CORALWARD
PRIVATE AI. ABSOLUTE SOVEREIGNTY.

PRIVATE AI · CYBERSECURITY
HONOLULU · HAWAII

FOR MEDICAL & DENTAL PRACTICES · HAWAII

Private AI for Medical & Dental Practices

Patient information stays where your patients left it. With you.

Clinics and dental practices hold the most sensitive data in any small business, on systems that were never designed for the AI era. Coralward gives your team **a private, sanctioned way to use AI** so the unsafe shortcuts stop.

The systems you run on

athenaOne / eClinicalWorks — cloud EHR and billing used by independent clinics

Epic — the hospital system your practice connects to, even if you don't run it

Dentrix / Dentrix Ascend — the dental practice standard — scheduling, charting, imaging, claims

Eaglesoft / Open Dental — server-based dental systems that live in your office

Insurer portals & e-prescribing — the credential paths claims and prescriptions move through

Clearinghouses & patient portals — claims, messages, and referrals handled by vendors on your behalf

Inside those systems: Patient charts and treatment notes, dental imaging, diagnoses and lab results, Social Security numbers, insurance and claims data, card payments, and the staff credentials for insurer and e-prescribing systems.

17% of healthcare providers and administrators surveyed admitted using **unapproved AI tools** in their work — most often just to get things done faster.

Where it can go wrong

- **Your vendor's breach becomes yours** — Change Healthcare (2024) was entered through a remote-access portal without MFA and affected roughly 193 million people and small practices felt it for months
- **Ransomware on the office server** — in-office dental and records servers with weak remote access and untested backups are routine targets. Downtime means a closed practice
- **Shadow AI with patient data** — notes or patient messages pasted into a tool with no Business Associate Agreement is an impermissible disclosure of PHI

What Coral Ward does

— **Cyber Audit & Review** — vulnerabilities, remote-access paths, backups and a clear-eyed review of every vendor touching patient data

— **Ask Your Files Anything** — private document intelligence over your protocols, policies, and consent forms; answers never leave the building

— **Private correspondence triage** — portal messages, referrals, and faxes sorted and drafted on-site. Your staff approve everything before it moves

THE RULES YOU ANSWER TO

HIPAA Privacy & Security Rules — a documented security risk analysis is required, and is the first thing regulators ask for · **Business Associate Agreements** — required before any vendor, including an AI tool, touches patient information · **Breach Notification Rule** — affected individuals notified within 60 days; larger breaches also go to HHS

Begin with a complimentary discovery call

30 minutes with Mo — how AI is already being used in your business, and what it looks like done privately. No obligation.

CORALWARD.COM

Statistic: Wolters Kluwer Health survey, Dec 2025 (n=518). Healthcare breach cost benchmark: $7.42M average — IBM, Cost of a Data Breach Report 2025. Coralward is a boutique consultancy; this overview is general information, not legal or compliance advice. © 2026 Coralward, Honolulu, Hawaii.