GDPR
Retningslinjer og Strategi

KBB Medic AS (org: 912 372 022 mva)

Opprettetdato:
28.04.2018

Endret dato:
20.10.2019

Thormøhllensgate 51
5006 Bergen

1. Bakgrunn

Norske leger må forholde seg til mer enn 5000 sider med retningslinjer, som oppdateres ved jevne mellomrom. Det blir følgelig veldig vanskelig, om enn ikke umulig å holde seg oppdatert. En av disse sykdommene er kols, der de norske retningslinjene for korrekt diagnose og behandling er på 173 sider.

KBB Medic AS har utviklet et online verktøy for diagnose, behandling og oppfølging av kols-pasienter. Verktøyet har blitt godt mottatt blant norske leger, da det sparer tid samtidig som det kvalitets-sikrer diagnosen, behandlingen og oppfølgingen. Behovet er det samme for flere sykdommer. KBB Medic planlegger å utvikle tilsvarende verktøy for: Astma, Blodtrykk, Hjertesvikt, Diabetes, Osteoporose og Smertebehandling i første omgang.

Verktøyet samler inn anonymiserte data som leger fyller ut for pasienten, som samles i en database på vår server. Verktøyene logger ikke hvilken lege som har plottet dataene og person informasjonen som kan identifisere pasienten er av typen, alder, kjønn, høyde, vekt og etnisitet. I tillegg lagres måle-verdier som spirometri (for kols) og symptomer som pasienten måtte oppleves. Det kan argumenteres for at denne type data er anonymiserte og at pasienten vanskelig/umulig kan identifiseres ut fra person data alene.

For å kunne følge opp en pasient gjennom verktøyet genereres det en kode som den behandlende legen kan ta vare på i sin journal. Denne koden danner en kobling mellom pasient og pasient-data, der legen sitter på koblingsnøkkelen. For å få tilgang til denne nøkkelen må man ha tilgang til legens journal. Vi mener derfor at pasientens data er godt beskyttet. Men siden det finnes en kobling, konkluderer vi med at dataene er pseudo-anonymiserte og at de må håndteres i henhold til GDPR regelverket.

I dag er verktøyene åpne og gratis, men KBB Medic AS planlegger å lage en løsning der legene registrerer seg for å kunne bruke verktøyene. Den registrerte informasjonen om hver lege faller også inn under GDPR regelverket og må håndteres etter gjeldende retningslinjer.

- Dette dokumentet følger Datatilsynets sjekkliste for behandling av personvernopplysninger.

2. Personvern prinsipper

Reglene for *behandling av person-opplysninger* bygger på noen grunnleggende prinsipper. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene som kan oppsummeres som: Lovlig, rettferdig og gjennomsiktig. Dette baserer seg på artikkel 6 og 9 i forordningen [1]

2.1 Lovlig

Det må finnes et rettslig grunnlag for den behandlingen en virksomhet ønsker å gjøre. Forordningens artikkel 6 regulerer i hvilke tilfeller det skal anses lovlig å behandle personopplysninger. Minst ett av vilkårene i denne bestemmelsen må være oppfylt for at behandlingen er tillatt. Dersom det behandles *sensitive personopplysninger* må i tillegg minst ett av vilkårene i artikkel 9 være oppfylt.

- **Vi vil basere vår behandling av data på samtykke fra pasient til å lagre pasient-informasjon for diagnoseverktøyene og person informasjon om de som registrerer seg i vår database for abonnement på bruk av verktøyene.**

- **Vi vil legge til rette for at pasienter kan få slettet den informasjon som er lagret om dem ved å kontakte legen. Vi vil legge til rette for at helsepersonell som er registrert i vår database over abonnenter kan få slettet informasjon som er lagret om dem.**

Vår intensjon er å skille mellom hvilke opplysninger som er nødvendig å behandle for å levere tjenesten, og hvilke andre opplysninger det kan være valgfritt å oppgi for å få tilgang til utvidede tjenester.

