UK WEB MARKETING · RESOURCE LIBRARY

Healthcare website checklist — DSPT-aware site for 2026

This is the 22-point checklist I run when onboarding an independent UK clinic. It assumes you are a Category 3 organisation under the NHS Data Security and Protection Toolkit (DSPT) — i.e. a non-NHS provider holding patient personal data. The DSPT was rebuilt around the National Data Guardian's ten standards, with a Category 3 strand published by NHS England for sole traders and small private providers.

A GUIDE FOR UK OPERATORS

Author
Jordan Gilbert, CTO · UK Web Marketing

Edition
v1.0 · June 2026

Audience

Independent UK clinics — dental, vet, podiatry, physio, optometry, chiropractic.

TABLE OF CONTENTS

01 The 22-point checklist — at a glance

#	ITEM	LIVES UNDER
1	DSPT Category 3 self-assessment current within 12 months	DSPT
2	Caldicott Guardian named on the website (or stated as not required)	DSPT
3	Information Asset Register includes the website + form vendors	DSPT
4	All staff with site access have done annual data-security training	DSPT
5	Documented breach-notification path to the ICO (72 hours)	DSPT
6	Privacy notice meets ICO clinic-specific guidance	Caldicott
7	"Need to know" justified for any patient identifier the site touches	Caldicott
8	No patient names, photos, or testimonials without explicit written consent	Caldicott
9	Hosting infrastructure provably in the UK or EU/EEA	Hosting
10	CDN edge nodes do not relay through US/non-adequate jurisdictions	Hosting
11	Backups encrypted at rest, restorable, geographic location stated	Hosting
12	Named human operator with root access, accountable in writing	Hosting
13	Every third party that touches data is listed publicly	Sub-processors
14	Each sub-processor's jurisdiction is stated	Sub-processors
15	DPA in place with every sub-processor (Article 28)	Sub-processors
16	The site declares when sub-processors change	Sub-processors
17	Cookie banner blocks non-essential cookies until consent	PECR
18	Analytics is cookieless OR consent-gated	PECR
19	Marketing pixels (Meta, TikTok, LinkedIn) are gated or removed	PECR
20	Embedded video uses a no-tracking mode	PECR
21	Fonts are self-hosted (no Google Fonts CDN)	PECR + GDPR
22	The privacy notice explains every cookie set, by name	PECR

02 DSPT alignment — 5 points

The Data Security and Protection Toolkit is the baseline for any UK provider that processes patient data. Independent clinics are Category 3 — a lighter assessment than NHS organisations, but still enforced.

2.1 Category 3 self-assessment current within 12 months

The DSPT is annual. If your last submission was July 2024, you are out of standards by July 2025 — regardless of whether your contract requires it. Find your status at **dsptoolkit.nhs.uk** by logging in with your ODS code.

2.2 Caldicott Guardian — named or formally not required

The Caldicott Guardian role is mandatory for NHS organisations and strongly recommended for any private provider holding patient-identifiable information. If your practice has one, name them in the privacy notice. If your practice has formally decided one is not required (sole-trader dental, for example), state that decision and who made it.

2.3 Information Asset Register lists the website

The DSPT requires you to maintain an Information Asset Register. The website is an information asset. So are the form vendor (Typeform, Jotform, Cognito, etc.), the email host, the booking system, and the CRM. If your IAR has "the website" as a single line, it is incomplete.

2.4 Annual data-security training

Every staff member with login access to the website, the form vendor, the CRM, or the booking system must have completed annual data-security training. The free e-Learning for Healthcare module "Data Security Awareness Level 1" satisfies this.

2.5 Documented breach-notification path

You have 72 hours to report a notifiable breach to the ICO. If your team does not know who to call, what to say, and what evidence to collect — you do not have a breach plan, you have a hope. Write it down. One sheet. Where the form vendor lives, where the host lives, where the email lives, and who the named operator at each is.

03 Caldicott posture — 3 points

The Caldicott Principles are eight national-data-guardian standards governing how patient-identifiable information moves. The site touches three of them daily.

