Personvernerklæring for CGM Journal

CompuGroup Medical Norway AS

1. Organisering av datasikkerhet og tildeling av ansvar for datasikkerhet

CompuGroup Medical Norway AS anser beskyttelse av personlig data og behandling av disse som et hovedprinsipp. CompuGroup Medical Norway AS forholder seg til en streng etterlevelse av alle relevante lover og reguleringer vedrørende lagring og behandling av personlig data.

CompuGroup Medical Norway AS forplikter seg gjennom tilknytning til Norsk Helsenett å følge Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen).

Andre relevante lovverk inkluderer lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven), forskrift av 15. juni 2018 nr. 876(personopplysningsforskriften), 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) og EUs personvernforordning (forordning 2016/679).

CGM SE har etablert et sentralt system for databeskyttelse som sikrer et høyt beskyttelsesnivå for personopplysninger og overholdelse av databeskyttelseslover i alle CGM-selskapene.

Denne personvernerklæringen tjener til å oppfylle lovforpliktelsene ved å gi opplysninger om håndtering av data innenfor CGM. Denne personvernerklæringen refererer spesielt til EPJ-systemet CGM Journal. Siste versjon av denne personvernerklæringen finnes til enhver tid på våre nettsider.

2. CGM Journal

CGM Journal er et elektronisk journalsystem til bruk i primærhelsetjenesten. CGM Journal støtter medisinsk kontor / praksis i samsvar med juridiske krav, strukturert dokumentasjon, kontorstyring, fakturering, resept og ytterligere krav som kan oppfylles av valgfrie programtillegg.

CGM Journal tilbyr dedikert brukerrettighetsadministrasjon som begrenser tilgangen til programvaren og eventuelle programtillegg til autoriserte personer. Utover tilgangskontroll til programvaren og programtillegg styrer brukerrettighetsadministrasjonen også styring av lese- og skriveadgang til data lagret og behandlet i systemet.

CGM Journal er utviklet basert på EPJ-standarden til Direktoratet for E-helse, og oppdateres i henhold til krav i Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen).

3. CGMs behandling av personopplysninger ifbm kundeforhold

Personlige data betyr all informasjon knyttet til en identifisert eller identifiserbar fysisk person. Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson. Typiske personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer.

I samsvar med gjeldende lovverk forplikter vi oss til å slette alle kontraktdata, loggdata og data fra teknisk drift etter at kontrakten er avsluttet.

Vi er imidlertid også forpliktet til av nasjonalt lovverk om kommersiell drift og finanslovgivning til å vurdere rettslige arkiveringsperioder som kan strekke seg utover terminering av kontrakten.

3.1 Kontrakt og registreringsdata

Kontrakts- og registreringsdata identifiserer og styrer kontraktsforholdet mellom behandlingsstedet/organisasjonen og CompuGroup Medical Norway AS. Disse dataene inkluderer:

- Data relatert til behandlingsstedet/organisasjonen
  - Navn
  - Type praksis
  - Adresse
  - Telefonnummer
  - Epostadresse
  - Identifikatorer / identifikasjonsnummer til praksisen

- Data relatert til kontaktpersoner
  - Tittel
  - Fornavn / etternavn
  - Navn suffiks
  - Identifikator / identifikasjonsnummer til helsepersonell
  - Epostadresse
  - Telefonnummer

- Ikke-obligatorisk informasjon som kan legges til
  - Kjønn
  - Fødselsdato
  - Land
  - Språk
  - Privat telefonnummer
  - Mobiltelefonnummer

Lagring og behandling av personopplysninger som utleveres til CompuGroup Medical Norway AS under forretningsforholdet og kontraktforholdet, tjener og er begrenset til formålet med å oppfylle kontrakten, særlig ordrebehandling og kundestøtte.

Disse dataene kan kun brukes til produktrelaterte kundeundersøkelser og markedsføringsformål dersom det er gitt tillatelse via en samtykkeerklæring.