2.2 Rettferdig

Behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal dessuten være gjennomsiktig og forståelig for de registrerte, den skal ikke foregå på fordekte eller manipulerende måter.

- **Vi vil baserer vår behandling av pasientinformasjon etter internasjonale retningslinjer der hver pasient skal behandles likt.**

- **Inndeling av pasienter i ulike kategorier vil basere seg på gjeldende internasjonale retningslinjer.**

- **De som abonnerer på vår løsning kan inndeles i kategorier etter hvilket abonnement de registrerer seg på.**

2.3 Gjennomsiktig

Behandling av personopplysninger skal være oversiktlig og forutsigbar for *den registrerte*. Den det behandles opplysninger om skal være informert om dette.

Gjennomsiktighet bidrar til å skape tillit og det setter den registrerte i stand til å bruke sine rettigheter og ivareta sine interesser.

- **Vi vil ha interaksjon mellom *lege* og den registrerte, slik at det gjøres enkelt for den registrerte å tilegne seg informasjon om hvordan personopplysningene behandles.**

- **Vi vil ha funksjonalitet for å gi informasjon om hvilke opplysninger som behandles, hva de brukes til og mulighet for de registrerte til å gjøre seg kjent med sine rettigheter og hvordan de skal utøve disse.**

- **Vi vil ha en personvernerklæring på vår nettside med generell informasjon om vår personvernpolicy.**

3. Personvernopplysninger i KBB Medic

Vi definerer 3 kategorier av personvernopplysninger i KBB Medic:

1. Egne ansatte, partnere, styret og tilknyttet fageksperter.
2. Personer som har registrert seg i vårt medlemssystem og abonnerer på våre tjenester.
3. Pasienter som er pseudoanonymisert i våre diagnose-og-behandlingssystemer, og kan identifiseres med en kode lagret i legens journal.

3.1 Egne ansatte, partnere, styret og tilknyttet fageksperter.

Dette er personer som direkte jobber med å utvikle KBB Medic, organisasjon, løsninger og fagkompetanse. Den omfatter også fageksperter som vi tilknytter oss for å få utviklet løsninger for nye sykdommer. Disse har i utgangspunktet har en løs kobling til KBB Medic, men omfattes av våre personvern retningslinjer.

3.2 Personer som har registrert seg i vårt medlemssystem

Vi vil tilby våre løsninger gjennom et medlemssystem der de som ønsker å bruke tjenestene må registrere seg. Dette er opplysninger tilknyttet rettigheter og betaling for tjenestene.

3.3 Pasienter som er pseudoanonymisert

For å kunne følge opp pasienter gjennom løsningene våre lagrer vi nøkkeldata som kjønn, alder, høyde etc. og også diverse diagnostiske parametere som symptomer og ulike måle-verdier. Pasientene kan ikke identifiseres i vårt system, men vi genererer en kode som behandlende lege kan lagre i sin journal. På den måten kan legen hente ut informasjon fra tidligere konsultasjoner ved å bruke denne koden. Vi kobler ikke informasjon om hvilken lege som behandler hvilken kode.

4. Formålet med å lagre personopplysninger i KBB Medic

Formålet med å lagre personopplysninger deler vi inn i de samme kategoriene som ble definert i kapitel 3.

1. Egne ansatte, partnere, styret og tilknyttet fageksperter.
2. Personer som har registrert seg i vårt medlemssystem og abonnerer på våre tjenester.
3. Pasienter som er pseudoanonymisert i våre diagnose-og-behandlingssystemer, og kan identifiseres med en kode lagret i legens journal.

4.1 Egne ansatte, partnere, styret og tilknyttet fageksperter.

Formålet med å behandle informasjon for denne gruppen handler om å ha kontakt informasjon og opplysninger vedrørende oppgaver etc. Behandling skal følge normal behandling av ansattopplysninger i Norske bedrifter.

