Adent

WHITE PAPER

Hvad skal en tandklinik kryptere

En guide til danske tandklinikker om kryptering af patient-kommunikation under GDPR, sundhedsloven og Datatilsynets skærpede praksis.

Version 1.0 · Juni 2026
Udgivet af Adent · adent-health.com

RESUMÉ

Resumé

Tandklinikker behandler hver dag helbredsoplysninger, og det er en særlig kategori af persondata under GDPR Artikel 9. Det betyder skærpede krav til kryptering ved transmission via email, og pligten gælder langt mere end CPR-numre.

Dette white paper gennemgår, hvad der i praksis skal krypteres på en tandklinik, hvorfor sundhedssektoren har skærpede krav, og hvilke konkrete eksempler klinikker ofte overser. Vi belyser kombinationsprincippet, der gør almindelig korrespondance til en helbredsoplysning, så snart en identifikator og en behandlingsinformation optræder i samme besked.

Vi gennemgår også de typiske faldgruber i emnefelter, filnavne og vedhæftninger samt myten om, at en kodeordsbeskyttet PDF i sig selv er en sikker forsendelse. Endelig samler vi Datatilsynets praksis og giver et overblik over, hvordan kravene kan håndteres automatisk i hverdagen.

Hovedpointer

- Helbredsoplysninger er en særlig kategori under GDPR Artikel 9 med skærpede sikkerhedskrav.
- Kombinationsprincippet: når en besked indeholder både en identifikator og en behandlingsinformation, er den en helbredsoplysning, også uden CPR.
- Emnefelter og filnavne krypteres ikke i alle løsninger og kan i sig selv lække patientdata.
- En kodeordsbeskyttet PDF er ikke transportsikkerhed. Lave entropi-koder som fødselsdato kan brydes på sekunder.
- Datatilsynet kræver dokumentation for, at krypteringen faktisk er sket, ikke kun at den var tilsigtet.

INDHOLD

Indholdsfortegnelse

AFSNIT 1

Hvorfor sundhedssektoren har skærpede krav

Tandlæger, tandplejere og klinikassistenter er sundhedspersoner. Det giver tre lag af regulering oven på de almindelige regler for behandling af personoplysninger.

GDPR Artikel 9 og 32

Helbredsoplysninger er en særlig kategori jf. Artikel 9, og kræver et særligt behandlingsgrundlag og skærpede sikkerhedsforanstaltninger. Artikel 32 nævner kryptering eksplicit som en passende foranstaltning ved behandling af personoplysninger.

Sundhedsloven §§ 40-46

Sundhedspersoner har tavshedspligt efter sundhedslovens §§ 40-46. Videregivelse af patientoplysninger kræver typisk samtykke eller særlig hjemmel, og kommunikationen skal i alle tilfælde være sikret mod uautoriseret indsigt.

Autorisationsloven § 17

Sundhedspersoner er forpligtet til at udvise omhu og samvittighedsfuldhed i deres virke. Det omfatter også håndteringen af patientdata og valget af tekniske foranstaltninger til at beskytte dem.

Datatilsynet har siden 2019 lagt en fast linje: Fortrolige og følsomme oplysninger må ikke sendes via ukrypteret email over åbne netværk. For helbredsoplysninger er udgangspunktet end-to-end-kryptering eller forced TLS med dokumentation.

AFSNIT 2

Tre kategorier af data

Det hjælper at kende de tre lag, fordi kravet til kryptering vokser med følsomheden.

Persondata

Enhver oplysning, der direkte eller indirekte kan henføres til en fysisk person. Navn, telefonnummer, email og IP-adresse er klassiske eksempler. Personoplysninger skal beskyttes, men kravet til kryptering afhænger af, hvor følsomt indholdet er.

Fortrolige oplysninger

Eksempelvis CPR-nummer og økonomiske forhold. Datatilsynet kræver kryptering ved transmission via åbne net.

Helbredsoplysninger

Alle oplysninger, der vedrører en fysisk persons fysiske eller psykiske helbred, inklusive den behandling, vedkommende modtager. Det er den særlige kategori i Artikel 9, og kravet til sikkerhed er det højeste. Hovedreglen for tandklinikker er, at langt det meste patientkorrespondance falder i kategorien fortrolige eller helbredsoplysninger.

