Databehandleravtale

mellom

Os kommune, 3430

("**Dataansvarlig**")

og

Helseplattformen AS

("**Databehandler**")

hver for seg også benevnt "**Part**" og i fellesskap "**Partene**".

1. BAKGRUNN

I forbindelse med anskaffelse av ny og felles pasientjournalløsning i Midt-Norge, skal helse- og personopplysninger migreres fra gammel til ny IT-løsning. Migreringen utføres av Helseplattformen AS som er forvaltningsorganisasjonen med ansvar for innføring -, og videre forvaltning av ny pasientjournalløsning.

Denne databehandleravtalen ("**Databehandleravtalen**") regulerer all behandling av Personopplysninger, inkludert Helseopplysninger, Databehandleren gjør på vegne av Dataansvarlig i forbindelse med migrering til ny løsning.

Databehandleravtalen skal sikre at Personopplysninger blir behandlet i samsvar med:

- Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven) som implementerer Forordning EU 2016/679 ("**Personvernforordningen**")
- Lov av 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven)
- Lov av 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp ("**Pasientjournalloven**")
- Den til enhver tid gjeldende versjon av Norm for informasjonssikkerhet i helse og omsorgstjenesten ("**Normen**")
- Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten av 28. oktober 2016 nr. 1250
- Annen lovgivning som får anvendelse for behandling av Personopplysninger i Norge.

Listen over lovgivning ovenfor er heretter referert til som ("**Gjeldende Helse- og Personvernlovgivning**").

Begreper som er skrevet med stor forbokstav i Databehandleravtalen skal ha samme betydning som fastsatt i Gjeldende Helse- og Personvernlovgivning med mindre annet fremgår eksplisitt.

2. BESKRIVELSE AV BEHANDLINGEN

Databehandler behandler Personopplysninger i den utstrekning dette er nødvendig i forbindelse med migreringen. De overordnede formålene med behandlingen av Personopplysninger, typer Personopplysninger og kategorier av Registrerte er angitt i er angitt i Vedlegg 1.

3. DATAANSVARLIGES PLIKTER

Dataansvarlig skal etablere rutiner i egen virksomhet for blant annet å

(i) påse at det foreligger et behandlingsgrunnlag etter Gjeldende Helse- og Personvernlovgivning for at Personopplysningene behandles for de formål som fremkommer av Vedlegg 1 og Databehandlers protokoller,

(ii) utarbeide protokoller over behandlingen, jf. Personvernforordningen artikkel 30 nr. 1,

(iii) foreta nødvendige risikovurderinger av migreringsaktivitetene,

(iv) ivareta de Registrertes rettigheter, herunder rett til informasjon og innsyn og til å få Personopplysninger slettet eller korrigert. Databehandler plikter i nødvendig utstrekning å bistå Dataansvarlig med effektuering av innsyn, retting eller sletting.

Dataansvarlig skal straks melde fra til Databehandler om forhold som vil kunne medføre behov for endringer i den måten Databehandler behandler Personopplysninger på.

4. DATABEHANDLERS PLIKTER

4.1 Etterlevelse av regelverket

Databehandleren skal opptre i samsvar med Gjeldende Helse- og Personvernlovgivning.

Databehandleren skal ikke, verken ved handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at denne misligholder noen av bestemmelsene i Gjeldende Helse- og Personvernlovgivning.

Databehandleren skal samarbeide med og yte rimelig bistand til Dataansvarlig for å sikre at Dataansvarlig oppfyller kravene i Gjeldende Helse- og Personvernlovgivning.

Databehandleren skal behandle Personopplysninger bare på dokumenterte instrukser fra Dataansvarlig.

4.2 Begrensninger vedrørende bruk

Databehandler skal ikke behandle Personopplysninger utover det som kreves for oppfyllelse av sine forpliktelser overfor Dataansvarlig.

Databehandler skal påse at Personopplysninger ikke utleveres til en tredjepart med mindre Dataansvarlig har gitt instruks om dette eller i tilfeller hvor det er pålagt ved lov. Denne bestemmelsen er ikke til hinder for utlevering til en tredjepart som opptrer som en underleverandør i henhold til Databehandleravtalen pkt. 4.7 eller i tilknytning til personell som er innleid og som er underlagt Databehandlers instruksjonsmyndighet.

Databehandler får ingen rettigheter til Personopplysninger som Databehandler får tilgang til som ledd i migreringsaktivitetene.