Data vil ikke bli overført eller solgt til noen tredjepart, med mindre det er nødvendig for å oppfylle kontraktsforpliktelsene eller hvis det er uttrykkelig tillatt med en samtykkeerklæring.

Som et eksempel kan det være nødvendig for CompuGroup Medical Norway AS å overføre adresse- og bestillingsdata til en salgs- og servicepartner når en bestilling er plassert. Det kan også være nødvendig å overføre adressen til et eksternt produksjonsfirma med det formål å produsere og sende oppdateringsdata.

Den registrerte har rett til å se og hente ut sine data, til å ha feilaktig data rettet, til å legge restriksjoner på og ha innvendinger mot behandlingen av sine data, samt rett til å få sine data slettet.

3.2 Data fra teknisk drift

Data fra teknisk drift er nødvendig for levering av tjenester beskrevet i kontrakten som f.eks. kundestøtte og programoppdateringer. CGM samler kun data fra teknisk drift for dette formålet. CGM undersøker regelmessig at kun data som er nødvendige for å gi og forbedre de tekniske operasjonene til produktet / tjenestene dine, vil bli samlet inn, lagret og behandlet.

Data fra journalsystemet samles kun etter at det er mottatt samtykke.

Når du bruker våre onlinetjenester, lagres følgende data for å opprettholde systemintegritet og sikkerhet midlertidig:

- Domenenavn
- IP-adressen til klientdatamaskinen
- Dato og klokkeslett for tilgangen
- Filforespørsel fra klientdatamaskinen (filnavn og URL)
- Antall byte overført under tilkoblingen.

Data fra teknisk virksomhet lagres i CGM konsernets felles CRM system på servere innenfor EU.

4. Behandling av personopplysninger i CGM Journal

- Opplysninger om praksisen og ansatte
- Pasientdata
    - Personopplysninger
    - Sensitive data

Data i CGM Journal lagres og behandles i databasen på praksisens server eller i CGM sin hostingtjeneste.

4.1 Grunnleggende data om praksisen og ansatte

Grunnleggende data om praksisen er lagret for å overholde lovkravene og for riktig bruk av visse moduler / avtaler.

Obligatoriske opplysninger for bruk av CGM Journal er merket tilsvarende i programmets administrasjonsmodul.
Grunnleggende data om praksisen og dets ansatte inkluderer:

- Praksisens navn
- Praksistype
- Praksisens adresse
- Praksisens telefonnummer, fax, e-postadresse
- Identifikatorer / ID-numre
- Medisinsk spesialitet
- Informasjon om legen / helsepersonell
    - Tittel
    - Fornavn / etternavn
    - Legenes / helsepersonellets identifikatorer / identifikasjonsnumre
    - Brukernavn / passord
- Ytterligere ansatte i praksisen
    - Tittel

- Fornavn / etternavn
- Brukernavn / passord

Grunnleggende data er nødvendig når ulike programmoduler automatisk utfører handlinger. Overføringen til tredjepart utføres etter forhåndsgodkjenning eller brukerinteraksjon. Endring, begrenset behandling eller sletting av disse dataene er mulig, men kan begrenses av lovkrav. Hvordan man endrer data, begrenser behandling eller sletter data er beskrevet i brukerhåndboken.

4.2 Pasientdata

Lagring, bruk og behandling av pasientdata er bare tillatt med pasientens samtykke eller basert på en lovlig forpliktelse. Pasientdata genereres ikke automatisk i CGM Journal. Pasientdata samles inn lagres i CGM Journal av legen / personalet som arbeider ved praksisen.

Personlige data: Pasientens grunnleggende informasjon er registrert ved hjelp av elektronisk datamedia (for eksempel folkeregisteret) og / eller inntastet eller fullført ved manuell dataregistrering.

Det skilles mellom nødvendige (obligatoriske) data for å overholde kontraktlige eller juridiske forpliktelser på den ene side og ytterligere ikke-obligatoriske data gitt av pasienten.