AFSNIT 3

Kombinationsprincippet

En af de største faldgruber er, at klinikker kun krypterer beskeder, der nævner CPR. Men kombinationer kan være lige så identificerende, og i det øjeblik en kombination afslører noget om helbred, bliver hele meddelelsen til en helbredsoplysning.

Et konkret eksempel: En mail med navn, adresse og "overslag på rodbehandling" indeholder ikke CPR-nummer. Men kombinationen identificerer en konkret person og oplyser om en planlagt behandling, og dermed om vedkommendes tandsundhed. Den er en helbredsoplysning og skal krypteres.

Princippet hedder indirekte identifikation. GDPR Artikel 4(1) definerer persondata som oplysninger, der kan henføres til en person, direkte eller via en kombination af elementer. Det betyder, at klinikken ikke kan vurdere én oplysning ad gangen, men skal se på den samlede besked.

Eksempler på kombinationer

- Navn + fødselsdato + behandlingstype
- Adresse + behandling, især i mindre byer
- Email + diagnose eller medicinering
- Telefonnummer + henvisning til specialist
- Initialer + behandlingsdato + klinikkens navn

Tommelfingerregel

Hvis en udefrakommende kunne læse mailen og med rimelig sandsynlighed gætte både, hvem patienten er, og hvad de fejler, skal mailen krypteres.

AFSNIT 4

Helbredsoplysning plus identifikator

Kombinationsprincippet bliver lettere at huske i praksis, hvis man tænker det som to kategorier. Hver kategori for sig er ikke nødvendigvis personhenførbar, men så snart en besked indeholder elementer fra begge, bliver hele beskeden til en helbredsoplysning.

HELBREDSOPLYSNING ELLER DOKUMENT

- Journalnotat eller journaludskrift
- Behandlingsplan eller overslag
- Diagnose
- Røntgenbillede
- Intraoralt foto
- Ydelseskode (f.eks. 4111 for rodbehandling)
- Medicinordination
- Henvisning til specialist
- Allergier og sygdomshistorik
- Tandstatus og parodontale målinger
- Aftaletype eller behandlingstype

IDENTIFIKATOR (PEGER PÅ EN PERSON)

- Navn
- CPR-nummer
- Adresse
- Email
- Telefonnummer
- Fødselsdato
- Patientnummer
- Initialer + by
- Foto af person

Reglen: Indeholder en besked mindst én oplysning fra venstre kolonne og mindst én fra højre, er den en helbredsoplysning og skal krypteres.

AFSNIT 5

Fem konkrete eksempler, der ofte glemmes

5.1 Fakturaer og kvitteringer med ydelseskode

En faktura med ydelseskode (f.eks. 1401 for tandrensning eller 4111 for rodbehandling) plus navn og adresse er en helbredsoplysning, også uden CPR. Ydelseskoderne er offentligt tilgængelige og kan slås op.

5.2 Behandlingsoverslag

Et behandlingsoverslag indeholder per definition en planlagt behandling. Sendt med navn, adresse eller kontaktoplysninger er det en helbredsoplysning. Selv uden CPR er kombinationen tilstrækkelig til at identificere både person og helbredsforhold.

5.3 Aftalebekræftelser med behandlingstype

Hvis klinikken besvarer en email, som patienten selv har sendt, f.eks. med "bekræftelse på rodbehandling tirsdag kl. 10", afsløres et konkret behandlingsforhold sammen med patientens email-adresse. Det gælder, selvom oplysningerne allerede var i den email, patienten selv har delt.

5.4 Korrespondance med forsikringsselskaber

Korrespondance med forsikringsselskaber indeholder næsten altid både helbredsoplysninger, økonomiske oplysninger og navne. Flere forsikringsselskaber er i dag på EDI-portalen. For dem, der ikke er, skal hele korrespondancen krypteres.

5.5 SMS-påmindelser med specifik information

"Vi minder om din tid til ortodontisk konsultation" sendt via almindelig SMS afslører et behandlingsforhold. Generelle påmindelser ("Du har en aftale i morgen") er som hovedregel mindre problematiske, men jo mere specifik beskeden er, jo strengere bliver kravet.

