INTERN DATABESKYTTELSE

BehandlerLab GDPR-dokumentation

Tekniske sikkerhedsforanstaltninger, dataflow, ansvar og praktisk tjekliste

Dokumentets formål

Dokumentet beskriver BehandlerLabs tekniske databeskyttelse og de arbejdsgange, som den app- og driftsansvarlige samt den enkelte behandlende terapeut skal følge. Dokumentet gælder uanset appens versionsnummer. Ansvarlig rolle: Den app- og driftsansvarlige.

LOKAL LAGRING	KRYPTET OVERFØRSEL	INGEN ANALYTICS
Patientarkiv og programmer gemmes som udgangspunkt på den anvendte enhed.	Engangsoverførsler udløber efter 10 min. Krypterede patientlinks efter 30 dage.	Ingen reklamesporing, brugerprofilering eller analyseværktøjer i appen.

Vigtig afgrænsning

BehandlerLab er ikke GDPR-godkendt eller certificeret. GDPR har normalt ingen forhåndsgodkendelse af en app. Den app- og driftsansvarlige skal dokumentere de tekniske foranstaltninger, mens den dataansvarlige terapeut eller organisation skal dokumentere sin konkrete anvendelse.

1 Formål, anvendelse og ansvar

BehandlerLab er udviklet efter principperne om dataminimering, privatliv som standard og risikobaseret sikkerhed. Appen anvendes udelukkende til udarbejdelse, formidling og opdatering af træningsprogrammer og skal ikke anvendes som patientjournal. Arbejdspladsens godkendte journalsystem anvendes til al journalføring.

I behandlerdelen anvendes kun patientens initialer eller et internt patient-ID. CPR-nummer, adresse, diagnoser, sygehistorik, journalnotater og andre unødvendige personoplysninger må ikke registreres. Appen afviser indtastninger, der ligner CPR-numre, i patientfeltet. Patientnavnet medsendes ikke automatisk i patientlinks eller ved patientens returnering af et program. Journalrelevante oplysninger dokumenteres i arbejdspladsens godkendte journalsystem.

Behandlerens patientarkiv og programmer gemmes som udgangspunkt lokalt på den enhed, hvor appen anvendes. Oplysningerne overføres derfor ikke automatisk til en central server. Enheden skal være beskyttet med opdateret styresystem, enhedskryptering, skærmlås og automatisk låsning. BehandlerLabs egen adgangskode er et ekstra skærmlag, men erstatter ikke enhedens sikkerhed.

Roller og ansvar

Den app- og driftsansvarlige for BehandlerLab er ansvarlig for appens tekniske udformning, opdateringer og serveropsætning. Den terapeut, klinik eller organisation, der bruger appen til patientforløb, er dataansvarlig for den behandling af personoplysninger, der sker i forbindelse med disse forløb.

Hvis en anden terapeut eller klinik bruger appen selvstændigt til egne patienter, er den pågældende terapeut eller klinik dataansvarlig for disse oplysninger. Den dataansvarlige fastlægger formål, behandlingsgrundlag, slettefrister, adgangsregler og patientinformation samt indgår relevante databehandleraftaler.

- BehandlerLab understøtter dataminimering, men kan ikke forhindre alle uhensigtsmæssige indtastninger.
- Sikkerheden afhænger både af appens teknik og den enkelte dataansvarliges enheder, adgangsstyring og arbejdsgange.
- Helbredsoplysninger er følsomme personoplysninger og kræver en dokumenteret, risikobaseret beskyttelse.

Dataminimering i praksis

Brug eksempelvis PT-1047 eller patientens initialer. Undlad CPR-nummer, adresse, telefonnummer, diagnose, journaltekst og fritekst om sygdomshistorik. Sådanne oplysninger hører til i arbejdspladsens godkendte journalsystem.

2 Tekniske sikkerhedsforanstaltninger

Lokal lagring og adskilte brugerflader

- Behandlerdata gemmes som udgangspunkt i browserens localStorage og IndexedDB på den konkrete enhed.
- Patientvisningen anvender et særskilt lokalt datalager og giver ingen adgang til behandlerudgaven.
- Patientens hentede program og smerteregistreringer gemmes lokalt på patientens enhed. Den krypterede originale linkpakke kan genhentes fra Cloudflare i 30 dage.
- Appens adgangskode beskytter brugerfladen, mens enhedens PIN-kode, biometri og kryptering beskytter selve enheden.