Obligatoriske opplysninger inkluderer:

- Personlig informasjon (fornavn, etternavn, fødselsdato, kjønn)

Ikke-obligatorisk tilleggsinformasjon inkluderer:

- Personlig informasjon (personnummer/id-nummer, sivil status)
- Adressedetaljer (gate, husnummer, postnummer, poststed, kommune/bydel, land)
- Informasjon om forsikring og refusjon
- Privat telefonnummer
- Mobilnummer
- E-post adresse
- Arbeidsgiver
- Yrke og utdanning
- Slektninger eller andre kontaktpersoner
- Helseforsikring for utlendinger

Sensitive data: Helseopplysninger er en særlig kategori av personopplysninger.

Å skrive inn data i pasientens journal er avledet av den juridiske forpliktelsen helsepersonell har til å dokumentere alle handlinger i henhold til helsepersonelloven og resultater som er relevante for pasientens nåværende og fremtidige behandling.

Disse dataene inkluderer:

- Anamnese
- Diagnose
- Undersøkelse
- Undersøkelseresultater
- Funn, vurdering og tiltak

- Behandlinger og resultater
- Samtykke-dokumentasjon
- Korrespondanse til eller fra legen
- Konto / faktureringsdata som
    - Faktureringsinformasjon
    - Fakturaer
    - Påminnelser og dunning nivåer

4.3 Behandling av praksisens data og sensitive personopplysninger | pasientdata i programvaremoduler

Oversikt over de mest brukte moduler som enten er integrert i CGM Journal eller kan legges til, og som behandler personlige data.

Integrerte moduler inkluderer:

- Korrespondansemodul: overføring av strukturert helsedata som inneholder person- og helseopplysninger mellom behandlingssteder.
- Legemiddelmodul: modul for forskrivning med overføring av person- og helseopplysninger til/fra sentral forskrivningsmodul (eresept).
- Laboratoriemodul: rekvirering og prøveresultater med overføring av person- og helseopplysninger mellom behandlingssteder.
- Regnskapsmodul: refusjonskrav fra behandler inkludert person- og helseopplysninger til Helfo.
- Sykemeldingsmodul: kommunikasjon av sykemelding/legeerklæring inkludert person- og helseopplysninger til NAV/Helfo.
- Database: informasjon som mates inn i grensesnittet, inkludert person- og helseopplysninger, håndteres på en server og lagres i en database.
- Utskrift: overføring av person- og helseopplysninger til utskriftstjeneste.

Valgfrie moduler inkluderer:

- Buypass ID: identifikasjon av behandlere i sanntid mot sentrale nasjonale tjenester som for eksempel sentral forskrivningsmodul (eresept). Sertifikater med personopplysninger hentes fra Windows sertifikatregister.
- Besøklegen.no: pasientkommunikasjon og avtalebooking med overføring av person- og helseopplysninger i sanntid direkte fra behandlers database.
- Helsenorge.no: pasientkommunikasjon og avtalebooking med overføring av person- og helseopplysninger til sentral tjeneste drevet av Direktoratet for ehelse.
- Adresseregister: overføring av personopplysninger fra helsespersonell til/fra NHN adresseregister
- Fastlege: import av personopplysninger fra NHN Fastlegeregister og fastlegelister.
- Personregister: import av personopplysninger fra folkeregisteret.
- Fakturaeksport: eksport av fakturainformasjon inkludert personopplysninger.
- Pasientreiser: eksport av personopplysninger i forbindelse med bestilling av pasienttransport .
- Labrekvisisjonsmoduler: rekvirering og mottak av prøveresultater inkludert person- og helseopplysninger.
- Kjernejournal: overføring av person- og helseopplysninger til/fra sentralt nasjonalt register.
- Betalingsterminal: overføring av fakturainformasjon inkludert personopplysninger til/fra tilknyttede terminaler.
- Noklus: overføring av person- og helseopplysninger.
- Sysvak: overføring av vaksinedata til/fra nasjonalt register inkludert person- og helseopplysninger.
- Frikort: overføring av personopplysninger til/fra Helfo for å sjekke pasienters frikortstatus.
- NPR: overføring av person- og helseopplysninger til Norsk PasientRegister.
- SMS og Epostvarsling: avtalevarsling via tjenesten eportal med overføring av personopplysninger til mottakers mobiltelefon eller epostkonto, opplysninger kan havne i tredjeland dersom mottaker befinner seg tilsvarende plass ved mottak.

