

Databehandleravtale for forskningsprosjekt mellom Universitetet i Oslo (org nr 993 467 049) og Akershus universitetssykehus HF (org nr. 983 971 636)

1	Kontraktens parter.....	1
2	Formål og virkeområde for avtalen.....	1
3	Varighet og oppsigelse.....	1
4	Partenes ansvarsområde.....	2
5	Ved opphør av avtalen.....	2
5.1	Tilbakelevering av data.....	2
5.2	Sletting eller destruering av data.....	2
6	Beskrivelse av formålet med bruken av data.....	2
7	Spesifisering av aktuelle data.....	2
8	Kontaktpersoner.....	3
9	Krav til informasjonssikkerhet.....	3
9.1	Krav til teknisk sikkerhet.....	3
9.2	Krav til tilgangskontroll.....	3
9.3	Krav til fysisk sikkerhet.....	4
9.4	Krav om rett til innsyn, inspeksjon og testing.....	4
10	Taushetsplikt.....	4
11	Mislighold og sanksjoner.....	5
12	Ansvar for underleverandører.....	5
13	Overdragelse av rettigheter og plikter.....	5
14	Rettsvalg og vernetting.....	5
15	Hjemmelsgrunnlag.....	5
	Undertegning.....	6

1 Kontraktens parter

Kontrakten inngås mellom Akershus universitetssykehus HF som databehandlingsansvarlig (heretter kalt Ahus) og Tjenester for sensitive data (TSD) ved USIT, Universitetet i Oslo (heretter kalt Databehandler).

2 Formål og virkeområde for avtalen

Formålet med kontrakten er å regulere TSD (databehandler) sin bruk og sikring av personopplysninger som er tilgjengeliggjort av Ahus. Det skal fremgå klart dersom Databehandleren kan overlate personopplysninger til andre for oppbevaring, bearbeiding eller annen bruk.

Tittel på prosjektet: **NorCAPITAL**

Prosjektleder: Vegard Bruun Wyller, professor/overlege, Barne- og ungdomsklinikken, Akershus universitetssykehus. Tlf: 91 16 66 81. Epost: v.b.wyller@medisin.uio.no

Formell referanse til prosjektet:

- REK-nr: 2009/2541
- Personvernombud ved Ahus: 14-084

Informasjon som utleveres i henhold til avtalen kan være lagret i forskjellig format (fil, system, applikasjon eller server) og kalles heretter Datasystemet.

3 Varighet og oppsigelse

Avtalen trer i kraft når den er signert av begge parter og har en varighet til 2026 i henhold til REK vedtak. Avtalen kan videre sies opp med 3 måneders varsel.

4 Partenes ansvarsområde

Ahus er i henhold til Lov om behandling av personopplysninger (personopplysningsloven) å anse som Ahus, jf lovens § 2 nr 4 og pkt 15. i herværende avtale.

Ahus er også ansvarlig for tilleggskrav som fremgår av:

- o helseregisterloven,
- o personopplysningsforskriften (forskriften)
- o norm for informasjonssikkerhet i helse-, omsorgs og sosialsektoren (Normen) www.normen.no

Det innebærer at Ahus har ansvar for å påse at kravene er oppfylt i forbindelse med oppbevaring og bruk av personopplysningene hos Databehandleren, jf personopplysningsloven § 15 og forskriften § 2-15. Omfatter datasettet pasientopplysninger som kan knyttes til enkeltpersoner gjennom kodelister, personnummer, NPR-nummer, telefonnummer eller liknende, gjelder helseregisterloven i tillegg til personopplysningsloven med forskrifter osv iht. Normen.

Databehandleren er ansvarlig etter personopplysningsloven § 2 nr 5, og kan kun behandle personopplysninger tilgjengeliggjort av Ahus i overensstemmende med denne avtale, jf personopplysningsloven § 15. Eventuell annen bruk av personopplysningene skal forhåndsavtales særskilt i form av skriftlig avtale med Ahus.

Sikringsmekanismer må etableres mellom personopplysninger som skriver seg fra forskjellige prosjekter, både fra egen og andre virksomheter.

Databehandler skal om avtalen har lengre varighet enn 3 år, hvert 3. år gi Ahus skriftlig melding om at opplysningene fremdeles lagres i henhold til personopplysningsloven og avtalen her, jf personopplysningsloven § 31 tredje ledd. Dette gjelder også om det ikke er gjort endringer.

5 Ved opphør av avtalen

5.1 Tilbakelevering av data

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle helseopplysninger som er mottatt på vegne av Ahus og som omfattes av denne avtalen, med mindre annet er avtalt med Ahus.

5.2 Sletting eller destruering av data

Databehandler skal slette og destruere 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.