3.1 Privacy notice meets ICO clinic-specific guidance

The ICO publishes specific guidance for healthcare providers. The privacy notice must explain:

- what data the site collects (forms, cookies, IP logs)
- the legal basis (consent for marketing, vital interest or contract for booking, public task for some NHS-adjacent work)
- how long the data is kept
- who else sees it (every sub-processor)
- how the patient exercises their rights (subject access, rectification, erasure, restriction)
- the ICO's address as the supervisory authority

3.2 "Need to know" justified for every identifier

Caldicott Principle 4 — access on a strict need-to-know basis. If the website knows the patient's date of birth, the contact form must justify it. "We need it to confirm identity at booking" is a justification. "We collect it because the form template had a field" is not.

3.3 No patient names, photos, or testimonials without explicit written consent

A signed model release for the photo. A documented consent file for the testimonial. The consent must be specific (this website, this photo, this paragraph) and revocable. Generic "I consent to marketing use" forms do not survive an ICO complaint.

---

04 EU-sovereign hosting — 4 points

After Schrems II (CJEU, July 2020), transfers of personal data to the United States require additional safeguards. The simplest safeguard is to not transfer at all. Choose hosting that keeps data in the UK or EU/EEA.

4.1 Hosting infrastructure provably in the UK or EU/EEA

"Provably" means there is documentation. AWS Frankfurt is EU. AWS US-East-1 is not. Hetzner is EU. DigitalOcean Frankfurt is EU but the parent is US — read the DPA for onward transfers. The hosting page on the vendor's site is not proof; the DPA is.

4.2 CDN edge nodes do not relay through non-adequate jurisdictions

A CDN (Cloudflare, Fastly, BunnyCDN) places copies of your site at edge nodes around the world. Some of those nodes are in non-adequate jurisdictions. For a UK clinic site, restrict the CDN to UK + EU pops, or use an EU-headquartered CDN (BunnyCDN is Slovenian). The default global setup leaks visitor IPs through the US.

4.3 Backups encrypted, restorable, located

Three questions: where are the backups, how often are they tested, are they encrypted at rest. If the host cannot answer all three in writing, the backup is theatre.

4.4 Named human operator with root access

There is a person whose name is on a contract who can recover your site if it falls over at 2am. If the answer to "who is your hosting operator" is "I think it was the developer who set it up four years ago", you do not have hosting. You have a hostage situation.

---

05 Sub-processor disclosure — 4 points

Article 28 of the UK GDPR requires every data processor to be governed by a written contract. Article 30 requires you to keep a record. Your patients have a right to know who sees their data.

5.1 Every third party that touches data is listed publicly

A sub-processor list lives on the site — usually at `/sub-processors` or as an appendix to the privacy notice. It lists every vendor: hosting, email, form, CRM, analytics, booking, payment.

5.2 Jurisdiction stated for each

Vendor name, what they do, where they store the data, what data they see. Three columns, one per row.

5.3 DPA in place — Article 28

For each sub-processor, you have signed (or accepted via click-through) a Data Processing Agreement. The DPA is filed where someone other than you can find it.

5.4 The site declares when sub-processors change

When you change the form vendor or the email host, the sub-processor page is updated and patients on a marketing list are informed (if the change materially alters where their data sleeps). This is good practice — and a defensible position if the ICO asks.

---

06 Consent + cookie law under PECR — 6 points

PECR (Privacy and Electronic Communications Regulations 2003) governs cookies and electronic marketing in the UK. The ICO has prosecuted clinics specifically for cookie-banner failures.

6.1 Cookie banner blocks non-essential cookies until consent

"Implied consent" stopped being valid in 2019. Non-essential cookies (analytics, marketing, embedded media) must not load until the patient clicks accept. A banner that says "by using this site you accept cookies" is not compliant — and the ICO knows it.

6.2 Analytics is cookieless OR consent-gated

Google Analytics 4 sets cookies. It also relays data to Google in the US. For UK clinic sites I default to **Plausible Analytics** (EU-hosted, cookieless, no PII) or **Fathom** (Canada/EU, cookieless). Both are legal without a banner.

6.3 Marketing pixels (Meta, TikTok, LinkedIn) gated or removed

The Meta Pixel sends a stream of behavioural data to Facebook. On a clinic site this routinely includes the URL of a page about a sensitive condition. It is a Schrems II transfer of special-category data. Remove unless you have a robust legal basis — and even then, gate behind consent.