- Produktråd: produktønsker fra brukere, overføring av brukeres personopplysninger til tredjeland (USA). Sertifisert med EU-US Privacy Shield.

For mer informasjon om modulene henvises det til CGM Journal brukermanual. Sletting av data som ikke omfattes av systemfunksjonalitet gjøres normalt via bestilling fra kunden basert på spesifikk instruks og i henhold til gjeldende lov- og regelverk. For sletting fra nasjonale registre henvises pasienten til aktuelle registre.

5. Dataoverføring

Elektronisk dataoverføring basert på juridisk, kontraktsmessig eller forhåndsgodkjenning utføres av CGM Journal bare etter brukerinteraksjon eller automatisk - hvis tillatelse er gitt.

Dataoverføring basert på lovbestemmelser

Persondata som inngår i helsedataregistre eller nasjonale løsninger overføres til ansvarlig myndighet i henhold til gjeldende krav.

Dataoverføring basert på kontraktsforpliktelser

CGM er pliktig til å inngå kontrakter som sikrer at personvern er ivaretatt. Dersom CGM skal inngå en kontrakt som inkluderer dataoverføring mellom CGM Journal og annet system, vil CGM kreve at både løsning og kontrakt er i henhold til gjeldende regelverk og ivaretar personvernet.

Elektronisk dataoverføring basert på samtykke

CGM legger inn systemstøtte i CGM Journal på områder der behandler er pliktig til å innhente samtykke, og der det er hensiktsmessig å ha systemstøtte - for eksempel ved innhenting av reseptinformasjon fra reseptformidler. Dette gjøres i henhold til gjeldende regelverk, hvilket som hovedregel tilsier at overføringen er kryptert.

6. Fortrolighet og databeskyttelsetrening

Ansatte i CompuGroup Medical Norway AS signerer en fortrolighetsavtale som blant annet regulerer behandling av pasientdata.

Utgangspunktet for CompuGroup Medical Norway AS i denne forbindelse er at vi ikke deler, modifiserer, sletter eller på annen måte behandler informasjonen våre kunder legger inn i våre systemer, med mindre det er spesifikt forespurt av kunden eller nødvendig for at vi skal kunne oppfylle våre forpliktelser til kunden (f.eks. kundestøtte, konsulentoppdrag, systemoppdateringer eller lignende). Ansatte ved CompuGroup Medical Norway AS forplikter seg til å sørge for at alt materiale og data av konfidensiell karakter behandles korrekt i henhold til internt regelverk, de ansatte har også signert en avtale om taushetsplikt. Ansatte ved CompuGroup Medical Norway AS gjennomgår trening i databeskyttelse i henhold til stillingens behov.

7. Sikkerhetstiltak / unngå risiko

CGM bruker nødvendige tekniske og organisatoriske sikkehetstiltak for å beskytte dine personlige data og personlige data fra pasientene mot uautorisert tilgang, endring, avsløring, tap, ødeleggelse og andre former for misbruk. Disse tiltakene inkluderer interne kontroller i henhold til Normen og kontroller av våre prosesser for datainnsamling, lagring og

prosessering samt sikkerhetstiltak for å beskytte IT-systemer der vi lagrer kontraktsdata og data fra tekniske operasjoner fra uautorisert tilgang.

