

Your clinicians are already using ChatGPT. Patient confidentiality doesn't survive the paste.

Sovara Browser checks every message and file against your organisation's policy — **locally, before it's sent** — across ChatGPT, Claude, Gemini, Copilot and Perplexity. Patient text never leaves the machine to be checked, and every decision lands in one audit trail.

1 in 4¹

UK GPs report using generative AI in clinical practice — a third of them for writing up patient documentation.

72%²

of US physicians now use AI in clinical practice, up from 48% a year earlier — the trend is one-way.

~40%³

of files uploaded to generative AI tools contain PII or payment-card data — and 82% of pastes come from unmanaged personal accounts.

\$7.4m⁴

average cost of a healthcare data breach — the most expensive of any industry, 15 years running.

THE REGULATORY POSITION

Health data is **special-category data** under UK GDPR. Pasting patient details into a public AI tool is a disclosure — engaging the Data Protection Act 2018 **and** the common law duty of confidentiality. NHS guidance on AI tools requires explicit patient consent, human verification, and no surprises for the patient in how their data is used.⁵

Three verdicts, shown at the moment of send

- Block** A hard stop. The message is held in the composer and never sent.
- Warn** A nudge to reconsider. The clinician can justify and proceed — both are recorded.
- Redact** Identifiers are masked with labelled placeholders before the message can be sent.

The Health preset, ready on day one

- NHS numbers**, medical record numbers (MRN), and patient ID patterns.
- Dates of birth** — a common re-identification vector — caught alongside names in your custom lists.
- Email and phone numbers redacted**, not just warned — the message goes through, the identifier doesn't.
- 24/7 access** — clinical work doesn't keep office hours — with sensible daily and monthly quotas.
- The full secrets suite** — card numbers (Luhn-checked), NI numbers, API keys, private keys.

PRIVACY-FIRST

Evaluated locally

The policy runs inside the browser. Patient text is never transmitted for a check — only audit metadata syncs.

UNIFIED AUDIT

Defensible record

Every decision becomes an integrity-chained audit event — evidence for information-governance reviews and incident investigations.

FILES TOO

Uploads governed

File attachments and drag-and-drop are checked by extension and size before they reach the chat.

DEPLOYMENT

Managed rollout

Deploy via Intune, Group Policy, or Google Admin. Staff can't override organisation configuration.

Covers the sites your people actually use

ChatGPT Claude Gemini Copilot Perplexity

All five verified blocking in a real browser. Site redesigns are fixed centrally by publishing new selectors — no extension update, no gap in coverage.

Plans

FREE

£0

/ single seat

TEAM

£7

/ user / mo,
annual

ENTERPRISE

£15+

/ user / mo

**Sovara — one policy for humans and AI agents,
one audit trail.**

Built by Weldon Web Ltd, UK · weldonweb.co.uk/sovara ·
Hosted in Azure UK South

1. UK GP online survey, Jan 2025 (BMJ Health & Care Informatics / PMC) · 2. American Medical Association physician survey 2026 · 3. LayerX Enterprise AI & SaaS Data Security Report 2025 · 4. IBM Cost of a Data Breach Report 2025 · 5. UK GDPR / DPA 2018; common law duty of confidentiality; NHS England guidance on AI tools (2025).