4.2 Personer som har registrert seg i vårt medlemssystem

Formålet med å behandle informasjon for denne gruppen handler om å ha oversikt over hvilke tjenester den enkelte abonnerer på, e-post addresse, faktura adresse og faktura status. Vi kan også be om tillatelse av den enkelte om de ønsker å motta informasjon om tilleggstjenester fra KBB Medic.

4.3 Pasienter som er pseudoanonymisert

Formålet med å lagre informasjon om denne gruppen handler om å kunne tilby best mulig behandling og oppfølging til legen som behandler pasienten. Endringer i innhentet informasjon fra gang til gang kan gi et bilde av hvordan sykdommen utvikler seg og om dette skal få følger for behandlingen.

5. Sensitive personopplysninger lagret av KBB Medic

I utgangspunktet er det forbudt å behandle visse kategorier av personopplysninger. Mange omtaler disse opplysningstypene som *sensitive personopplysninger*.

5.1 Sensitive opplysninger for de pseudoanonymiserte pasientene

For de pseudoanonymiserte pasientene lagrer vi:

1. Opplysninger om etnisk opprinnelse. (I noen tilfeller der dette er relevant)
2. Helseopplysninger

5.2 Håndtering av sensitive opplysninger

Det finnes mange unntak fra forbudet. Lovens system er at det må foreligge et særskilt grunnlag i tillegg til *behandlingsgrunnlag* for å behandle denne typen opplysninger. I forordningen (artikkel 9 nr. 2 og 3) er det en oversikt over når opplysningene i punkt 1 til 10 likevel vil kunne behandles.

KBB Medic vil med bakgrunn i forordningens artikkel 9 nr 2 og 3 behandle sensitive opplysninger ved at:

- *Den registrerte* gir uttrykkelig samtykke.
- *Informasjonen er anonymisert og **kun** kan hentes frem og kobles til pasienten ved hjelp av nøkkel som er lagret i legens journal.*

6. Håndtering av informasjonsplikten

Virksomhetene har plikt til å behandle personopplysninger på en åpen måte. Dette innebærer at de må gi kort og forståelig informasjon om hvordan de behandler personopplysningene. Det stilles også krav til hvordan de kommuniserer med enkeltpersoner.

En virksomhet kan kommunisere med enkeltpersoner på mange måter – for eksempel gjennom personvernerklæringer. Virksomheten må da kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.

6.1 Egne ansatte, partnere, styret og tilknyttet fageksperter.

Ansatte informeres gjennom arbeidskontrakt hvilke opplysninger KBB Medic lagrer om den enkelte.

6.2 Personer som har registrert seg i vårt medlemssystem

Ved registrering av abonnement på løsningene våre må abonnentene registrere personlig informasjon om seg selv eller foretak som står som abonnent. Vi vil opplyse om hvilke opplysninger vi lagrer på en lettfattelig måte, at det er mulig å slette seg i vår medlemsdatabase med den følge at medlemskapet opphører.

6.3 Pasienter som er pseudoanonymisert

Når en lege ønsker å diagnostisere og behandle en ny pasient må han opplyse pasienten om at systemet lagrer anonymiserte data som kan hentes opp for en best mulig oppfølging. Legen må verifisere at pasienten har akseptert eller om han/hun ikke aksepterer før man går videre i programmet.

Vi vil lage løsningene våre på en slik måte at de fungerer uavhengig om man lagrer informasjon eller ikke. Hvis man ikke lagrer informasjon må alt tastes inn på nytt ved neste konsultasjon.

7. Håndtering av rettigheter for den det lagres data om

Alle virksomheter har plikt til å legge til rette for at brukere/kunder får oppfylt rettighetene sine på en enkel måte. Det skal som hovedregel gjøres uten kostnad for kunden og innen 30 dager.

Rettigheter forholder seg til 3 punkter: 1.Kredittvurdering, 2.Fødselsnummer, 3. Sletting av søketreff i søkemotorer.

