ClevrMarketing

1. HIPAA & PHI Protection

- [ ] Remove or anonymize all Protected Health Information (PHI) from marketing materials.
- [ ] Obtain written patient authorization (HIPAA-compliant) for any testimonial, photo, or video.
- [ ] Store web-form submissions and chat transcripts in a HIPAA-compliant CRM/EHR.
- [ ] Sign Business Associate Agreements (BAAs) with every vendor touching PHI (email, chat, call tracking, telehealth, etc.).
- [ ] Use encrypted transmission (HTTPS, TLS email) for all patient data.

2. FTC Truth-in-Advertising & Testimonials

- [ ] Ensure all claims are truthful, substantiated, and not misleading ("Typical results may vary").
- [ ] Disclose any compensation or incentives for reviews or influencer endorsements (#ad, #sponsored).
- [ ] Publish average success rates only if sourced from peer-reviewed data and footnoted.
- [ ] Never remove negative reviews; respond professionally without revealing PHI.

3. FDA & State Board Guidelines

(If marketing prescription drugs, devices, or certain therapies)

- Include fair-balance risk information when promoting FDA-regulated products.
- Verify that all "off-label" references are strictly educational, not promotional.
- Check state medical board rules on physician advertising (e.g., no "best doctor" superlatives without recognized awards).

4. CAN-SPAM, CASL & Email/SMS Rules

- [ ] Use accurate "From" name and subject lines—no clickbait.
- [ ] Include a physical mailing address in every email.
- [ ] Provide clear unsubscribe links; honor opt-outs within 10 business days.
- [ ] Acquire express written consent for any automated SMS or voice outreach (TCPA).
- [ ] Include "Text STOP to opt out" in every SMS campaign.

5. ADA & Website Accessibility

- [ ] Ensure website meets WCAG 2.1 AA standards (alt text, keyboard navigation, color contrast).
- [ ] Caption all videos and supply transcripts for audio content.
- [ ] Run quarterly audits with tools like WAVE or Axe.

6. Privacy & Data Security (CCPA, GDPR, etc.)

- [ ] Publish an up-to-date privacy policy detailing data usage, retention, and third-party sharing.
- [ ] Provide mechanisms for data access, correction, and deletion requests (California, EU).
- [ ] Encrypt data at rest and in transit; implement two-factor authentication for staff.

7. Social Media & Influencer Content

- [ ] Moderate public comments to remove PHI disclosures.
- [ ] Use “educational” disclaimers on health tips posted to social channels.
- [ ] Archive posts and stories for at least six years for audit purposes.

8. Review & Reputation Management

- [ ] Solicit reviews through automated, non-coercive requests.
- [ ] Avoid offering cash/gifts of > $10 without clear disclosure (FTC).
- [ ] Respond to reviews with empathy; never confirm patient status or details.

9. Asset Approval & Recordkeeping

- [ ] Maintain a version-controlled repository of all ads, emails, landing pages, and approvals for six years.
- [ ] Implement a two-person sign-off (marketing + compliance or medical director) before launch.
- [ ] Schedule quarterly audits covering website, ad platforms, email sequences, and patient forms.

10. Incident Response Plan

- [ ] Document step-by-step actions for a suspected PHI breach (notification timelines, remediation).
- [ ] Train staff annually on breach recognition and reporting.
- [ ] Review cyber-liability insurance coverage and contact list.