Krypteret internetoverførsel

- Programmet AES-GCM-krypteres på afsenderens enhed før upload.
- Cloudflare Worker modtager et tilfældigt ID, størrelse, tidsstempler og krypterede bytes - ikke dekrypteringsnøglen.
- Nøglen står efter # i linket. Browserfragmentet bliver ikke sendt med HTTP-anmodningen til serveren.
- Almindelige overførsler og patientretur udløber efter 600 sekunder og slettes efter vellykket modtagelse.
- En patientlinkpakke kan genhentes i 30 dage. Serveren har fortsat kun krypterede bytes; dekrypteringsnøglen står i linkets browserfragment.
- Udløbne pakker ryddes ved statuskontroller og nye uploads.
- QR-streaming kan anvendes som direkte, offline overførsel mellem enheder.

Billeder, fællesbibliotek og AI

- Valgte fotos genkodes lokalt før lagring, hvilket normalt fjerner den oprindelige fils kamera- og EXIF-metadata.
- Fællesbiblioteket må kun indeholde generelle øvelsesbilleder, beskrivelser og tags - aldrig patientdata.
- Ved AI-generering sendes kun den tekst, brugeren skriver som øvelsesbeskrivelse. Der må ikke indtastes patientoplysninger.
- OpenAI API-nøglen opbevares som en krypteret Worker-secret i Cloudflare og ligger ikke i appens klientkode.

Web- og serverhærdning

- Sikkerhedsheaders begrænser indlejring, referrer-lækage, MIME-sniffing og unødvendige browserfunktioner.
- Appen indeholder ikke analytics, reklamesporing eller brugerprofilering.
- Vedvarende Cloudflare Workers Logs og Traces er deaktiveret. Cloudflare kan fortsat behandle nødvendig teknisk driftsmetadata efter sine vilkår.

3 Dataflow og opbevaring

Tabellen viser, hvilke datatyper der kan forekomme, hvor de befinder sig, og hvordan de slettes. Den dataansvarlige fastlægger og dokumenterer slettefristerne for sin konkrete anvendelse og sine patientforløb.

Funktion	Oplysninger	Placering	Sletning
Patientarkiv	Initialer/internt ID og gemte programmer	Terapeutens enhed	Slet patienten under Programmer
Patientlink	Øvelser, billeder og træningsparametre	Patientens enhed samt krypteret linkpakke i Cloudflare D1	Lokalt: ryd appdata. Server: automatisk efter 30 dage
Almindelig overførsel og patientretur	Tilfældigt ID, størrelse, tidsstempler og krypterede bytes	Cloudflare D1	Efter modtagelse eller senest efter 10 min.
Fællesbibliotek	Generelle øvelsesbilleder, navn, beskrivelse og tags	Cloudflare D1/R2	Centralt lager; må ikke indeholde patientdata
AI-billede	Den skrevne øvelsesbeskrivelse	Cloudflare Worker og OpenAI API	Skriv aldrig identifikatorer eller patienthistorik
Backupfil	Hele behandlerarkivet	Den placering brugeren vælger	Slet efter indlæsning eller den fastsatte frist

Særligt om backup

Manuelle backupfiler er ikke krypterede

En .oesbackup-fil kan indeholde initialer, programmer, kommentarer og helbredsoplysninger. Den må kun opbevares i et lager, som den dataansvarlige har godkendt og adgangsbeskyttet, og bør slettes, når den er indlæst eller har nået den fastsatte slettefrist.

Patientens rettigheder og gennemsigtighed

- Patienten bør informeres om, hvilke oplysninger træningsprogrammet indeholder.
- Patienten bør vide, at program og registreringer gemmes lokalt, mens den krypterede oprindelige patientlinkpakke kan genhentes i op til 30 dage.
- Patienten bør vide, at returdata kan sendes krypteret til behandleren.
- Den dataansvarlige skal oplyse slettefristen og kontaktvejen for indsigt, rettelse og sletning for de patientforløb, hvor appen anvendes.

4 Praktisk GDPR-tjekliste

Tjeklisten anvendes af den app- og driftsansvarlige og de relevante dataansvarlige og tilpasses den konkrete anvendelse. Sæt dato og ansvarlig på kontrollen.

Før appen tages i brug

- ☐ Appen anvendes udelukkende til træningsprogrammer og ikke som patientjournal; al journalføring sker i arbejdspladsens godkendte journalsystem.
- ☐ Der anvendes kun initialer eller internt patient-ID.
- ☐ CPR-nummer, adresse, diagnoser, sygehistorik og journaltekst registreres ikke.
- ☐ Alle enheder har PIN-kode eller biometri, enhedskryptering og automatisk lås.
- ☐ Kun den app- og driftsansvarlige eller særskilt autoriserede administratorer har administrativ adgang til Cloudflare-kontoen, som er beskyttet med totrinsbekræftelse.
- ☐ Den app- og driftsansvarlige har vurderet og dokumenteret Cloudflares databehandleraftale og underdatabehandlere.
- ☐ Den dataansvarlige har besluttet konkrete slettefrister for patientarkiver, returdata og backupfiler.
- ☐ Patientinformationen beskriver appens behandling af oplysninger.

