Mal:

Databehandleravtale

i henhold til personopplysningsloven § 15 og
personopplysningsforskriften kapittel 2

om behandling av person- og helseopplysninger

mellom

Databehandlingsansvarlig, org.nr. ... ...
(" databehandlingsansvarlige")

og

Databehandler, org. nr. ... ...
("databehandler")

1. Avtalens formål

Denne avtalen gjelder for tjenesteoppdrag som omfatter behandling av person- og helseopplysninger som er tilgjengelig på utstyr/løsning som eies, leies eller på annen måte disponeres av den databehandlingsansvarlige.

Formålet er å regulere hvordan databehandleren skal behandle person- og helseopplysninger på vegne av den databehandlingsansvarlige, jf. personopplysningsloven[1] § 15. Avtalen skal sikre at opplysningenes ikke brukes urettmessig og at konfidensialitet, integritet og tilgjengelighet ivaretas under oppdraget. Avtalen skal videre sikre at partene ivaretar tilfredsstillende informasjonssikkerhet og internkontroll iht bestemmelsene:.

2. Forholdet til andre avtaler

Norm for informasjonssikkerhet i helse- og omsorgstjenesten ("Normen")[2] er bindende for databehandler.

Denne avtalen supplerer andre avtaler som er inngått mellom partene, for eksempel kjøps- og leieavtaler, tjenestenivåavtaler (SLA), serviceavtaler, oppdragsavtaler og avtale om tilgang til utstyr.

Når det gjelder informasjonssikkerhet ved databehandling av person- og helseopplysninger skal bestemmelsene i denne avtalen ha forrang fremfor bestemmelser i andre avtaler, med mindre alternative bestemmelser gir et sterkere vern av opplysningene enn bestemmelsene her.

[1] Lov av 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[2] ehelse.no/normen

3. Tilgang til person- og helseopplysninger

Databehandleren gis tilgang til person- og helseopplysninger enten ved personlig oppmøte og bruk av utstyret til den databehandlingsansvarlige eller ved fjerntilgang. I begge tilfeller gjelder tilgangen for et spesifisert databehandleroppdrag. Tilgangen skal ikke benyttes til andre formål.

Helse Vest IKT AS er ansvarlig for etablering og drift av fjerntilgang over datanettverket. Leverandøren skal følge de krav Helse Vest IKT AS stiller til brukere av fjerntilgang.

4. Behandling av person- og helseopplysninger

Person- og helseopplysninger omfatter opplysninger om noens legems- eller sykdomsforhold, jf. helsepersonelloven[3] §§ 21 flg. Videre omfattes også opplysninger om noens personlige forhold, jf. forvaltningsloven[4] § 13 første ledd, og opplysninger om pasienters fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, jf. spesialisthelsetjenesteloven[5] § 6-1 andre ledd.

Med *behandling* av person- og helseopplysninger menes enhver bruk, for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. personopplysningsloven § 2 nr. 2 eller pasientjournalloven § 2 bokstav b eller helseregisterloven § 2 bokstav c). Også sikkerhetskopiering, testing, analytisk bearbeiding av opplysninger og bruk av opplysninger i opplæring regnes som behandling av person- og helseopplysninger.

Databehandleren skal ikke behandle person- og helseopplysninger på annen måte enn det som er avtalt skriftlig med den databehandlingsansvarlige.

Databehandler kan ikke benytte tredjepart (underleverandører) i sin behandling av personopplysninger for Databehandlingsansvarlig, uten at dette på forhånd er skriftlig avtalt med Databehandlingsansvarlig. Dersom tredjepart engasjeres, er Databehandler ansvarlig for utførelsen på samme måte som om han selv stod for utførelsen.

5. Krav til informasjonssikkerhet

Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet i personopplysningsloven § 13 eller pasientjournalloven § 22 eller helseregisterloven § 21 og personopplysningsforskriften kapittel 2. For helseopplysninger må krav til tilgang sikres iht Norm for informasjonssikkerhet i helsesektoren.

