HIPAA MARKETING COMPLIANCE · CHECKLIST

Patient Stories, Photos & Testimonials

The 11 controls OCR expects before patient content goes public · Prepared by Secure Nomad | securenomad.ai

Ten minutes, honest answers. If any box stays unchecked, that's your to-do list — it's the same list OCR would hand you, minus the fine.

1 The compliance gate — who approves what goes public

- ☐ One named person signs off on every post, page, and testimonial before it goes live — and they know PHI rules.
  "The marketing person handles it" is not a control.
- ☐ You keep a log of what was approved, by whom, and when.
  If you can't show it, it didn't happen.
- ☐ Your website and social accounts have been audited in the last 12 months for patient names, faces, conditions, or "success stories."
  All of it counts as PHI — even if the patient loved the post.

2 Training — the real kind, not the checkbox kind

- ☐ Everyone who touches your website, social media, or marketing — including your outside agency or the front-desk person who posts to Facebook — has HIPAA training that specifically covers public-facing content.
- ☐ That training happened in the last year and you have the records.
  A generic annual module that never mentions marketing doesn't cover this.

3 Written §164.508 marketing authorizations — one form per patient, per use

- ☐ Every patient story, photo, review response, or testimonial has its own signed HIPAA marketing authorization.
  A photo release is not a HIPAA authorization. Verbal consent is worth exactly nothing here.
- ☐ The form says what will be shared, where, and that the patient can revoke it — and you know where the signed copies live.
- ☐ When a patient revokes, you have a process to pull the content down.
  Fast.

4 Policy and damage control — when something already went out

- [ ] You have a written social media policy that says who can post, from which accounts, and what never goes public.
  Staff have actually read it.
- [ ] You know your takedown drill: if PHI went out without authorization, who pulls it, who documents it, and who runs the breach risk assessment under §164.402.
  Deleting the post is step one, not the whole response.
- [ ] If content already went out wrong, you've assessed it — not just quietly removed it and hoped.
  Hope is not a safeguard.

Want a second set of eyes on any of these? That's literally my job — just reply here.

— Ricky Martin, Secure Nomad