet via Nettskjema, er tidligere førerkortvurderingspasienter med cerebral parese på Sunnaas sykehus HF i perioden 2008-2013. Formålet er å sammenstille aktuelle data fra Nettskjema med medisinske og nevropsykologiske data fra deres førerkortvurderingsopphold på Sunnaas i perioden 2008-2013. Resultatene vil som i annen forskning brukes i vitenskapelige publikasjoner, presenteres på relevante konferanser, kurs og møter og andre relevante fora som CP-Bladet og CP-Foreningens hjemmesider.
Prosjektet er behandlet i REK (prosjekt nr. 2017/1359 REK Sør-Øst C), der de konkluderte med følgende: «Prosjektet kan gjennomføres uten godkjenning av REK innenfor de ordinære ordninger for helsetjenesten med hensyn til for eksempel regler for taushetsplikt og personvern.»
Koblingen mellom data fra Nettskjema og data fra førerkortvurderingen deltakerne gjennomgikk i 2008-2013 ble godkjent av Personvernombudet 21.10.17.

5. Spesifisering av data som skal behandles

Deltakerne i studien svarer på spørsmål som omhandler bilrelaterte forhold så som førerkortopplæringen, bil og tilpasninger i bil og kjøreatferd/kjørestil. Deltakerne får også spørreskjemaer som omhandler helserelaterte forhold så som egenvurdering av kognitiv og eksekutive funksjon, grad av egenopplevde smerter og trettbarhet og livskvalitet.
I det første spørsmålet i Nettskjemaet bes deltakerne skrive inn sitt unike IDNR som de får tilsendt i mailen med linken til Nettskjemaet (f.eks. IDNR 001, 002 osv.). Prosjektleder oppbevarer en innelåst papirliste med de unike IDNR i prosjektet og respektive navn på deltakerne.

6. Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet og internkontroll, samt tilgangskontroll, etter bestemmelsene i helseregisterloven, personopplysningsloven og

personopplysningsforskriften.

Databehandleren skal sikre at all behandling av helse- og personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av Behandlingsansvarlig. Som en del av dette skal Databehandler legge fram risikovurderinger av egen sikkerhet.

Det forutsettes at databehandler har definert sikkerhetsmål, -strategi, -organisering og ansvar i samsvar med helseregisterloven, personopplysningsloven og personopplysningsforskriften og at dette følges opp med nødvendig internkontrollsystem.

Sikkerhetsbrudd eller mistanke om sikkerhetsbrudd, skal umiddelbart rapporteres til den Behandlingsansvarlig.

Databehandleren skal ha klare rutiner for logging av feil og avvik i systemer som brukes til å behandle helse- og personopplysninger, og som er omfattet av denne avtalen. Dersom det avdekkes slike feil eller avvik, skal Databehandleren så snart som mulig, og senest innen 24 timer (48 timer dersom hendelse oppstår i helg eller på offentlig helligdag), varsle Behandlingsansvarlig om dette. Databehandleren skal i et slikt tilfelle straks igangsette tiltak for å minimere mulig skade for Behandlingsansvarlig.

Behandlingsansvarlig kan til enhver tid kreve dokumentasjon av Databehandleren for å forsikre seg om at Databehandleren overholder alle relevante krav i helseregisterloven, personopplysningsloven og personopplysningsforskriften vedrørende informasjonssikkerhet. Behandlingsansvarlig kan kreve tilgang til Databehandlerens rapporter mv knyttet til periodiske revisjoner av sine prosedyrer og rutiner.

Databehandler skal kunne fremvise gode rutiner knyttet til informasjonssikkerhet, herunder særlig teknisk sikkerhet, tilgangskontroll, og fysisk sikkerhet.

Behandlingsansvarlig er ansvarlig for tilstrekkelig sikkerhet på enhetene som benyttes til fjernaksess til TSD. I mange tilfeller vil dette tilsi at enhetene må være i Behandlingsansvarliges eller nært tilknyttedes driftsregime mtp. oppdateringer og viruskontroll.

7. Behandlingsansvarliges rett til innsyn, inspeksjon og testing

Behandlingsansvarlig skal ha rett til innsyn i og verifikasjon av hvordan løsningen er sikret. Med innsyn menes dokumentasjon, intervjuer, møte, samt eventuelle andre former for verifikasjon som kan være hensiktsmessig. Databehandleren aksepterer at innsyn kan gjennomføres av Behandlingsansvarlig eller den tredjepart Databehandlingsansvarlig måtte velge til gjennomføring så fremt dette kun strekker seg til det området dedikert til behandling av behandlingsansvarliges data. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten som leveres Databehandlingsansvarlig.