Det forutsettes at virksomheten har definert sikkerhetsmål, -strategi, -organisering og ansvar i samsvar med personopplysningsloven og –forskriften og at dette følges opp med nødvendig internkontrollsystem.

Databehandlingsansvarlig plikter å ha kunnskap om sikkerhetsstrategien hos Databehandler, og skal jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet. Databehandlingsansvarlig kan for å oppfylle denne plikten gjennomføre sikkerhetsrevisjoner hos Databehandler.

Databehandlingsansvarlig har rett til å la en tredjepart revidere Databehandlers informasjonssikkerhet. Kostnadene for dette skal dekkes av Databehandlingsansvarlig.

Databehandler skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av Databehandlingsansvarlig. Gjennomført risikovurdering skal fremlegges av Databehandler for egen og eventuelle underleverandørers sikkerhet som del av dette.

Dersom Databehandlingsansvarlig anser at sikkerhetsnivået hos Databehandler ikke er tilfredsstillende, plikter Databehandler å justere sikkerhetsnivået etter instruks fra Databehandlingsansvarlig.

Kompromittering eller mistanke om kompromittering av opplysningene, skal umiddelbart rapporteres til

[3] Lov av 02.07.1999 nr. 64 om helsepersonell m.v. (helsepersonelloven).
[4] Lov av 10.02.1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).
[5] Lov av 02.07.1999 nr. 61 om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven).

Databehandlingsansvarlig.

Databehandler plikter å informere Databehandlingsansvarlig dersom det skjer endringer i sikkerhetsstrategien som vil kunne påvirke kravene i denne avtalen eller i andre samhandlingsavtaler mellom partene. På samme måte plikter Databehandlingsansvarlig å informere Databehandler ved endringer i sikkerhetsstrategien som vil kunne påvirke kravene i denne avtalen eller i andre samhandlingsavtaler mellom partene.

Databehandler skal ha klare rutiner for logging av feil og avvik som er av betydning for Databehandlingsansvarliges informasjonssikkerhet og som er omfattet av denne avtalen. Dersom det avdekkes slike feil eller avvik, skal Databehandler så snart som mulig, og senest innen 24 timer, varsle Databehandlingsansvarlig om dette. Databehandler skal i et slikt tilfelle straks igangsette tiltak for å minimere mulig skade for Databehandlingsansvarlig.

Databehandlingsansvarlig kan til enhver tid kreve dokumentasjon hos Databehandler for å forsikre seg om at Databehandler overholder alle relevante krav i personopplysningsloven og –forskriften vedrørende informasjonssikkerhet. Databehandlingsansvarlig kan kreve tilgang til Databehandlers rapporter mv knyttet til periodiske revisjoner av sine prosedyrer og rutiner.

6. Overføring av personopplysninger til utlandet

Dersom personopplysninger skal lagres utenfor Norge må man være spesielt oppmerksom på kravene i personopplysningsloven kapittel 5 og personopplysningsforskriften kapittel 6. Eventuell lagring av data i utlandet må vurderes særskilt av databehandlingsansvarlig.

7. Formål og beskrivelse av behandlingen av person- og helseopplysninger

7.1 Følgende opplysninger skal eller kan behandles

.....
.....
.....

7.2 Følgende behandlinger skal eller kan utføres

.....
.....
.....

7.3 Følgende roller autoriseres til å utføre behandlingen

.....
.....
.....

7.4 Beskrivelse av løsningen / utstyr

.....
.....
.....

8. Taushetsplikt

Alle ansatte som gjennomfører tjenesteoppdrag etter avtalen her skal undertegne taushetserklæring, jf. vedlegg til denne avtalen. Signerte taushetserklæringer skal arkiveres av enten databehandlingsansvarlig eller databehandler.

