



A physician's own case log and continuity-of-care record

PDI Med is a documentation and case-log tool built by a physician. A physician uses it to keep an organized record of the patients they care for and to prepare the case list the American Board of Obstetrics and Gynecology (ABOG) requires for certification. This page describes what it does and does not do with patient information.

WHAT IT IS USED FOR

- **Continuity of care:** the physician's own record of the patients they have seen. Treatment, 45 CFR 164.501
- **ABOG case lists:** cases sorted into ABOG's categories. The list submitted to ABOG carries no identifiers except age.
Health care operations: certification
- **ABOG audits:** ABOG requires candidates to keep their own record of who each patient is. The physician's encrypted vault is that record.

HOW PATIENT INFORMATION IS PROTECTED

Encrypted vault

Notes, and the map from placeholders back to real identifiers, are encrypted in the physician's browser (AES-256-GCM) with a key only the physician can unlock: a passkey such as Face ID, or a 12-word recovery code. PDI Med stores the encrypted vault and cannot decrypt the vault's contents.

Outside the vault

Our servers hold account details and de-identified case-log data (diagnoses, procedures, lab names and values) with dates of service. We treat this as PHI: encrypted at rest with AWS keys and separated by physician.

THE AGREEMENT

PDI Med signs a HIPAA Business Associate Agreement with the physician containing the 45 CFR 164.504(e) terms: permitted uses only, Security Rule safeguards, breach reporting within 60 days, AWS bound to the same terms, and return or destruction of PHI when the agreement ends. It is available on request, with our full security description.

No printing needed. Type into the fields below (a typed signature is fine) and email this PDF back, or approve by replying "Approved" to the physician's email from your work address.

PHYSICIAN

I will use PDI Med as described on this page, only for my own patients' care and my board certification case list. I will review every de-identified note before it is sent and keep my devices and recovery code secure.

NAME _____ SIGNATURE _____ DATE _____

WHAT IT IS NOT

- Not an EHR or a medical device; makes no clinical decisions.
- No connection to your EHR or network: no integration, API access or credentials. The physician pastes note text into their own browser.
- No employer, payer or insurer views, and no ranking of physicians. Data is never sold or used to train AI models.
- No data sharing. PDI Med's physician-only intelligence network is switched off, and nothing is contributed from any account. Before it is switched on, we will send you a new letter describing it.

De-identified before AI

The browser replaces identifiers with placeholders, the physician reviews the result, and our servers block recognizable identifiers before the text reaches Claude on Amazon Bedrock, in our own AWS account in US regions, under our BAA with AWS. Prompt logging is off; nothing is sent to Anthropic.

Access and audit

Invitation-only accounts, a required authenticator app (MFA), Argon2id password hashing, TLS 1.2+, a 60-minute idle lock and a 24-hour session limit. Security logs are kept indefinitely; a tamper-evident audit ledger is published to a public transparency log every six hours.

WHAT WE DON'T CLAIM

No automated de-identification is perfect: an identifier both the software and the physician miss can reach our servers and the model, which is why the physician reviews every note. That exposure stays inside our own AWS account, under our Business Associate Agreement with AWS: note text reaches our servers only to be checked and sent, de-identified, to the model, and is not stored in readable form.

PRIVACY OR SECURITY OFFICER

- ☐ Approved: the physician named here may use PDI Med as described. The Business Associate Agreement PDI Med signs with the physician is accepted as the assurance for our patient information the physician enters.

NAME _____ TITLE _____

ORGANIZATION _____ SIGNATURE _____ DATE _____