AFSNIT 6

Det skjulte i mailen

En overset faldgrube er, at emnefelter og filnavne ikke krypteres i alle løsninger, selvom selve indholdet gør.

Emnefeltet

"Vedr. behandlingsplan for Lars Hansen" i emnefeltet er en helbredsoplysning, før modtageren overhovedet åbner mailen. Hold emnefeltet generisk, f.eks. "Vedr. din næste aftale" eller "Sikker post fra klinikken".

Filnavne

Et filnavn som "Jensen_OPG_2026.jpg" røber både identitet og indhold (OPG er forkortelsen for ortopantomogram, et røntgenbillede af hele kæben). Brug filnavne uden patientidentifikation, eller send filer via sikker patientportal.

Vedhæftninger

En PDF, et røntgenbillede eller et foto følger de samme regler som selve mailen. En krypteret mail med en vedhæftet OPG i klartekst er ikke godt nok, hvis krypteringen ikke omfatter vedhæftningen.

AFSNIT 7

Myten om kodeordsbeskyttede PDF’er

En udbredt misforståelse er, at en kodeordsbeskyttet PDF, der låses op med en SMS-kode, automatisk er en sikker forsendelse. Det er den ikke. Der er flere lag, der skal være på plads, før kommunikationen er reelt sikker.

7.1 PDF-kodeord er ikke transportsikkerhed

En adgangskode på selve PDF-filen beskytter kun, når filen åbnes. Den siger ikke noget om, hvordan filen sendes fra klinikken til patientens mailserver. Hvis mailen sendes via ukrypteret SMTP, kan en angriber opsnappe selve PDF-filen undervejs, gemme den og arbejde med den i ro og mag bagefter. Derfor er TLS-kryptering på selve transmissionen stadig nødvendig, også selvom PDF’en er låst.

7.2 Lave entropi-koder kan brydes på sekunder

Sikkerheden af en kodeordsbeskyttet PDF afhænger af adgangskodens styrke. Mange klinikker bruger oplysninger, som patienten allerede kender, f.eks. fødselsdato eller CPR-nummer. Det er meget svagere, end det lyder.

- Fødselsdato (6 cifre, DDMMÅÅ): kun 1 million mulige kombinationer. Brydes på sekunder, også på en ganske almindelig computer.
- CPR-nummer (10 cifre): ser ud som 10 milliarder kombinationer, men de første 6 cifre er fødselsdatoen, som ofte kan gættes eller udledes af mailens kontekst. De sidste 4 cifre følger desuden strukturelle regler. Den effektive entropi er langt lavere end 10 milliarder.
- SMS-kode på 4-6 cifre: hvis den er reelt tilfældig og kun gælder kort tid, tilbyder den begrænset, men reel beskyttelse. Hvis den genbruges, gemmes eller har lang levetid, falder beskyttelsen markant.

Selv på en almindelig kontorcomputer kan en sekscifret kode brute-forces på minutter.

7.3 Offline-brute-force har ingen rate limit

Det er forskellen på et online-system og en offline-fil. På en patientportal kan systemet låse efter f.eks. fem forkerte forsøg. På en PDF-fil, som angriberen allerede har hentet ned, er der ingen begrænsning. Angriberen kan prøve uendeligt mange adgangskoder uden klinikkens vidende og uden nogensinde at blive opdaget.

7.4 Hvad skal der så til?

En kodeordsbeskyttet PDF kan være et nyttigt ekstra lag, men kun under tre forudsætninger.

- Selve transmissionen er krypteret med TLS, så filen ikke kan opsnappes som klartekst.
- Adgangskoden er reelt tilfældig og ikke baseret på fødselsdato, CPR eller andre oplysninger, der kan gættes.
- Koden har kort levetid og bruges kun til den konkrete forsendelse.

Den mest robuste model er en sikker patientportal med MitID eller 2FA-kode, hvor adgangen er online-kontrolleret og kan låses ved mistanke om misbrug.

AFSNIT 8

Datatilsynets praksis

Datatilsynet skærpede i juli 2018 sin praksis for kryptering af email med fortrolige og følsomme personoplysninger. For den private sektor trådte den nye praksis i kraft den 1. januar 2019. Hovedlinjerne kan opsummeres således.

