Oslo universitetssykehus | Databehandleravtale

Databehandleravtale mellom Oslo universitetssykehus HF (org nr. 993 467 049) ved MBT-Kvalitetslaboratorium og _____[Sett inn foretak]

1 Kontraktens parter

Kontrakten inngås mellom databehandlingsansvarlig _____[Sett inn foretak] (heretter kalt Databehandlingsansvarlig) og Oslo universitetssykehus HF ved MBT-Kvalitetslaboratorium (heretter kalt Databehandler).

Saksnummer hos Databehandler: 2013/4282.

2 Hensikt med og virkeområde for avtalen

Hensikten med avtalen er å regulere rettigheter og plikter etter Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften).

Avtalen regulerer Databehandlerens bruk og sikring av helseopplysninger som er tilgjengeliggjort av Databehandlingsansvarlig. Det skal fremgå klart dersom Databehandleren kan overlate helseopplysninger til andre for oppbevaring, bearbeiding eller annen bruk.

3 Partenes ansvarsområde under helseregisterloven og personopplysningsloven med forskrifter

Den databehandlingsansvarliges ansvar er definert i henhold til lov om helseregistre og behandling av helseopplysninger, jf lovens § 2 nr 8. Den databehandlingsansvarlige har ansvar for å påse at krav, herunder krav til sikkerhet, som stilles i helseregisterloven og personopplysningsforskriften er oppfylt. Det innebærer blant annet også at Databehandlingsansvarlig har ansvaret for å påse at kravene er oppfylt i forbindelse med oppbevaring og bruk av helseopplysningene hos Databehandleren, jf helseregisterloven § 18 og personopplysningsforskriften § 2-15, jf. helseregisterloven § 36.

Databehandleren er å anse som databehandler etter helseregisterloven § 2 nr 9 og kan kun behandle helseopplysninger tilgjengeliggjort av Databehandlingsansvarlig i henhold til denne avtale, jf helseregisterloven § 18. Eventuell annen bruk av helseopplysningene skal i forkant avtales skriftlig med Databehandlingsansvarlig.

Databehandleren skal sikre at helseopplysninger tilgjengeliggjort av Databehandlingsansvarlig holdes atskilt fra egne og andres opplysninger og tjenester.

4 Beskrivelse av formålet med bruken av databehandler

MBT-kvalitetslaboratorium skal kvalitetssikre pågående MBT-psykoterapier utført av psykoterapeuter i Norge, med henblikk på etterlevelse og kompetanse i henhold til prinsipper for mentaliseringsbasert terapi. MBT-terapeuter sender inn lyd- og billedopptak av psykoterapi (data) i henhold til vår prosedyre for bruk av MBT-kvalitetslaboratorium (se vedlegg: "Prosedyre for bruk av MBT-kvalitetslaboratorium"). Opptak skal observeres av personell ansatt i MBT-kvalitetslaboratorium, og danner grunnlaget for en klinisk tilbakemelding som MBT-kvalitetslaboratorium skriver og returnerer til innsender sammen med innsendt datamateriale. Opptak skal ikke kobles til annen type personopplysninger.

5 Data som skal overføres

Data som skal overføres er minnepinner og dvder med opptak av psykoterpitimer. Pasientens identitet er ikke direkte identifiserbar. Data skal overføres i henhold til prosedyre for bruk av MBT-kvalitetslaboratorium hvilket innebærer sending per post. (se vedlegg : "Internprosedyre for håndtering av innsendt data").

6 Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet og internkontroll i helseregisterloven §§ 16 og 17 og personopplysningsforskriften kapittel 2. Tilgang til helseregisteret skal reguleres i henhold til helseregisterloven § 13.

Databehandleren skal sikre at all behandling av helseopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av Databehandlingsansvarlig. Som en del av dette skal Databehandler legge fram risikovurderinger av egen og eventuelle underleverandørers sikkerhet.

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

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

Databehandleren skal ha klare rutiner for logging av feil og avvik i systemer som brukes til å behandle helseopplysninger, 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 Databehandlingsansvarlig om dette. Databehandleren skal i et slikt tilfelle straks igangsette tiltak for å minimere mulig skade for Databehandlingsansvarlig.

Databehandleren skal ha klare rutiner for oppfølging av ansatte som urettmessig tilegner seg helseopplysninger, jf. helseregisterloven § 13a.

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

6.1 Krav til teknisk sikkerhet

Det stilles følgende krav til teknisk sikkerhet:

- Tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord. Tilgang til helseopplysninger skal være basert på 2-nivå autentisering.
- Kun autoriserte medarbeidere skal ha tilgang til helseopplysninger som er omfattet av denne avtalen.
- All tilgang til helseopplysninger omfattet av denne avtalen skal logges.
- Helseopplysninger skal sikres mot uaktsom utlevering. Tekniske tiltak skal være på plass for å forhindre at helseopplysninger kan flyttes ut av sikker sone eller fra godkjent lagringssted.
- Sikkerhet skal ivaretas ved fjerndrift av Databehandlers systemer. Alt utstyr som brukes ved fjerndrift skal være eid av Databehandler. Det skal benyttes kryptert VPN-forbindelse med sperring mot samtidig tilgang til internett. Utstyr som benyttes i forbindelse med fjerntilgang skal ikke brukes av venner, familie eller andre uautoriserte personer.
- 2-nivå autentisering skal benyttes dersom tilgang til Databehandlers systemer skjer via usikre nettverk.
- Kommunikasjon skal sikres med kryptering dersom den går over usikre nettverk.