4.3 Informasjonssikkerhet

Databehandleren skal gjennomføre tekniske og organisatoriske tiltak som er egnet for å oppnå et sikkerhetsnivå som står i forhold til risikoen behandlingen representerer, jf. Personvernforordningen artikkel 32. Tiltakene skal sikre konfidensialitet, integritet og tilgjengelighet for Personopplysninger i henhold til Pasientjournalloven § 22 og Normen, så langt dette regelverket får anvendelse.

Databehandler forplikter seg til å følge opp risiko som er identifisert i risikovurderingen som er gjort forut for migreringen. Der risikovurderingen peker på tiltak som er nødvendige for å holde risikoen på et akseptabelt nivå, forplikter Databehandler seg til å implementere disse tiltakene. Risikovurderingen utgjør vedlegg 2 til denne Databehandleravtalen.

Gjennomføres en eller flere nye risikovurderinger i forbindelse med migreringen skal disse risikovurderingene også være vedlegg til denne databehandleravtalen.

4.4 Håndtering av sikkerhetsbrudd

Enhver mistanke om eller oppdagelse av et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet i tilknytning til migreringen, skal varsles til Dataansvarlig. Slikt varsel skal gis uten ugrunnet opphold etter at bruddet eller mistanken om bruddet har oppstått. Varslet skal inneholde den informasjonen som kreves etter Personvernforordningen artikkel 33 nr. 3.

Dataansvarlig har ansvaret for at sikkerhetsbrudd meldes til Datatilsynet og berørte Registrerte. Databehandler skal på anmodning fra Dataansvarlig bistå i denne forbindelse.

Databehandler skal ha på plass rutiner og systematiske prosesser for å følge opp sikkerhetsbrudd, som skal omfatte gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse.

4.5 Sikkerhetsrevisjoner

Databehandler skal minst årlig gjennomføre sikkerhetsrevisjoner av systemer og utstyr som benyttes ved behandling av Personopplysninger. Databehandler kan velge å la en autorisert tredjepart gjennomføre revisjonen. Revisjonen skal omfatte, men ikke være begrenset til, en vurdering av Databehandlers oppfyllelse av sikkerhetsrelaterte plikter som er fastsatt i denne Databehandleravtalen (jf. pkt. 4.3 og Vedlegg 1) og Databehandlers bruk av underleverandører

(jf. pkt. 44.7). Resultatet fra sikkerhetsrevisjon skal dokumenteres og rapporten skal gjøres tilgjengelig for Dataansvarlig senest 1 måned etter at den foreligger.

Databehandler skal på forespørsel fra Dataansvarlig legge til rette for at Dataansvarlig kan gjennomføre en sikkerhetsrevisjon hos Databehandler. Dataansvarlig kan bestemme at sikkerhetsrevisjonen skal gjennomføres av en uavhengig tredjepart i henhold til anerkjente standarder for sikkerhetsrevisjon. Dataansvarlig eller oppnevnt tredjepart skal undertegne Databehandlers taushetserklæring forut for slik revisjon og oppnevnt tredjepart kan ikke være en direkte konkurrent av Databehandler.

4.6 Overføring av Personopplysninger til utlandet

Databehandler skal ikke overføre Personopplysninger til et land utenfor EØS-området, som ikke sikrer et tilstrekkelig beskyttelsesnivå i henhold til Personvernforordningen artikkel 45 ("**Tredjeland**") uten skriftlig forhåndssamtykke og fullmakt fra Dataansvarlig.

Dersom Dataansvarlig har gitt skriftlig samtykke til overføring av Personopplysninger til et Tredjeland, plikter Databehandler etter fullmakt fra Dataansvarlig å inngå EUs standardkontrakt for overføring av Personopplysninger til tredjeland (2010/87/EC) eller andre bestemmelser som erstatter 2010/87/EC-bestemmelsene. Dataansvarlig kan også samtykke til overføring på grunnlag av andre instrumenter som utgjør et rettslig grunnlag for overføringen i henhold til Gjeldende Helse- og Personvernlovgivning.

Databehandler plikter å påse at behandling av Personopplysninger i et Tredjeland ikke skjer før Databehandler (etter fullmakt fra Dataansvarlig), som eksportør av data, og den ikke-EØS-baserte underleverandøren som dataimportør, har signert EUs standardkontrakt for overføring til tredjeland.

