



UiO • Universitetet i Oslo

P71

**AVTALE OM BEHANDLING AV
PERSONOPPLYSNINGER**

**Lagring av forskningsdata i Tjeneste for
Sensitive Data**

Elektronisk tilgang til pasientjournal

1. Avtalens parter

1.1 Parter

Avtalen inngås mellom databehandlingsansvarlig: Nasjonalt senter for samhandling og telemedisin, Universitetssykehuset Nord-Norge HF (Org.nr 983974899) (heretter kalt Databehandlingsansvarlig) og Databehandler: Tjenester for Sensitive Data ved UiO (Org.nr. 971 035 854) (heretter kalt TSD).

1.2 Kontaktpersoner:

Kontaktperson hos Databehandlingsansvarlig: Tove Sørensen, tove.sorensen@telemed.no, mob. 91195696, prosjektleder.

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

2. Formålet med avtalen

Avtalen regulerer TSDs behandling og sikring av person- og helseopplysninger som er tilgjengeliggjort av Databehandlingsansvarlig i forbindelse med prosjektet «Elektronisk tilgang til pasientjournal».

Tjenester for Sensitive Data tilbyr lagringstjeneste til forskere og andre 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).

Det skal fremgå klart av denne avtale dersom TSD skal gjøre bruk av underleverandører og dersom TSD skal kunne overlate person- og helseopplysninger til underleverandører eller andre for oppbevaring, bearbeiding eller annen behandling av dataene.

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

Tittel på prosjektet: Elektronisk tilgang til pasientjournal.

3. Partenes ansvarsområde under helseregisterloven og personopplysningsloven med forskrifter

Universitetssykehuset Nord-Norge HF er i henhold til lov om helseregistre og behandling av helseopplysninger § 2 nr 8 og personopplysningsloven § 2 nr 4 å anse som Databehandlingsansvarlig.

T.h.

Den Databehandlingsansvarlige 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 Databehandlingsansvarlig har ansvaret for å påse at kravene er oppfylt i forbindelse med oppbevaring og bruk av helse- og sensitive personopplysninger hos Databehandler.

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

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

4. Beskrivelse av formålet med bruken av databehandler

Databehandler kan ikke behandle personopplysningene på annen måte enn det som er skriftlig avtalt med Databehandlingsansvarlig i denne avtalen.

Formålet med bruken av dataene er å prøve ut en pilotteneste, tilbudt av Universitetssykehuset Nord-Norge i samarbeid med helsenorge.no (Helsedirektoratet), for å gi pasienter innsyn i egen sykehusjournal via helsenorge.no. Dataene skal også brukes til å evaluere pilotpasientenes erfaringer med bruk av tjenesten, og for å kunne kontakte pasientene for dybdeintervjuer (basert på samtykke fra pasienten ved registrering som deltaker i prosjektet) i etterkant.

5. Spesifisering av data som skal behandles

Prosjektdeltakernes navn, adresse, fødselsnummer, mobilnummer, e-postadresse (frivillig), samtykkeerklæring til å delta i prosjektet, eventuelt samtykke til å bli kontaktet for dybdeintervju i etterkant og tilbakerapporteringsskjema for erfaringer med bruk av tjenesten som tilbys i prosjektet (frivillig) skal registreres. Dataene er direkte identifiserbare. Fødselsnummeret er nødvendig for å kunne vite hvilke personer som skal få tilgang til tjenesten under helsenorge.no (manuell innrapportering av fødselsnumrene fra prosjektansvarlig til helsenorge.no).

Dersom Databehandlingsansvarlig finner det nødvendig å endre data som skal behandles, eller legge ny type data til det som skal behandles, må det foretas en ny sikkerhetsvurdering. Dersom endringen er vesentlig, kan ikke endringen skje uten at ny databehandleravtale er signert.

6. Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet og internkontroll, samt tilgangskontroll, slik det fremgår av bestemmelsene i helseregisterloven, personopplysningsloven, personopplysningsforskriften og annet relevant regelverk.

Databehandler skal sikre at all behandling av helse- og personopplysninger 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 og annen dokumentasjon av egne sikkerhetsforanstaltninger.

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 Databehandlingsansvarlige.

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 den Databehandlingsansvarlige om dette. Databehandleren skal i et slikt tilfelle straks igangsette tiltak for å minimere mulig skade for Databehandlingsansvarlig.

Databehandlingsansvarlig 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. Databehandlingsansvarlig kan kreve tilgang til Databehandlerens rapporter m.v. knyttet til periodiske revisjoner av prosedyrer og rutiner.

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

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

7. Databehandlingsansvarliges 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, samt eventuelle andre former for verifikasjon som kan være hensiktsmessig. Databehandleren aksepterer at innsyn kan gjennomføres av Databehandlingsansvarlig eller den tredjepart Databehandlingsansvarlig måtte velge til gjennomføringen, så fremt dette kun strekker seg til det området dedikert til behandling av Databehandlingsansvarliges data. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten som leveres Databehandlingsansvarlig.

Databehandleren forplikter seg til på fire 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 så raskt det er mulig korrigere avvik. Databehandleren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

T. Ly.

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 i næringsvirksomhet eller annet.

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 fratrede 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.

Den gjelder til prosjektet er avsluttet eller til den sies opp av en av partene med tre 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 Databehandlingsansvarlige og som omfattes av denne avtalen, med mindre annet er avtalt med Databehandlingsansvarlig.

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.

T.h.

11. 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.

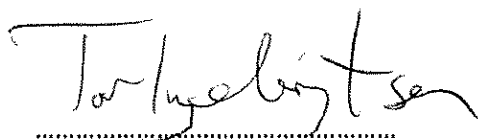
12. Rettsvalg og vernetting

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. Oslo tingrett vedtas som vernetting.

13. Signering

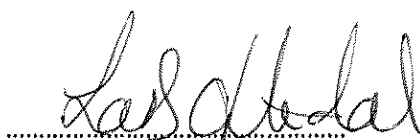
Denne avtale er undertegnet i 2- to- eksemplarer, hvorav hver part beholder 1- ett- eksemplar.

Tromsø, den 24.11.2014



Tor Ingebrigtsen
(med trykte bokstaver)
Databehandlingsansvarlig
Stilling: Administrerende direktør,
Universitetssykehuset
Nord-Norge HF

Oslo, den 29/5-2015



Lars Oftedal
(med trykte bokstaver)
Databehandler
Stilling: IT-dir, UiO/USIT