Ingen av disse punktene er relevante for KBB Medic. Men KBB Medic vil legge til rette for at:

1. medlemmer kan bli slettet fra medlemsdatabasen.
2. Pasienter på enkel måte kan be legen om å bli slettet i diagnosesystemene.

8. Personvern Strategi i KBB Medic. Innebygd personvern.

KBB Medic leverer IT-løsninger som behandler personopplysninger og helseopplysninger. KBB har etablert en målsetning om innebygd personvern i alle utviklingsprosjekter. Dette medfører at:

1. alle nyansatte vil bli informert om at KBB Medic tar personvern på alvor.
2. At hvert nytt produkt eller større versjonsendring vil bli revidert med fokus på personvern håndtering.

9. Databehandler avtaler

Personvernforordningen skiller mellom begrepene *behandlingsansvarlig* og *databehandler*. Den behandlingsansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.

KBB Medic leier inn eksterne resurser for utvikling og håndtering av personopplysninger. KBB Medic vil i alle forhold være behandlingsansvarlig og skal:

1. **Tegne databehandler avtale med underleverandører.**

10. Andre forhold

Dette kapittelet tar for seg vurdering av flytting av personvern til utlandet, personvernombud, internkontroll, informasjonssikkerhet, avviksbehandling, protokollføring.

10.1 Flytting av personvern til utlandet

EUs personvernforordning gjelder for EØS-området. Det inkluderer alle EU-land, Island, Liechtenstein og Norge. Når personopplysninger overføres til et land som er etablert utenfor EØS-området, og som ikke er underlagt personvernforordningsregler, gjelder spesielle krav for overføringen slik at beskyttelsesnivået som gjelder i EØS-området ikke undergraves. Personopplysningene må behandles på en forsvarlig måte, selv om de er utenfor forordningens virkeområde.

KBB Medic vurderer å etablere virksomhet i andre deler av verden, Kina, USA etc. Vi vil etablerer egne servere for hver geografisk region.

- **KBB Medic vil derfor <u>ikke</u> behandle persondata som er beskyttet av GDPR i regioner med annet regelverk.**

10.2 Personvernombud

Et personvernombud skal gi råd om hvordan den behandlingsansvarlige best mulig kan ivareta personverninteressene. Noen virksomheter har plikt til å ha ombud, mens andre kan ha det dersom de ønsker. På disse sidene har vi samlet all relevant informasjon om personvernombudsrollen.

- **KBB Medic er et lite selskap i utvikling og vil ikke ha et eget personvernombud.**
- **Daglig leder skal ha det overordnete ansvaret for personvern i selskapet.**

10.3 Internkontroll

Virksomheten må sikre en forsvarlig *behandling av personopplysninger* ved at man ivaretar den registrertes rettigheter og friheter, samtidig som man ivaretar virksomhetens mål ved behandlingen. Etter personvernforordningen (artikkel 24) innebærer det en forholdsmessighet hvor man ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter, og ut fra det gjennomfører egnede tekniske og organisatoriske tiltak. Internkontroll skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte. Tiltakene skal dokumenteres og oppdateres ved behov.

10.4 Informasjonssikkerhet

Personvernregelverket krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for dem.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

- **KBB lager anonymisert informasjon om pasienter på dedikert server leiet inn av underleverandør som har skrevet databehandleravtale. Serveren er sikret med RSA kryptering der tilgang er basert på krypteringsnøkler tildelt enkeltpersoner i KBB som har tilgang.**

10.5 Avviksbehandling

KBB Medic er behandlingsansvarlig virksomhet. Dersom det skjer et avvik (brudd på personopplysningssikkerheten), skal dette rapporteres inn til datatilsynet så snart som mulig.

11. Protokollføring

Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar.

Foretak og organisasjoner med færre enn 250 ansatte har unntak fra kravet om å føre protokoll for visse behandlingsaktiviteter. Unntaket er imidlertid snevert og det vil derfor svært sjeldent gjelde som et absolutt unntak fra hele bestemmelsen.

Protokollen føres i eget xl ark etter mal fra datatilsynet.