- Ved transmission af fortrolige og følsomme oplysninger via åbne net, herunder almindelig email, skal der anvendes kryptering.
- For helbredsoplysninger er udgangspunktet end-to-end-kryptering eller forced TLS med dokumentation for, at krypteringen faktisk er etableret.
- Klinikken skal kunne dokumentere, at krypteringen er sket, ikke kun at den var tilsigtet.
- Manglende kryptering kan udløse påtaler, bøder og pligt til at underrette patient og Datatilsynet ved brud.

Bevisbyrden ligger hos klinikken som dataansvarlig. Hvis Datatilsynet beder om dokumentation, skal klinikken kunne fremvise, at den konkrete mail blev sendt krypteret, og hvilken krypteringsstandard der blev brugt.

AFSNIT 9

Sådan automatiseres kravene i hverdagen

Adent leverer en løsning, der krypterer forsendelser automatisk fra klinikkens journalsystem og fra Outlook, så personalet ikke selv skal vurdere, hvad der skal krypteres og hvordan.

Tre leveringsveje vælges automatisk

- Forced TLS-sikkermail: til almindelig patientkommunikation, hvor modtagerens mailserver understøtter krypteret forbindelse.
- Tunnelmail med certifikat: til kommuner, regioner, forsikringsselskaber og andre klinikker, hvor certifikat-baseret kryptering er påkrævet.
- Sikker patientportal: hvis ingen krypteringsmetode kan etableres, leveres beskeden via portal med MitID eller 2FA-kode.

Hver afsendelse logges med dokumentation for kryptering og levering, så klinikken har beviset klar ved tilsyn. Personalet skal ikke vurdere, om en mail skal krypteres, det sker automatisk i baggrunden.

REFERENCER

Kilder

GDPR (Forordning 2016/679)
Art. 4(1) definition af personoplysninger; Art. 4(15) helbredsoplysninger; Art. 5(1)(f) integritet og fortrolighed; Art. 9 særlige kategorier; Art. 32 sikkerhed ved behandling; Betragtning 35.

Databeskyttelsesloven
Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Sundhedsloven
Kapitel 9, §§ 40-46, om tavshedspligt og videregivelse af helbredsoplysninger.

Autorisationsloven
§ 17 om sundhedspersoners pligt til omhu og samvittighedsfuldhed.

Bekendtgørelse om patientjournaler
BEK nr. 1225 af 8. juni 2021 om autoriserede sundhedspersoners patientjournaler.

Datatilsynet — Skærpet praksis ift. krypteret e-mail (juli 2018)
datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail

Datatilsynet — Vejledning om behandlingssikkerhed
datatilsynet.dk (vejledninger om sikkerhedsforanstaltninger i henhold til GDPR Art. 32)

European Data Protection Board (EDPB)
edpb.europa.eu — Guidelines om særlige kategorier af persondata.

ENISA — Procurement Guidelines for Cybersecurity in Hospitals
enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

UDGIVER

Om Adent

Adent leverer digitale løsninger til danske tandklinikker. Vores fokus er at fjerne manuelle arbejdsgange og sikre, at klinikkens kommunikation med patienter, kolleger, forsikringsselskaber og myndigheder lever op til kravene i GDPR og sundhedsloven, uden at det belaster personalet i hverdagen.

Vores sikkermail-løsning krypterer automatisk forsendelser fra klinikkens journalsystem (DentalSuite, al dente og Muntra) og fra Outlook (både Web og Classic desktop). Systemet vælger den rette leveringsvej for hver besked og logger dokumentation for kryptering og levering, klar til Datatilsynet.

Kontakt

Adent
adent-health.com
Kontakt via formular på adent-health.com/kontakt

Disclaimer

Dette dokument er udarbejdet som en generel vejledning og udgør ikke juridisk rådgivning. Konkrete vurderinger af klinikkens behandling af personoplysninger bør foretages med inddragelse af klinikkens databeskyttelsesrådgiver eller advokat. Indholdet er baseret på gældende ret og Datatilsynets praksis pr. juni 2026.