4.7 Bruk av underleverandører

Databehandler kan inngå avtaler med underleverandører for oppfyllelse av sine forpliktelser overfor Dataansvarlig. Dataansvarlig har på tidspunktet for signering av Databehandleravtalen samtykket til bruk av de underleverandører som er eksplisitt nevnt i Vedlegg 1 pkt. D). Dersom Databehandler vil engasjere en ny underleverandør eller gjøre endringer i listen over underleverandører, skal Databehandler varsle Dataansvarlig senest 21 dager før underleverandøren starter behandling av Personopplysninger. Dataansvarlig kan innen 14 dager etter at skriftlig varsel er mottatt motsette seg endringen. Dataansvarlig kan, dersom det er nødvendig for å få gjennomført nødvendige sikkerhetsvurderinger, be om 14 dagers utsettelse av fristen (til sammen 28 dager). Endring av underleverandør skal alltid skje i form av skriftlig aksept fra Dataansvarlig. Databehandler skal på forespørsel gi Dataansvarlig innsyn i navnelister over personell som underleverandøren stiller til Databehandlers disposisjon.

Databehandler kan benytte konsulenter fra andre virksomheter ved behandling av Personopplysninger under denne Databehandleravtalen, forutsatt at konsulentene er underlagt Databehandlers instruksjonsmyndighet og tilgang til Personopplysninger utelukkende gis fra Databehandlers godkjente lokaler som er avsatt til formålet. Det samme gjelder en underleverandørs bruk av konsulenter fra andre virksomheter. Skriftlig forhåndssamtykke fra Dataansvarlig er ikke nødvendig for bruk av konsulenter i tråd med denne bestemmelsen, og det er heller ikke krav om noen databehandleravtale med virksomheten konsulentene er innleid fra.

Databehandler skal påse at aksepterte underleverandører påtar seg ansvar i samsvar med forpliktelsene som angitt i denne Databehandleravtalen.

4.8 Taushetsplikt

Databehandleren har taushetsplikt vedrørende dokumentasjon og Personopplysninger som Databehandleren får tilgang til under Databehandleravtalen. Taushetsplikten er lovfestet når det kommer til håndtering av Helseopplysninger, jf. Pasientjournalloven § 15.

Databehandler skal påse at alt personell og andre som måtte være involvert i behandlingen av Personopplysninger under Databehandleravtalen er kjent med og forpliktet av taushetsplikten under denne Databehandleravtalen.

Personer som ikke er bundet av en lovfestet taushetsplikt skal signere en taushetserklæring forut for tilgang til Personopplysninger. Dette er Databehandlers ansvar.

Denne bestemmelsen gjelder også etter opphør av Databehandleravtalen.

4.9 Varslingsforpliktelser

Databehandleren skal uten ugrunnet opphold etter å ha blitt klar over forholdet, skriftlig varsle Dataansvarlig:

(i) ved mistanke om at Dataansvarliges instruksjoner er i strid med Gjeldende Helse- og Personvernlovgivning;
(ii) dersom en hendelse medfører at Databehandlers evne til å utføre behandlingen i tråd med Gjeldende Helse- og Personvernlovgivning eller Databehandleravtalen svekkes eller hindres;
(iii) ved enhver forespørsel om utlevering av Personopplysninger under Databehandleravtalen fra myndigheter, unntatt hvor det vil være i strid med obligatorisk lovgivning å varsle.
(iv) om enhver forespørsel fra Registrerte eller andre tredjeparter vedrørende innsyn eller utøvelse av andre rettigheter under Gjeldende Helse- og Personvernlovgivning.

Databehandleren skal uten ugrunnet opphold varsle Dataansvarlig dersom Databehandler er eller sannsynligvis vil bli ute av stand til å etterleve sine forpliktelser under Databehandleravtalen.

Denne bestemmelsen avskjærer eller erstatter ikke andre varslingsforpliktelser i Databehandleravtalen.

5. VARIGHET OG OPPHØR AV DATABEHANDLERAVTALEN

Denne Databehandleravtalen gjelder så lenge Databehandler behandler Personopplysninger på vegne av Dataansvarlig. Dersom det fremkommer eksplisitt, vil enkelte bestemmelser gjelde også etter at Databehandleravtalen opphører.