8. Tekniske og organisatoriske tiltak

CGM er avhengig av tillit hos sine kunder og erkjenner den kritiske rollen informasjonssystemer spiller i CGM sine forretningsaktiviteter. Dette gjør det nødvendig for oss å sikre en konsistent og høy standard for beskyttelse av av personlig data og forsikre oss om at vi overholder gjeldende databeskyttelseslover.

CGM forplikter seg i denne forbindelse til å benytte nødvendige organisatoriske og tekniske tiltak for å beskytte personopplysninger vi behandler, avhengig av hvilken informasjon som behandles og den risikoen behandlingen utgjør for våre kunder.

CGM gruppen sentralt (hovedkontoret i Tyskland) utarbeider felles policyer og retningslinjer for alle forretningsenheter innenfor EU/EØS. Spesielt viktig er disse tiltakene:

Organisatoriske tiltak:

- CGM gruppen har en egen komite for informasjonssikkerhet som produserer, fornyer og opprettholder firmaets strategier og policyer for informasjonssikkerhet.
- Personvernombud for rådgivning innenfor personvern og håndtering av avvik.
- Obligatorisk opplæring i datasikkerhet og personvern for alle ansatte.
- Føring av protokoller over behandlingsaktiviteter.
- Risikovurdering ved tilgang til eller behandling av personopplysninger.
- Databehandleravtaler med brukersteder og underleverandører.

.

Tekniske tiltak:

- Prosedyrer og verktøy for overvåkning som sørger for datasikkerhet.
- Kontrollere medarbeideres tilgang til data; det vil si at den rette informasjonen er tilgjengelig på rett sted og tidspunkt til en autorisert bruker.
- Behandle datatilgjengelighet i samsvar med gjeldende lovgivning, policyer og retningslinjer og kundens instruksjoner.
- Avvikshåndtering: rutiner og verktøy for styring av brudd på personvernet.
- Jevnlige sikkerhetsrevisjoner som vurderer om tekniske og organisatoriske tiltak er tilstrekkelige for å oppfylle kravene til gjeldende lovgivning.

For å sørge for god datasikkerhet overvåker CGM kontinuerlig utvikling i sikkerhetsteknologien. Dette inkluderer konsekvens-, risiko- og sårbarhetsvurderinger.

I tillegg utføres tester som regelmessig tilpasses for å vurdere og evaluere effektiviteten av de tekniske og organisatoriske tiltakene som sørger for at sikkerheten til de ulike kategoriene av personlig databehandling vi utfører eller som våre kunder utfører i våre produkter.

Følgende retningslinjer skal regulere gjennomføringen av passende tekniske og organisatoriske tiltak:

- **Data backup**

  For å forhindre tap, sikkerhetskopieres data jevnlig.

- **Personvern ved design**

  CGM tar hensyn til databeskyttelse og datasikkerhetsprinsipper gjennom design og utviklingsprosesser i våre IT-systemer. Tiltak for å oppnå innebygd databeskyttelse, for eksempel sikker godkjenning eller kryptering, vurderes ved begynnelsen av utviklingsprosessen.

- **Personvern som standard**

  CGM-produkter leveres med fabrikkinnstillinger som er optimalisert for personvern, slik at bare de personopplysninger som er nødvendige for den aktuelle hensikten, behandles.

- **Kommunikasjon via e-post (praksis / CGM)**

  Hvis du vil kontakte CGM via e-post, vær oppmerksom på at personvernet til den overførte informasjonen ikke kan garanteres fordi innholdet av e-postmeldinger kan ses av tredjeparter. Vi anbefaler at du bruker telefon, post eller video når du ønsker å overføre konfidensiell informasjon.

- **Fjernaksess**

  Ansatte eller underleverandører av CGM må av og til ha tilgang til pasient- eller kundedata. Denne tilgangen er underlagt generelle CGM regler.