6 Beskrivelse av formålet med bruken av data

Kronisk utmattelsessyndrom (CFS/ME) er et betydelig helseproblem blant ungdom. De underliggende sykdomsmekanismene er i stor grad ukjente, men tidligere forskning har blant annet dokumentert endring i viktige reguleringssystemer: det autonome nervesystemet, hormonsystemet og immunsystemet. Disse endringene kan føre til endret aktivitet i en rekke ulike gener, noe som igjen kan bidra til onde sirkler og slik vedlikeholde symptomene. Den underliggende årsaken til avvikende reguleringssystemer kan være endringer i hjernens automatiske responser. NorCAPITAL sikter mot en grundig kartlegging av disse sykdomsmekanismene. Vi fokuserer spesielt på to perspektiver: a) Endringer i genaktivitet i blodet, noe som særlig kartlegges gjennom sekvensering av RNA-molekyler og b) Endringer i hjernens automatiske responser, noe som særlig kartlegges gjennom funksjonelle MR-undersøkelser (fMRI).

7 Spesifisering av aktuelle data

Datainnsamlingen, journal og laboratoriedata fra pasientene, er ferdigstilt. Data er innhentet fra pasienter ved OUS. Data oppbevares aidentifisert ved TSD, kodenøkkel oppbevares på Ahus.

8 Kontaktpersoner

Følgende kontaktpersoner er oppnevnt i forbindelse med denne avtalen:

Databehandlingsansvarlig:

Prosjektleder: Vegard Bruun Wyller, professor/overlege, Barne- og ungdomsklinikken, Akershus universitetssykehus. Tlf: 91 16 66 81. E-post: v.b.wyller@medisin.uio.no

Databehandleren:

Prosjektadministrator: Gard Thomassen, Tjeneste for sensitive data (TSD) ved USIT, UiO, Tlf: 22 84 09 34. E-post: g.o.s.thomassen@usit.uio.no

9 Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2. For helseopplysninger må krav til tilgang sikres iht krav fastsatt i Normen.

Databehandleren skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av Ahus. Gjennomført risikovurdering skal fremlegges av databehandler for egen og eventuelle underleverandørers sikkerhet som del av dette jf. Normen, fakta ark nr. 7 risikovurdering.

Det forutsettes at Databehandler har definert sikkerhetsmål, -strategi, -organisering og ansvar i samsvar med Normen og tilhørende faktaark, og at dette følges opp med nødvendig internkontrollsystem.

Kompromittering eller mistanke om kompromittering av opplysningene, skal umiddelbart rapporteres til Ahus sitt personvernombud for forskning.

Databehandleren skal ha klare rutiner for logging av feil og avvik som er av betydning for Ahus' informasjonssikkerhet 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, varsle Ahus om dette, og straks igangsette tiltak for å minimere mulig skade for Ahus.

Ahus kan til enhver tid kreve dokumentasjon vedrørende informasjonssikkerhet hos Databehandleren for å forsikre seg om at Databehandleren overholder alle relevante krav som fremgår av Normen. Ahus kan kreve tilgang til Databehandlerens rapporter knyttet til periodiske revisjoner av prosedyrer og rutiner.

9.1 Krav til teknisk sikkerhet

Følgende krav stilles til teknisk sikkerhet:

- Tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord.
- Lagring av opplysninger overlevert av Ahus skal sikres slik at kun autoriserte medarbeidere har tilgang.
- Sensitive personopplysninger skal sikres mot uaktsom utlevering.
- Best mulige tekniske tiltak bør etableres for å forhindre at sensitive personopplysninger kan flyttes ut av sikrede områder på godkjent lagringssted.
- Kommunikasjon skal sikres med kryptering dersom den går over usikre nettverk og det sendes sensitive personopplysninger.

9.2 Krav til tilgangskontroll

Databehandleren har ansvar for at eget personell (eller underleverandører som denne benytter) med elektronisk tilgang til data fra Ahus, alltid skal ha underskrevet taushetserklæring før tilgang gis. Denne skal angi eksplisitt at taushetsplikten også gjelder etter at oppdraget er avsluttet og inntil Ahus eventuelt skriftlig opphever taushetsplikten for vedkommende.

Databehandleren skal ha rutiner for tilgangsautorisasjon og -styring som sikrer at bare de av Databehandlerens medarbeidere som har reelt behov får tilgang til Datasystemet. Tilgangsnivå skal

være i henhold til reelt behov knyttet til å gjennomføre leveransen. Databehandler skal til enhver tid ha oversikt over eget personell som er autorisert for tilgang til Ahus informasjon og tjenester ved å føre lister som kan fremvises på forespørsel. På forespørsel skal slik oversikt fremlegges for Ahus. Dersom Ahus har innvendinger mot at en gitt person har fysisk og/eller elektronisk adgang til Datasystemet, skal autorisasjon for denne personen inndras.

Dersom Databehandleren benytter bærbare klientmaskiner til drift, skal Databehandleren ha rutiner som sikrer at disse bare benyttes til brukerstøtte eller support fra programleverandør evt. via fjernaksess

Dersom tredjepart eller underleverandør i forbindelse med brukerstøtte eller tilsvarende skal ha tilgang til Datasystemet, skal det benyttes midlertidige passord eller tilsvarende. Dette skal endres/sperres umiddelbart når behovet for tilgang opphører. Databehandler skal på forespørsel kunne fremskaffe oversikt over hvem hos underleverandørene som har fått tilgang til data som tilhører Ahus.

