melin medical
time to treat

Databehandleravtale

mellom

Den dataansvarlige:

ALMINNELEG HELSEVERN I KVINNHERAD

CVR 974614669

Rosendalsvegen 10

5470 ROSENDAL

Norway

og

Melin Medical AS (org. 995 250 640)

databehandler

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Personopplysningsloven av 15.06.2018 nr. 38, Personvernforordningen og Pasientjournalloven av 20. juni 2014 nr. 42. Avtalen skal bl.a. sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers behandling av personopplysninger på vegne av den databehandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse som beskrevet nedenfor.

2. Aktører

Melin Medical AS er leverandør av betaling og administrasjonsløsninger til databehandleransvarlig. Melin Medical AS er ansvarlig for innfordring av faktura, og forfalte fordringer (fakturainformasjon) på oppdrag for den enkelte klinikk.
Det er dermed klinikken som er databehandlingsansvarlig og Melin Medical AS er databehandler overfor klinikken.

3. Formål og behandling av opplysninger

Databehandler leverer en portalløsning som tilgjengeliggjør informasjon om betaling til klinikken, som omfatter funksjonalitet for:

- innsyn i fakturaer
- fakturahistorikk
- utestående fakturaer
- betalingsavtaler
- evt. annen funksjonalitet som kan knyttes til betaling og administrasjon.

De opplysninger som databehandler behandler vil omfatte personopplysninger som er nødvendig for å kunne utføre funksjonalitetene beskrevet over. Dette vil omfatte personopplysninger som fødselsnummer, navn, adresse, telefonnummer og epostadresse til de personer som databehandleransvarlig ønsker å drive innfordring mot.

Avtalen omfatter også behandling av personinformasjon i tilknytning til databehandlers løsning for pasientbetaling gjennom betalingsautomat.

4. Databehandlers plikter

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også

etter avtalens opphør. Databehandler plikter å behandle personopplysninger på en slik måte at krav til konfidensialitet, integritet, tilgjengelighet og kvalitet som følger av det til enhver tid gjeldende lovverk er ivaretatt.

Databehandler kan ikke benytte personinformasjon som behandles på vegne av klinikken til egne formål, og informasjon som behandles for én databehandlingsansvarlig skal holdes adskilt fra både egne og andre virksomheters informasjon og tjenester.

Alle oppslag og endringer i adresseinformasjon logges, og vil vise hvem som har gjort oppslaget og når dette ble gjort.

Databehandler skal sikre god og forutsigbar informasjon til pasientene om hvilke tjenester som er tilgjengelig, at det er frivillig å benytte seg av disse tjenestene, at avgitt samtykke kan trekkes tilbake på et senere tidspunkt og annet som er viktig for den enkelte slik at denne kan ivareta sine rettigheter.

5. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal databehandlingsansvarlig underrettes om dette i eget skriv før behandlingen av personopplysninger starter.

Ved bruk av underleverandør(er) er databehandler ansvarlig for at de etterlever de plikter og rettigheter som følger av denne avtalen.
Databehandler er ansvarlig for sine underleverandører som utfører oppgaver knyttet til tjenestene på samme måte som om databehandler selv sto for utførelsen.

6. Sikkerhet

Pasientenes personvern skal tas på alvor og det er viktig for den databehandlingsansvarlige at aktuelle person- og helseopplysninger sikres på forsvarlig vis. Løsningen skal være i tråd med:

- kravene til Norsk Helsenett
- kravene i norm for informasjonssikkerhet i helsesektoren
- krav som følger av Pasientjournalloven § 22
- krav som følger av Personopplysningsloven

Følgende tiltak er gjeldende for å gi tilfredsstillende sikkerhet mht. konfidensialitet, integritet og tilgjengelighet for personopplysninger:

- Digital signering og kryptering av kommunikasjon med helsevirksomheter slik at uvedkommende ikke vil få tilgang til informasjonen.

- Automatisk overvåking av tjenestene for å avdekke feilsituasjoner, misbruk og innbruddsforsøk m.m.
- Tilfredsstillende fysisk sikring av drifting av tjenestene i form av adgangskontroll, lokasjonsovervåkning og låste serverrom.
- Daglig sikker og ekstern backup av pasientenes opplysninger.
- Logging av dataflyt og oppfølging av disse.
- Implementerte ledelsessystem for informasjonssikkerhet, herunder:
    - Dokumenterte rutiner og oppfølging av bruk av systemadministratortilganger.
    - Prosedyrer for hendelseshåndtering inkludert kommunikasjon til eksterne parter (Business continuity plan).
    - Veldefinerte SLA-kontrakter med eksterne leverandører.

Databehandleren har uavhengig av opplistingen over en selvstendig plikt til å etterleve det til enhver tid gjeldende regelverk på området, og må påse at det samlede valg av tiltak er fastsatt på bakgrunn av konkrete risikovurderinger som sikrer en akseptabel risiko. Slik risikovurdering skal være dokumentert og sikkerhetstiltakene skal jevnlig evalueres og ved behov tilpasses endret risikobilde.

Personopplysningene skal ikke overføres til land utenom EU/EØS området.

Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle kravene i avtalen. Dokumentasjonen skal være tilgjengelig på databehandlingsansvarliges forespørsel. Databehandler plikter for øvrig å bistå etter anmodning, slik at databehandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Eventuelle avvik skal meldes til databehandlingsansvarlig. Databehandlingsansvarlig har selv ansvaret for at avviksmeldinger og oppfølging av avvik.

7. Sikkerhetsrevisjoner

Sikkerhetsrevisjoner for systemene som inngår i denne avtalen skal gjennomføres minimum årlig. Revisjonene vil bli gjennomført i samsvar med krav til slike som finnes i Norm for informasjonssikkerhet for helse- og omsorgstjenesten, og gjennomføres i tråd med det omfang som er anbefalt der.

Databehandler vil oppsummere resultatene og iverksette nødvendige utbedringstiltak minimum årlig. Om behandlingsansvarlig ønsker innsyn i slik oppsummering, må det fremsettes skriftlig krav om dette.

Om databehandleransvarlig ønsker en revisjon utført i en hyppigere frekvens, eller gjennomført av en tredjepart, er det for databehandlersansvarlig egen kostnad.

8. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av databehandlingsansvarlig.

Detaljer om varighet og oppsigelse av kundeforhold er avtalt i egen merkantil avtale.

Ved brudd på denne avtale eller personopplysningsloven kan databehandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

9. Ved opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den databehandlingsansvarlige og som omfattes av denne databehandleravtalen og som behandler ikke selv har tilgjengelig.

Videre skal databehandlingsansvarlig ved avtalens opphør for øvrig slette eller forsvarlig destruere alle andre gjenværende personopplysninger som omfattes av avtalen som eventuelt finnes hos databehandler. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandler plikter å ivareta regnskapsopplysninger i minimum 5 år, eller til Databehandlingsansvarlig gir skriftlig beskjed om å slette materialet.

Databehandler skal som ledd i avslutning av avtaleforholdet skriftlig bekrefte at sletting og eller destruksjon er foretatt i henhold til avtalen etter avtalens opphør. Slik bekreftelse skal senest skje etter 3 måneder etter avtalens opphør.

10. Meddelelser

Meddelelser etter denne avtalen til databehandler skal sendes skriftlig til: privacy@melinmedical.com.

11. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

***

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Sted og dato

Databehandlingsansvarlig	Databehandler
(underskrift)	(underskrift)