  - Fjernaksesspunkter er stengt som standard og krever godkjenning av kunde.
  - Passord for å få tilgang til kunders IT-systemer utstedes kun for fjernaksess.
  - Vi bruker fjernaksessverktøy som spør kunden om aktivt å gi tilgang, og sporer sesjoner.
  - Fjernaksess logges i CRM-systemet. Følgende data logges: ansvarlig person, dato og klokkeslett, varighet, målsystem, fjernstyringsverktøy og en kort beskrivelse av oppgavene som er utført.
  - Opptak av fjernstyring er forbudt.

9. Den registrertes rettigheter

Personlige data fra praksisen og dets ansatte

- Du har rett til å bli informert om data lagret om deg, samt retten til å få tilgang til disse dataene, du har rett til rettelse, sletning, begrensning av behandling, dataportabilitet og rett til å motsette seg behandling av dine personlige data.
- Du har rett til å trekke samtykket til enhver tid. Tilbakekallingen vil ha en fremtidig effekt.
- Du har rett til å sende inn en klage til den ansvarlige overordnede myndigheten hvis du tror at vi behandler dataene dine feilaktig.
- Vi forplikter oss til å slette alle kontraktdata, loggdata og alle data fra teknisk drift etter at kontrakten er avsluttet uten at du henvender deg til oss.

Vi er likevel forpliktet av kommersiell og finanslov til å overholde rettslige oppbevaringsperioder, som kan strekke seg utover kontraktsfestet avtaletid. Data fra teknisk drift lagres kun så lenge det er teknisk nødvendig og slettes senest etter at kontrakten er avsluttet.

Personlige data til pasienten

Dine pasienter har rett til å bli informert om data lagret om dem, samt retten til å motta og overføre sine personopplysninger (dataportabilitet) og retten til rettelse, sletting, begrensning av behandling og rett til å motsette seg behandling av personopplysninger.

Når du mottar slettingsforespørsler fra pasienter, er du uansett forpliktet til å overholde gjeldende oppbevaringsperioder.

Dine pasienter har rett til å trekke tilbake sitt samtykke når som helst. Tilbakekallingen vil ha en fremtidig effekt.

Dine pasienter har rett til å sende inn en klage til den ansvarlige tilsynsmyndigheten hvis de mener at du behandler dataene deres feilaktig.

10. Håndhevelse

Overholdelse av de databeskyttelsesregler som er beskrevet her, blir regelmessig gjennomgått av CGM.

Dersom CompuGroup Medical Norway AS mottar en formell klage, kontakter selskapet klageren for å løse eventuelle problemer knyttet til behandling av personopplysninger.

CompuGroup Medical Norway AS forplikter seg til å samarbeide med berørte parter og tilsynsmyndighetene.

11. Endringer i denne personvernerklæringen

Vær oppmerksom på at denne personvernerklæringen kan bli gjenstand for endringer og tillegg. Ved betydelige endringer vil vi publisere en detaljert melding. Hver versjon av denne personvernerklæringen kan identifiseres med dato og versjonsnummer. I tillegg arkiveres alle tidligere versjoner av denne erklæringen og gjøres tilgjengelig ved forespørsel til personvernombud.

12. Ansvarlig for CompuGroup Medical Norway AS

CompuGroup Medical Norway AS
Lysaker Torg 15
1325 Lysaker
Norge

Personvernombud
Spørsmål vedrørende behandlingen av personopplysninger i CGM Journal skal rettes til systemadministrator for aktuell kunde siden kunden er behandlingsansvarlig for opplysninger som behandles i systemet. Dersom det er behov for det kan systemadminstrator videreformidle henvendelsen til personvernombud hos CompuGroup Medical Norway AS.

Spørsmål vedrørende det avtalemessige forholdet mellom CGM og kunde kan rettes til personvernombud hos CGM Norge via e-post: gdpr.norway.no@cgm.com

13. Tilsynsmyndighet

Datatilsynet
E-post: postkasse@datatilsynet.no
Telefon: 22 39 69 00