Databehandleren forplikter seg på fire ukes varsel å utlevere eller på annen måte sørge for

mulighet for innsyn i sikkerhetsmessig dokumentasjon relevant for Behandlingsansvarlig.

Dersom Behandlingsansvarlig gjør bruk av retten til innsyn og avvik i sikring av Databehandlers systemer oppdages, skal Databehandleren så raskt det er mulig korrigere avvik.
Databehandleren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

8. Taushetsplikt

Partene skal bevare taushet om alle konfidensielle opplysninger, noens personlige forhold, sikkerhetsmessige og forretningsmessige forhold, opplysninger som kan skade en av partene eller som kan utnyttes av utenforstående.

Taushetsplikten gjelder partenes ansatte og andre som handler på partenes vegne i forbindelse med gjennomføringen av kontrakten. Alle ansatte skal ha undertegnet taushetserklæring.

Partene plikter å ta de forholdsregler som er nødvendig for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.
Ansatte og andre som fratrer sin tjeneste hos en av databehandlerne skal pålegges taushet også etter fratredelse om forhold som nevnt over.

Denne bestemmelsen gjelder også etter avtalens opphør.

9. Ikrafttredelse, varighet og opphør

9.1 Ikrafttredelse og varighet

Avtalen trer i kraft når den er signert av begge parter, og kan sies opp med 3 måneders skriftlig varsel.

9.2 Opphør

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle helse- og personopplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne avtalen, med mindre annet er avtalt med Behandlingsansvarlig.

Databehandler skal slette alle dokumenter, data, harddisker, cd-er og andre lagringsmedier som inneholder opplysninger som omfattes av avtalen. Sletting skal gjennomføres slik at opplysningene ikke kan gjenfinnes. Dette gjelder også for eventuelle sikkerhetskopier.

10. Mislighold

Mislighold foreligger dersom en av partene ikke oppfyller sine plikter etter denne avtalen og dette ikke skyldes forhold som den andre parten har ansvaret for eller risikoen for.
Dersom en av partene ønsker å påberope seg mislighold, skal dette meddeles den andre parten skriftlig uten ugrunnet opphold.

Ved mislighold kan den krenkede part holde tilbake sin motytelse, men ikke åpenbart mer enn det som synes påkrevd for å avhjelpe virkningene av misligholdet, og bare inntil forholdet er brakt i overensstemmelse med avtalen.

Hvis det foreligger vesentlig mislighold, kan den andre parten – etter å ha gitt skriftlig varsel og rimelig frist til å bringe forholdet i orden – heve hele eller deler av avtalen med øyeblikkelig virkning og kreve erstatning for eventuelle tap dette har medført.

11. Overdragelse av rettigheter og plikter

Behandlingsansvarlig kan helt eller delvis overdra sine rettigheter og plikter etter avtalen til en annen norsk statlig virksomhet, som da er berettiget til tilsvarende vilkår. Databehandleren kan kreve å få dekket eventuelle merutgifter som er forbundet med overdragelsen.

Databehandleren kan overdra sine rettigheter og plikter etter avtalen med skriftlig samtykke fra Behandlingsansvarlig. Slikt samtykke kan ikke nektes uten saklig grunn. Rett til vederlag etter avtalen kan fritt overdras, men overføring fritar ikke Databehandleren for hans plikter og ansvar.

12. Rettsvalg og verneting

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne avtalen skal behandles ved de ordinære domstoler. Oslo tingrett vedtas som verneting.

13. Signering

Denne avtale er undertegnet i 2- to- eksemplarer, hvorav hver part beholder 1- ett- eksemplar.

Sted, den Nesodden, 03.11.17	Oslo, den 8/11-17
Behandlingsansvarlig (signatur)	TSD, UIO (signatur)
Sissel Ertenstein	Lars Oftedal
Navn: Sissel Ertenstein (med trykte bokstaver)	Navn: ...Lars Oftedal..... (med trykte bokstaver)
Stilling: Informasjonssikkerhetsleder	Stilling:.....IT-dir, UiO/USIT.....