9.3 Krav til fysisk sikkerhet

Det skal benyttes adgangskontroll med bruk av adgangskort med personlig kode eller tilsvarende. Adgangskontroll til begrensede områder (f.eks. drift og serverrom) skal være basert på faktiske behov. Personell som ikke er autoriserte, skal følges. Adgangskontroll med låste dører gjelder for følgende typer lokaler: datahall/serverrom, IT lokaler (drift/support), lokaler med IT relatert utstyr (koblingsmatriser, svitsjer/rutere), eller liknende.

9.4 Krav om rett til innsyn, inspeksjon og testing

Ahus skal ha rett til innsyn i og verifikasjon av hvordan løsningen er sikret dvs. foreta stedlig revisjon. Med innsyn menes dokumentasjon, intervjuer, møtereferater, tester, sikkerhetsovervåking av nettverkstrafikk og aktivitet på server samt eventuelle andre former for verifikasjon som kan være hensiktsmessig. Databehandleren aksepterer at innsyn kan gjennomføres av Ahus eller den tredjepart Ahus måtte velge til gjennomføring. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten som leveres til Ahus.

Databehandleren forplikter seg på to ukers varsel å utlevere eller på annen måte sørge for innsyn i sikkerhetsmessig dokumentasjon relevant for Ahus. Dersom Ahus gjør bruk av retten til innsyn, og avvik i sikring av Datasystemet oppdages, skal Databehandleren uten ugrunnet opphold korrigere avvik. Databehandleren skal skriftlig redegjøre for korrigerende tiltak og plan for gjennomføringen. Databehandleren skal som en del av kontrakten vederlagsfritt bidra med relevant personell og nødvendig omfang av innsats ved oppfølging og rettelser av avvik relatert til sikkerhet i Datasystemet. Dette gjelder når avvik og eventuelle behov for rettelser skyldes handlinger eller mangel på slike hos Databehandleren eller underleverandører denne måtte benytte.

10 Taushetsplikt

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

Taushetsplikten gjelder partenes ansatte og andre som handler på partenes vegne i forbindelse med gjennomføringen av avtalen. Alle ansatte skal ha undertegnet taushetserklæring (taushetserklæringene skal gi tilsvarende dekning som Ahus egne taushetserklæringer). Kopi av taushetserklæring skal fremlegges på forespørsel og eventuelt korrigeres ved behov. Partene plikter å ta de forholdsregler som er nødvendig for å sikre at opplysninger i Datasystemet ikke blir gjort kjent for andre.

Taushetsplikten gjelder også etter at kontrakten er opphørt. Ansatte og andre som fratrer sin tjeneste hos Databehandler skal pålegges taushet også etter fratrede om forhold som nevnt over uten tidsbegrensning.

11 Mislighold og sanksjoner

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 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.

12 Ansvar for underleverandører

Dersom en av partene engasjerer underleverandører til å utføre ytelser som følger av denne avtalen, er parten selv fortsatt fullt ansvarlig for utførelsen av disse ytelsene på samme måte som om parten selv stod for utførelsen. Ahus skal skriftlig forhåndsgodkjenne Databehandlers bruk av underleverandører. Databehandleren skal sørge for at underleverandører undertegner og forplikter seg til å følge Ahus sin databehandleravtale, herunder taushetsplikten.

13 Overdragelse av rettigheter og plikter

Ahus kan helt eller delvis overdra sine rettigheter og plikter etter avtalen til en annen norsk offentlig virksomhet, som da er berettiget til å tre inn i avtalen på samme 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 forhåndssamtykke fra Ahus. 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.

14 Rettsvalg og vernetting

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. Nedre Romerike tingrett vedtas som vernetting.

15 Hjemmelsgrunnlag

- helseregisterloven, Lov om helseregistre og behandling av helseopplysninger LOV 2001-05-18 nr 24
- personopplysningsforskriften: Forskrift om behandling av personopplysninger FOR-2000-12-15-1265
- personopplysningsloven: Lov om behandling av personopplysninger LOV 2000-04-14 nr 31
- norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Normen)
www.normen.no, er et omforent sett av krav til informasjonssikkerhet basert på lovverket og er en bransjenorm

Undertegning

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

Nordbyhagen, den 26/6-14

Oslo, den 27-14

Akershus universitetssykehus HF

Tjenester for Sensitive Data,

Universitetet i Oslo

Hilde Lurås
Databehandlingsansvarlig (signatur)

Lars Oftedal
Databehandleren (signatur)

(med trykte bokstaver)

(med trykte bokstaver)

Stilling: Direktør for forskning og innovasjon

Stilling: IT-DIR, UIO

Navn: Hilde Lurås

Navn: LARS I. OFTEDAL