Sådan behandler vi personfølsomme data i Reach Psykologer ApS

Formål

Dette dokument beskriver, hvordan vi i Reach Psykologer ApS arbejder med personfølsomme og fortrolige oplysninger i praksis.

Alle psykologer tilknyttet Reach har tilsluttet sig disse retningslinjer og har skrevet under på, at de følger dem i deres daglige arbejde. Det er en del af vores fælles faglige og etiske ansvar at beskytte klienters data med høj omhu.

Dokumentet supplerer vores privatlivspolitik og skal sikre en fælles, ansvarlig og gennemsigtig praksis for databeskyttelse.

Overordnede principper

- Al kommunikation og databehandling skal ske med et sikkerhedsniveau, der passer til oplysningernes følsomhed.
- Der skelnes mellem almindelige personoplysninger og særligt følsomme oplysninger (fx helbredsoplysninger, CPR-numre og erklæringer).
- Sikkerhedsforanstaltninger tilpasses datatypens følsomhed.
- Retningslinjerne beskriver vores faste praksis og arbejdsgange. Hvis der opstår fejl eller afvigelser, arbejder vi for at opdage dem, rette op og forbedre vores procedurer.

E-mail og sikker kommunikation

Vi anvender to sikkerhedsniveauer i vores e-mailkommunikation:

1) TLS-kryptering (standardniveau)

- TLS (Transport Layer Security) anvendes som minimum ved e-mailkommunikation.
- TLS beskytter overførslen mellem servere og anvendes til almindelig, ikke-særlig-følsom kommunikation (fx praktiske aftaler).
- Hos vores mailudbyder (Zoho) er mails og vedhæftninger desuden krypteret på serverniveau.
- Almindelig e-mail anvendes ikke til udveksling af særligt følsomme oplysninger.

Praksis:

- Der må ikke laves usikrede sikkerhedskopier af mails.
- Mails må ikke videresendes til usikre systemer.
- Klienter opfordres til at slette korrespondance løbende og anvende opdaterede systemer.

2) End-to-end-kryptering (forhøjet sikkerhed)

- End-to-end-kryptering anvendes som standard ved udveksling af særligt følsomme oplysninger, herunder:
    - CPR-numre
    - helbredsoplysninger
    - psykologerklæringer
    - bankoplysninger
- Ved denne metode er indholdet krypteret, så kun den tilsigtede modtager kan læse det.
- Denne metode er vores faste praksis ved udveksling af særligt følsomme data.

Hvis klienter selv skal sende følsomme oplysninger, vejleder vi dem i at anvende sikre metoder.

Læs mere om Zoho's kryptering her:
https://www.zoho.com/encryption.html

Retningslinjer fra myndigheder og faglige anbefalinger

Datatilsynet

- TLS er minimumskrav ved overførsel af fortrolige eller følsomme oplysninger.
- Ved særlig høj risiko (fx helbredsoplysninger) anbefales stærkere foranstaltninger, såsom end-to-end-kryptering (god praksis).

Dansk Psykologforening

Dansk Psykologforening anbefaler bl.a., at:

- Ansvaret for personfølsomme data altid ligger hos psykologen og ikke kan fraskrives.
- Man ikke svarer direkte på usikre eller ukendte mailtråde, men opretter en ny, sikker mailtråd.
- Kalendere og systemer anvendes med dataminimering (fx initialer eller interne ID'er).
- Der ikke foretages usikrede backups til private eller ukrypterede cloud-tjenester.
- Kommunikation om klientforhold ikke foregår via sociale medier.

Kilde:
https://www.dp.dk/wp-content/uploads/spoergsmaal-om-datasikkerhed-1.pdf

---

Systemer og databehandlere hos Reach

Vi opbevarer og behandler personoplysninger i følgende systemer, afhængigt af formål:

- Zoho (e-mail)
- Wix (hjemmeside, booking og administration)
- Aidaform (formularløsninger)
- Whereby (videokonsultation)
- Bank og betalingsudbyder (fx Stripe)
- Vores journalsystem

Vi anvender kun systemer, der lever op til gældende krav om datasikkerhed, og vi har indgået relevante databehandleraftaler, hvor det er påkrævet.

Interne retningslinjer (god praksis)

- Vi har som standard opsat to-trins-godkendelse på alle relevante platforme.
- Almindelig e-mail anvendes kun til praktisk og ikke-særlig-følsom kommunikation.
- End-to-end-kryptering anvendes som standard ved særligt følsomme oplysninger.
- Klienter vejledes i sikker fremsendelse af følsomme oplysninger.
- Der svares ikke direkte på usikre henvendelser – der oprettes i stedet en ny, sikker mailtråd.
- Klienter informeres om, at vi ikke kan garantere sikkerheden af indhold, når mails ligger i deres egen indbakke, og opfordres løbende til at slette korrespondance.
- Vi har en praksis for løbende at gennemgå og slette mails, som udgangspunkt efter 6 måneder uden kontakt, medmindre indholdet er relevant for journalisering. Relevant indhold overføres i så fald til journalen eller opbevares sikkert.
- Når et forløb afsluttes, har vi en fast praksis for at slette klientens kontaktoplysninger i relevante systemer (fx Zoho og Wix).
- Af hensyn til journalpligt opbevares nødvendige basisoplysninger i journalen i minimum 5 år.
- Når en klientprofil slettes, informeres klienten herom.

Særligt om Aidaform

Aidaform har servere uden for EU. Derfor anvender vi ekstra sikkerhedsforanstaltninger:

- Der anvendes svar-ID i stedet for navn eller andre direkte personhenførbare oplysninger.
- Svar-ID genereres af psykologen og opbevares i klientens journal.
- Klienter opfordres kun til at anvende fornavn som identifikation i formularbesvarelser.

Særligt om Wix

Vores hjemmesideudbyder Wix er certificeret inden for bl.a. ISO, PCI og TLS.
Læs mere her:
https://support.wix.com/en/article/security-of-wixs-billing-services-and-pci-compliance#iso-compliance

Ved brug af synkronisering til kalender kan klientnavne efter opstart af forløb ændres til initialer. Klienten informeres herom.

Opbevaring af journal

- Digitale journaler opbevares på en sikker, ekstern harddisk.
- Journaler er ikke tilgængelige fra internettet.
- Adgang til journaler er beskyttet med adgangskode.
- Fysiske journaler opbevares aflåst i overensstemmelse med gældende regler.

Revision og efterlevelse

- Retningslinjerne gennemgås løbende og opdateres ved ændringer i systemer, praksis eller lovgivning.
- Alle psykologer tilknyttet Reach er forpligtet til at kende og efterleve disse retningslinjer.