Ved daglig brug

- ☐ Det kontrolleres, at det rigtige program sendes til den rigtige patient.
- ☐ Patientlinks behandles som fortrolige adgangsnøgler og sendes direkte til modtageren.
- ☐ Der uploades aldrig patientbilleder eller patientoplysninger til fællesbiblioteket.
- ☐ AI-beskrivelser indeholder ingen patientoplysninger.
- ☐ Der skrives ikke oplysninger i appen, som hører til i arbejdspladsens godkendte journalsystem.
- ☐ En mistet eller stjålet enhed håndteres straks af den dataansvarlige og meddeles den app- og driftsansvarlige, hvis appens fælles adgangskoder kan være berørt.

Kontrol udført af	Dato	Næste kontrol

4 GDPR-tjekliste - fortsat

Overførsel og backup

☐ Internetoverførsel eller direkte QR-overførsel anvendes til programmer.

☐ Overførslen testes på modtageren, inden den betragtes som gennemført.

☐ Backupfiler opbevares kun i et godkendt og adgangsbeskyttet lager.

☐ Backupfiler sendes ikke via almindelig ukrypteret e-mail.

☐ Midlertidige backupfiler slettes efter indlæsning.

Løbende kontrol

☐ Udløbne patientarkiver, programmer og backupfiler slettes mindst én gang om måneden.

☐ Den app- og driftsansvarlige kontrollerer kvartalsvist Cloudflare-kontoens totrinsbekræftelse, bindings, secrets og deployments.

☐ Workers Logs og Traces forbliver deaktiveret, medmindre der er et dokumenteret fejlsøgningsbehov.

☐ Eventuel midlertidig administrativ Cloudflare-adgang til andre fjernes straks, når behovet ophører.

☐ Appens fælles adgangskoder skiftes af den app- og driftsansvarlige, hvis uvedkommende kan have fået kendskab til dem.

☐ Appens patientlink, patientretur, krypterede overførsel, sletning og backup testes efter opdateringer.

☐ Sikkerhedsbrud registreres, dokumenteres og vurderes i forhold til anmeldelse til Datatilsynet.

Ved mistet enhed eller mulig datalækage

• Forsøg straks at låse eller fjernslette enheden via Apple, Google eller en eventuel central enhedsstyring.

• Fjern brugeradgang, og bed den app- og driftsansvarlige skifte relevante fælles adgangskoder, hvis de kan være kompromitteret.

• Notér tidspunkt, berørte oplysninger, sandsynlige konsekvenser og gennemførte afhjælpninger.

• Vurder uden unødigt ophold, om hændelsen skal anmeldes til Datatilsynet og eventuelt meddeles patienten.

5 Begrænsninger, beslutninger og kilder

Det teknikken ikke kan løse alene

- Appen kan ikke gøre en uhensigtsmæssig arbejdsgang lovlig.
- Den dataansvarlige skal fastlægge behandlingsgrundlag, oplysningspligt og slettefrister for de patientforløb, hvor appen anvendes.
- Den indbyggede fælles adgangskode er et ekstra skærmlag, ikke stærk kryptering, og må ikke stå alene.
- Manuelle backupfiler er ukrypterede.
- Advarsler mod patientdata i AI og fællesbibliotek kræver, at brugerne følger dem.
- Eksterne leverandørers vilkår, underdatabehandlere og eventuelle tredjelandsoverførsler skal vurderes løbende.

Ingen forhåndsgodkendelse
En almindelig app skal normalt ikke godkendes af Datatilsynet før brug. GDPR bygger på ansvarlighed: Den app- og driftsansvarlige skal dokumentere appens tekniske foranstaltninger, mens den enkelte dataansvarlige dokumenterer sin konkrete anvendelse. Frivillig certificering er ikke et krav og fjerner ikke ansvaret.

Beslutninger og ansvar

App- og driftsansvarlig	_____
Formål med behandlingen	_____
Patientarkivets slettefrist	_____
Returdata og registreringers slettefrist	_____
Backupfilers slettefrist og placering	_____
Ansvarlig for kvartalsvis kontrol	_____
Dato for seneste risikovurdering	_____

Autoritative udgangspunkter

- Datatilsynet - Rollefordeling: dataansvarlig og databehandler
- Datatilsynet - Risikovurdering
- Datatilsynet - Cloud
- GDPR - artikel 5, 25 og 32
- Cloudflare - GDPR og databehandleraftale

Dokumentstatus: Udarbejdet som intern dokumentation for BehandlerLab den 24. august 2026. Dokumentet gælder uanset appens versionsnummer. Det er intern støtte og ikke juridisk rådgivning og bør gennemgås igen, hvis appens formål, datalagring, leverandører eller funktioner ændres.