Ved opphør av Databehandleravtalen skal Databehandler (og godkjente underleverandører, jf. pkt. 44.7) returnere samtlige dokumenter og elektroniske data som Databehandler måtte ha i sin besittelse i egenskap av Databehandler. Dataansvarlig skal dekke kostnadene forbundet med dette.

Personopplysninger skal bli tilbakelevert innen en rimelig tidsfrist satt av Dataansvarlig og i et standardisert format og medium sammen med nødvendige instruksjoner som sikrer Databehandlers videre bruk av Personopplysningene. Om gjennomførbart, kan Dataansvarlig bestemme at Personopplysninger i stedet skal overføres til en annen leverandør. Dataansvarlig skal dekke dokumenterte kostnader forbundet med slik overføring.

Som et alternativ til tilbakelevering kan Dataansvarlig bestemme at alle eller deler av opplysningene som omfattes av Databehandleravtalen skal ugjenkallelig slettes av Databehandleren etter mottak av skriftlig instruks fra Dataansvarlig. Databehandler har ingen rett til å beholde kopier av opplysninger i noe som helst format, med unntak av opplysninger som Databehandleren i henhold til obligatorisk lovgivning er forpliktet til å ta vare på.

Databehandler må fremlegge skriftlig dokumentasjon på at sletting og/eller destruksjon har funnet sted i henhold til Databehandleravtalen innen rimelig tid etter opphør av denne, og må bekrefte at Databehandler ikke har beholdt noen kopi, utskrift eller annen gjengivelse av noen som helst del av materialet, uansett bruk av medium.

Databehandler plikter å sjekke og dokumentere at ovennevnte krav også er overholdt av eventuelle godkjente underleverandører.

6. LOVVALG

Databehandleravtalen er underlagt norsk rett. Verneting er Trondheim tingrett.

7. SIGNATUR

Databehandleravtalen er undertegnet i to eksemplarer, ett til hver Part.

Os i Østerdalen, 21.12.2021	Sted/dato_____
Signatur Dataansvarlig	Signatur Databehandler
Jukka M. Peramaa	Torbjørg Vanvik
Leder, IKT og sikkerhet	Administrerende direktør Helseplattformen
Jukka M. Peramaa Leder - IKT og sikkerhet	
---	---

Vedlegg 1

Dette vedlegget representerer Dataansvarliges ytterligere instruksjoner til Databehandler i tilknytning til Databehandlers behandling av Personopplysninger på vegne av Dataansvarlig, og er en integrert del av Databehandleravtalen.

A) BEHANDLINGENS FORMÅL OG KARAKTER

Det overordnede formålet med behandlingen er å forberede datagrunnlaget i eksisterende journalløsninger for migrering til ny journalløsning ("Helseplattformen"). Man må sikre at informasjonen og alle nødvendige egenskaper ved opplysningene overføres og presenteres riktig i ny løsning.

Behandlingen innebærer at helse- og personopplysninger i eksisterende journalløsninger kopieres inn i et sikkert migreringsmiljø (kalt Staging) for analyse og bearbeidelse. Målet med behandlingen er å strukturere dataene på en måte som gjør det mulig å velge ut hvilke data som skal inngå, og plasseres på riktig sted, i ny løsning.

Når opplysningene er tilstrekkelig analysert, eksporteres de til en testversjon av Epic (kalt PJX), der de valideres av fageksperter, oppnevnt av helseforetakene, for å sikre at flyttingen har blitt gjennomført i henhold til spesifikasjonene. PJX-miljøet har etablert tilgangskontroll slik at kun navngitte personer med tjenstlig behov, har tilgang. Som ledd i testingen vil PJX-miljøet kunne slettes og bygges opp på nytt mens testingen pågår, og opplysninger fra flere kunder vil eksistere i samme miljø, for å sikre en sammenhengende journal for alle kunder som ønsker å inngå et journalsamarbeid etter go-live. PJX-miljøet vil alltid kun være et testmiljø, og skal aldri brukes i produksjon. Når tidspunktet for GO-Live inntreffer, vil den utviklede uttrekksløsningen kopiere data fra eksisterende systemer og inn i det etablerte produksjonsmiljøet kalt PRD. På det tidspunktet vil nødvendige avtaler, f.eks etter pasientjournalloven § 9, måtte være på plass.