6.4 Embedded video uses a no-tracking mode

YouTube `youtube-nocookie.com` is the no-track embed. Vimeo's privacy-friendly mode is opt-in in the embed settings. Default embeds set tracking cookies on page load.

6.5 Fonts are self-hosted

Google Fonts served from the Google CDN leaks the visitor IP to Google. The German courts ruled this a GDPR violation in January 2022 (LG München I, 3 O 17493/20). Download the font, host it on your own server, point the CSS at the local file.

6.6 Every cookie is explained, by name

The privacy notice has a table: cookie name, what it does, who sets it, how long it lasts, whether it is essential. If the table has gaps, the privacy notice is incomplete.

---

07 Named EU-sovereign alternatives — by category

CATEGORY	REPLACE THIS	WITH THIS	WHY
Hosting	AWS US, DigitalOcean US, Vercel default	**Hetzner (Falkenstein/Helsinki), AWS Frankfurt, Scaleway (Paris)**	EU-sovereign, German/French operator, mature DPAs
CDN	Cloudflare global, Fastly default	**BunnyCDN (Slovenia, EU-only mode), Fastly EU-only POPs**	Edge stays in EU; documented in DPA
Email	Gmail, M365 default tenancies	**Fastmail UK, Mailbox.org (DE), Tutanota (DE)**	Sovereign mail, no US tenancy
Forms	Typeform, Jotform	**Formbricks (open source, self-host), Fillout (EU-hosted plan), Tally (EU)**	Form data stays in EU/UK
Analytics	Google Analytics 4	**Plausible (Hetzner DE), Fathom (CA/EU), Matomo (self-host)**	Cookieless, no transfer
CRM	Salesforce, HubSpot US	**Pipedrive (EU), Capsule CRM (UK), Salesforce Hyperforce UK**	EU/UK data residency
Booking	Calendly, Acuity	**Cal.com (EU host), Setmore (EU plan), TidyCal (consent-gated)**	Sovereign or gated
Payment	Stripe default	**Stripe (with UK + EU data residency add-on), GoCardless UK**	Data residency add-on signed
Live chat	Intercom, Drift	**Crisp (FR), HelpCrunch (EU plan), Chatwoot (self-host)**	EU-sovereign chat
Newsletter	Mailchimp, ConvertKit	**MailerLite (LT), Brevo (FR), Buttondown (Postmark EU)**	EU sender infrastructure

08 What I do NOT do — the anti-checklist

A few opinionated negatives. These are not legal requirements — they are positions I take when I'm the operator.

- **I do not run Meta Pixel on clinic sites.** The legal basis is fragile and the data is special-category. If marketing wants Meta, they get a separate landing-page subdomain with explicit consent before the pixel loads.

- **I do not embed Google Maps without consent.** The Google Maps embed sets cookies on load and pings the US. For clinic sites I use a static map image with a "View on Google Maps" link, or an OpenStreetMap embed via Leaflet.
- **I do not use Cloudflare's default automatic mode for clinics.** Cloudflare is fine — but the default routes traffic through the nearest POP, which can be US. I set the dedicated EU-only routing where available, or use BunnyCDN.
- **I do not let a third-party developer hold the registrar account.** The clinic owns the domain at the registrar level. Always. (There is a separate guide for this — *5 questions before letting an agency host your domain*.)

---

09 Sources + further reading

- NHS Digital — Data Security and Protection Toolkit · `dsptoolkit.nhs.uk`
- National Data Guardian — Caldicott Principles (2020 review) · `gov.uk/government/publications/the-caldicott-principles`
- ICO — Guide to the UK GDPR · `ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/`
- ICO — Healthcare sector guidance · `ico.org.uk/for-organisations/sector-specific-guidance/health/`
- ICO — Cookie guidance · `ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/cookies-and-similar-technologies/`
- CJEU C-311/18 — Schrems II judgment · `curia.europa.eu`
- LG München I, 3 O 17493/20 — Google Fonts ruling, January 2022
- e-Learning for Healthcare — Data Security Awareness Level 1 · `elearning.hee.nhs.uk/programme/data-security-awareness/`

A note on the long-form version

This is the v1.0 edition. The long-form version (planned for late 2026) will include worked examples — a real clinic's IAR, a real DPA file structure, the cookie-table CSV I use during onboarding. If you want to be told when it ships, message me — same email, same person.