6.2 Krav til tilgangskontroll

Databehandleren har ansvar for at personell (hos Databehandleren eller underleverandører som denne benytter) med elektronisk tilgang til Databehandlers systemer, alltid skal ha underskrevet taushetserklæring før tilgang gis. Taushetsplikten gjelder også etter at oppdraget er avsluttet og inntil Databehandlingsansvarlig eventuelt skriftlig opphever taushetsplikten for vedkommende.

Databehandleren skal ha rutiner for tilgangsautorisasjon og -styring som sikrer at bare de av Databehandlerens medarbeidere som et reelt behov for tilgang til systemet og helseopplysningene, har tilgang. 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 Databehandlingsansvarliges informasjon og tjenester. På forespørsel skal slik oversikt forelegges Databehandlingsansvarlig.

Dersom Databehandlingsansvarlig har innvendinger mot at en gitt person har fysisk og/eller elektronisk adgang til systemet, skal autorisasjon for dette inndras.

Databehandler skal ha rutiner og teknisk mulighet til å sperre tilgang til en registrerts opplysninger dersom den registrerte ønsker det, jf. pasientrettighetsloven § 5-3 og helsepersonelloven §§ 25 og 45.

Dersom tredjepart eller underleverandør i forbindelse med support eller tilsvarende skal ha tilgang til systemet, skal det benyttes midlertidige passord eller tilsvarende. Dette skal endres/sperres umiddelbart når behovet for tilgang opphører.

6.3 Krav til fysisk sikkerhet

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

6.4 Krav om rett til innsyn, inspeksjon og testing

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

Databehandleren forplikter seg på to ukes varsel å utlevere eller på annen måte sørge for mulighet for innsyn i sikkerhetsmessig dokumentasjon relevant for Databehandlingsansvarlig.

Dersom Databehandlingsansvarlig gjør bruk av retten til innsyn og avvik i sikring av Databehandlers systemer oppdages, skal Databehandleren uten ugrunnet opphold korrigere avvik. Databehandleren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring. Databehandleren skal som en del av kontrakten vederlagsfritt bidra med relevant personell og nødvendig omfang av innsats ved oppfølgning og rettelser av avvik relatert til sikkerhet i systemene. Dette gjelder når avvik og eventuelle behov for rettelser skyldes handlinger eller mangel på slike hos Databehandleren eller underleverandører denne måtte benytte.

7 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 i næringsvirksomhet.

Taushetsplikten gjelder partenes ansatte og andre som handler på partenes vegne i forbindelse med gjennomføringen av kontrakten. Alle ansatte skal ha undertegnet taushetserklæring. Ansatte som har tilgang til helseopplysninger skal være pålagt taushetsplikt etter helseregisterloven § 15. For øvrig skal taushetserklæringene skal gi

tilsvarende dekning som Databehandlingsansvarliges 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 materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

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

8 Varighet og oppsigelse

Avtalen trer i kraft på det tidspunkt signert versjon sendes til MBT Kvalitetslaboratorium fra den databehandlingsansvarlige sammen med opptaket som skal vurderes. Avtalen opphører i det MBT Kvalitetslaboratorium har returnert opptaket til den databehandlingsansvarlige. Dersom behovet gjelder flere opptak fra samme terapeut(er) som er navngitt i denne avtalens punkt 4, og behovet er gjentagende over et lengre tidsrom, gjelder avtalen fra første opptak er sendt til Databehandler og til 12 kalendermåneder etter dette. Deretter må avtalen fornyes ved behov ihht. prosedyren.

9 Ved opphør

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle opptak / data som er mottatt på vegne av den Databehandlingsansvarlige og som omfattes av denne avtalen, med mindre annet er avtalt med Databehandlingsansvarlig.
Databehandler skal slette eller forsvarlig 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.

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.

11 Sanksjoner ved mislighold

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.

Databehandler kan ikke under noen omstendighet sperre Databehandlingsansvarligs tilgang til helseopplysninger i helseregisteret.

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 Databehandler benytter seg av underleverandører eller andre som ikke normalt er ansatt hos Databehandler skal dette avtales skriftlig med Databehandlingsansvarlig før behandlingen av personopplysninger starter. En slik avtale bør gjøres som et tillegg til denne avtalen.

Samtlige som på vegne av Databehandler utfører oppdrag der bruk av de aktuelle helseopplysningene inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

13 Overdragelse av rettigheter og plikter

Databehandlingsansvarlig 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 Databehandlingsansvarlig. 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 Kontaktpersoner

Følgende kontaktpersoner er oppnevnt i forbindelse med denne avtalen:

- hos Databehandlingsansvarlig:

  _____

- hos Databehandleren: Kjetil Bremer tlf: 23016972 epost: kjetil.bremer@ous-hf.no. Daglig leder MBT-kvalitetslaboratorium

15 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.

16 Undertegning

Ved første gangs bruk av MBT-kvalitetslaboratoriums tjenester inngås denne avtalen. Denne signeres av en med myndighet til dette hos den databehandlingsansvarlige og terapeuten som ønsker bistand fra MBT-lab. Det nederste feltet blir stående åpent til signatur fra nivå – 3 leder ved Oslo Universitetssykehus.

Signert avtale sendes i retur til MBT-kvalitetslaboratorium med videomateriale og rekvisisjon.

Neste gang den databehandlingsansvarlige ønsker MBTs bistand, sendes kun "*forenklet databehandleravtale*" til terapeuten pr. epost, Denne signeres av terapeuten og returneres til OUS sammen med opptaket.

Signatur Databehandleransvarlig: _____ Dato:_____

Navn og stilling med blokkbokstaver: _____

Signatur Terapeut: _____ Dato:_____

Navn og stilling med blokkbokstaver: _____

Signatur N-3 Leder OUS: _____Dato:_____

Navn og stilling med blokkbokstaver: _____