B) KATEGORIER AV REGISTRERTE

Registrerte kan deles inn i to hovedgrupper:

- Pasienter
- Ansatte
- Pårørende

C) KATEGORIER AV PERSONOPPLYSNINGER

Opplysningskategoriene er mange og omfatter i hovedsak:

- Pasienter:
    - *Administrative opplysninger*: Kontaktinformasjon som navn, adresse, telefonnummer og personnummer.

- *Journaldata*: Helseopplysninger som medikamentbruk, behandling og resultat av behandling, resultat fra undersøkelser, vurderinger fra helsepersonell om pasientens helse mv.

- Ansatte: Forfatter av opplysninger i pasientjournalen.
- Pårørende: Administrative opplysninger (Kontaktinformasjon som navn, adresse og telefonnummer.)

D) UNDERLEVERANDØRER

Databehandler vedlikeholder en oversikt over underleverandører som til enhver tid benyttes. På tidspunktet for signering av denne Databehandleravtalen benyttes følgende underleverandører:

Ernst & Young AS, org.nr: 976 389 387, Dronning Eufemias gt. 6, 0191 Oslo

Helse Midt-Norge RHF, v/ Hemit, org.nr: 983 658 776, Abels gt. 9, 7030 Trondheim

Epic Systems Corporation, 1979 Milky Way, Verona, Wisconsin, USA 53593

IBM, org.nr: 931 482 580, Lakkegata 53, 0187 Oslo

E) SIKKERHETSTILTAK

Databehandler forplikter seg til å følge opp risiko og implementere de tiltak som er identifisert i den risikovurderingen som er gjort forut for migreringen. Risikovurderingen er inntatt som vedlegg 2 til denne Databehandleravtalen.

Databehandleren skal uavhengig av risikovurderingen oppfylle følgende grunnleggende krav:

(i) Etablere tilgangskontroll til systemer og data. Både autorisert bruk og forsøk på ikke-autorisert bruk av systemer skal registreres. Dokumentasjon skal oppbevares i minst tre måneder;

(ii) Etablere tilgangskontroll til bygninger og utstyr som benyttes ved behandling av Personopplysninger;

(iii) Benytte verktøy for virusbeskyttelse, spam-filtre og brannmurer når dette er nødvendig eller påkrevet;

(iv) Logge alle kritiske systemoperasjoner;

(v) Ha systemer for back-up/gjenopprettingsprosess for alle kritiske systemer og gjenopprettingstester;

(vi) Kryptere kommunikasjon dersom det er nødvendig eller påkrevet;

(vii) Forsvarlig oppfølging av underleverandører når det kommer til informasjonssikkerhetskrav.

Databehandler skal kunne dokumentere tiltakene som er opplistet ovenfor så langt Gjeldende Helse- og Personvernlovgivning krever dette. Dokumentasjonen skal være tilgjengelig for Dataansvarlig på forespørsel.

Følgende tiltak er besluttet gjennomført etter risikovurderingen og skal være effektuert før behandlingen av personopplysninger starter. Disse tiltakene er nedfelt i prosedyre i Helseplattformen og ansvaret er tillagt riktige roller.

Taushetserklæringer

Alle som er involvert i migreringsaktiviteten skal signere på en egen taushetserklæring på denne aktiviteten som pålegger taushet om opplysninger man får kjennskap til, og som også gjelder etter at oppdraget er utført.

Fysisk skjerming

Samtlige som er involvert i migreringsaktiviteten skal kun utføre arbeid i migreringsmiljøet fra forhåndsdefinerte lokaler og arealer. Egne arealer er laget for denne aktiviteten. Det er fysisk adgangskontroll til disse arealene.

Tilgangsstyring til, og innad i migreringsmiljøet

All tilgang til migreringsmiljøet gis ved autentisering og autorisering med personlige brukere. Miljøet består av flere datakilder og der det er mulig å avgrense tilgangen innad i miljøet, skal dette gjøres. Alle bestillinger om tilgang skal gå via prosjektleder for migreringen.

Opplæring

Alle som skal ha tilgang til data i migreringsmiljøet skal ha gjennomført e-læringskurs i informasjonssikkerhet som er laget i HMN.

Logging av oppslag

Alle oppslag som gjøres via applikasjoners brukergrensesnitt skal logges på samme måte som i produksjonsmiljøene.

Iverksette sletting av data

Dataansvarlig virksomhet kan pålegge Databehandler sletting av Personopplysninger fra migreringsmiljøet i tilfeller der Dataansvarlig selv har fått pålegg om slik sletting.