TOTALLY PRIVATE AI

AI for Enterprise Healthcare

Private AI infrastructure for hospital systems, health networks, & healthtech organisations.

Your clinicians are already using AI. The question is whether patient data is still protected.

> *Presented in partnership with* **[Partner Name]** | *[Partner logo]*
> *Remove this box for direct TPAI distribution.*

A TRAP WITH NO EASY EXIT

If you are responsible for data protection in a European healthcare organisation, the pressure is coming from both directions.

Enable public AI tools, and patient data immediately starts moving through infrastructure you did not procure, cannot audit, and have no contractual right to inspect. **The productivity gain is real. So is the Article 9 exposure.**

What if you refuse? The same thing happens without your knowledge. Clinicians paste discharge summaries into ChatGPT at 11pm. Nurses photograph patient notes with their phones. Registrars use consumer AI to draft referral letters. **You have not prevented AI adoption. You have lost any chance of governing it.**

> **The DPO asks why patient data touched a US AI vendor's server. The board asks why clinical staff are burning out when AI could help. Both questions land on your desk.**
> *There is no version of this where "block everything" ends well. The question is whether AI adoption happens under your governance, or outside it.*

In either case, patient data is leaving your governed environment: either with your approval, or without it.

The stakes are unusually high. Patient health data is special category data under GDPR Article 9, the highest protection tier, carrying penalties of up to 4% of global annual turnover. The EU AI Act classifies clinical decision support as high-risk AI, subject to conformity requirements before deployment. NIS2 brings healthcare into critical infrastructure obligations. **A single avoidable breach does not just generate a fine. It ends careers and destroys patient trust built over decades.** [1]

Shadow AI in a clinical environment is not a policy problem. It is a tooling vacuum.

THE THIRD PATH

You don't need to choose between productivity and protection.
You need a boundary.
You need governance.
You need evidence.

Totally Private AI (TPAI) Enterprise is not a safer way to use public AI. **It is a different architecture entirely.** TPAI Enterprise is a private AI platform deployed directly into your own AWS account. Your infrastructure, your keys, your data.

Public AI is productivity without protection. An internal build is protection without speed. **TPAI is productivity with protection, at speed.**

Your TPAI environment is your AWS account and VPC boundary, deployed and governed entirely by your team. Not a vendor's cloud. Not a shared tenant. **Your environment, your encryption keys, your access controls.**

Every clinical note. Every patient record. Every query. Encrypted at the application layer, per user, using AWS KMS with customer-managed keys. TPAI operators have no routine access to your content. There is no public internet egress path. Patient data does not leave your environment. Other vendors handle patient data carefully. **TPAI does not handle it at all.** We deploy the infrastructure. You own everything that runs on it.

Build vs. Buy

A comparable internal build takes 18 to 36 months and typically exceeds €1.5M, with ongoing engineering cost to maintain and secure it. **A TPAI proof of concept is live in 1 to 2 weeks. Full enterprise deployment in under 30 days.**

The Cost of Waiting

If a 500-bed hospital deploys AI documentation support across 300 clinical staff, and each saves 45 minutes of paperwork per shift, the productivity gain runs to **thousands of clinical hours per week.** That is time returned to patients. Every month of delay is that value foregone, while clinician burnout continues and competitors move ahead.

Your patients did not consent to their health data becoming a vendor record. With TPAI, that record is never created outside your boundary in the first place.

The safest disclosure response is the one you never have to make.

Your Data. Your AI. Totally Private.

HIGH-VALUE CLINICAL WORKFLOWS

Capability	What your teams can do
Clinical Documentation	Turn rough consultation notes into structured discharge summaries, progress notes, and referral letters, inside your environment, with patient data never leaving
Care Coordination	Summarise complex cases for multidisciplinary team handoffs, care plan drafts, and specialist referrals with full clinical context intact
Compliance and Audit	Map clinical procedures against regulatory requirements, prepare for accreditation reviews, and produce audit documentation with a complete internal trail
Patient Communications	Generate personalised patient education materials, medication guides, and aftercare instructions in plain language and multiple languages

Clinical Research Support	Review literature, explore treatment protocols, and synthesise evidence, with your proprietary research and patient cohort data kept private

Every workflow runs inside your environment. Patient data never touches a third-party server.

WHY NOT THE ALTERNATIVES

Approach	The limitation
Public AI (OpenAI, Anthropic)	Patient data processed on US vendor infrastructure. Special category data under GDPR Article 9. Subject to US legal process.
Consumer health AI tools	Designed for patients, not for clinical governance. No data residency controls, no audit trail, no GDPR Article 9 compliance posture.
Internal cloud build	Full control. Also: 18 to 36 months, €1.5M+, specialist clinical AI expertise required, and ongoing maintenance burden.
TPAI Enterprise	Deployed in your AWS account, your EU region. Patient data never leaves your environment. TPAI holds nothing. Operational in weeks.

The choice is not between AI and patient safety. It is between architectures.

SECURITY ARCHITECTURE

Control	What it means for you
Network Isolation	No public internet egress. No outbound path means no exfiltration path and no channel for patient data to leave your environment.
Per-User Encryption	Application-layer encryption per user via AWS KMS with customer-managed keys. TPAI has no decryption access.
Operator Access	No routine TPAI access to your content. Any support engagement requires your explicit authorisation and is fully logged.
Data Residency	Deploy in any EU AWS region. Patient data stays in the jurisdiction you choose, meeting GDPR data localisation requirements.
Model Training	Patient data is not used to train base models under the AWS Bedrock deployment model and service terms. [2]
Compliance Alignment	Architecture mapped to GDPR Article 9, NIS2, and ISO 27001 controls. EU AI Act high-risk alignment in progress. Evidence pack available under NDA.

Model training: patient data is not used to train base models. See Note 2 below.

Designed to satisfy DPIA scrutiny and procurement diligence without creating a new external data custodian.

Notes

[1] GDPR Article 9 designates health data as special category data requiring explicit legal basis for processing. Penalties under Article 83(5) reach €20M or 4% of global annual turnover, whichever is higher. EU AI Act Annex III classifies AI systems used in clinical decision support as high-risk. NIS2 Directive (EU) 2022/2555 includes healthcare in critical infrastructure obligations from October 2024.

[2] AWS Service Terms, Section 50.10 (Amazon Bedrock): "Amazon Bedrock does not use your prompts and completions to train the base models." See: aws.amazon.com/service-terms

HOW WE WORK TOGETHER

Designed for security and compliance leaders who need to enable AI productivity without creating new GDPR Article 9 exposure.

Proof of Concept: A dedicated TPAI-hosted proof of concept. 20 to 30 users, 6 weeks, real clinical workflows. You evaluate the platform before any broader commitment. Evidence pack covering GDPR Article 9, NIS2, and ISO 27001 controls is available before you commit.

Enterprise Deployment: 100 to 500+ seats deployed into your AWS account in your chosen EU region, with full onboarding, training, and ongoing maintenance. Your clinical teams use the AI. We run the infrastructure.

Built by security architects with 25+ years of enterprise experience across regulated industries. Technical deployment is typically 4 to 6 weeks, subject to your security review and procurement timeline.

Next Step: 30 Minutes

See the architecture. Review the security controls. Understand exactly what you are deploying and what patient data never touches.

If you are evaluating AI for clinical workflows, start with a 6-week proof of concept in a dedicated private environment.

Book: calendly.com/rcastillo-totally-private

Email: rcastillo@totallyprivate.ai

Your Data. Your AI. Totally Private.