9. Avvik og sikkerhetsrevisjon

Tilfeller av sikkerhetsbrudd og rutinesvikt skal behandles som avvik, jf. personopplysningsforskriften § 2-6. Databehandleren skal umiddelbart informere den behandlingsansvarlige om avvik. Avtalepartene skal deretter gjennomføre de tiltak som er nødvendige for å gjenopprette normal drift, fjerne årsaken til avviket og hindre gjentakelse. Databehandleren skal bistå med kompetent personell og andre tilgjengelige ressurser.

Avviksbehandlingen skal dokumenteres skriftlig.

Dersom avviket har ført til uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig skal Datatilsynet varsles.

For å forebygge avvikshendelser har den databehandlingsansvarlige rett til å revidere databehandlers sikkerhetstiltak. Den databehandlingsansvarlige kan utføre revisjonen selv eller benytte en ekstern revisor etter eget valg. Den databehandlingsansvarlige dekker kostnadene ved ekstern revisor. Ved gjennomføringen av revisjon skal databehandlerens rettmessige kommersielle og tekniske interesser ivaretas.

Databehandlingsansvarlig skal ha tilgang til resultat av sikkerhetsrevisjoner.

Dersom behandlingen går ut over det som er avtalt i punkt 6 og 7skal databehandleren informere den databehandlingsansvarlige om dette umiddelbart.

Behandlingen kan bare fortsette når det er inngått en skriftlig tilleggsavtale med oppdaterte opplysninger vedrørende punkt 6 og 7.

10. Varighet og opphør

Dersom behandlingen av helse- og personopplysninger opphører, så skal Databehandler tilrettelegge for og medvirke til overføring av alle opplysninger som Databehandler har behandlet på vegne av Databehandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til og bekreftet mottatt av Databehandlingsansvarlig, skal Databehandler slette opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer.

Databehandler skal gi Databehandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over

11. Avtalebrudd(mislighold) og erstatning for økonomiske utlegg

Avtalebrudd foreligger dersom en part ikke oppfyller sine forpliktelser etter avtalen, og dette ikke skyldes forhold som den andre parten har ansvaret eller risikoen for. Den som vil påberope seg avtalebrudd må meddele dette til den annen part med skriftlig begrunnelse, uten ugrunnet opphold etter at det aktuelle forholdet ble kjent.

Dersom en part i vesentlig grad misligholder sine forpliktelser etter avtalen kan den andre parten heve avtalen. Den som ønsker å heve skal i skriftlig varsel sette en rimelig frist for retting av forholdet. Av varselet skal det fremgå at avtalen vil bli hevet dersom forholdet ikke er rettet innen fristen.

Overtredelse av taushetsplikt vil alltid anses som vesentlig mislighold.

Dersom avtalebrudd fører til økonomisk tap i form av økte utgifter eller reduserte inntekter, kan den skadelidte parten kreve at motparten dekker tapet.

12. Meddelelser og kontaktpersoner

Alle meddelelser som gis i henhold til denne avtalen skal være skriftlige. Andre språk enn norsk kan bare brukes dersom det er avtalt.

Avsender plikter å vurdere om meddelelsen har et slikt innhold at den skal unntas offentlighet på grunn av personopplysninger eller næringsopplysninger, jf. forvaltningsloven §§ 13 flg.

Følgende kontaktpersoner er oppnevnt i forbindelse med avtalen.

For den databehandlingsansvarlige:

Navn, rolle, kontaktinformasjon

For databehandleren:

Navn, rolle, kontaktinformasjon

Skifte av kontaktperson skal så snart som mulig meddeles skriftlig til den andre parten.

13. Rettsvalg og verneting

Denne avtalen reguleres av norsk rett.

Partene skal søke å løse tvister gjennom forhandlinger. Tvister som ikke er løst innen 60 dager etter at en part har satt frem krav om forhandlinger, kan hver av partene bringe inn for de ordinære domstoler. <…..Tingrett> vedtas som verneting.

14. Undertegning

Denne avtalen undertegnes i to eksemplarer og partene beholder ett hver.

_____	_____
Sted og dato	Sted og dato
_____	_____
Databehandlingsansvarlig Stilling og navn	Databehandler Stilling og navn