

HIPAA-COMPLIANT HEALTHCARE CONTENT AUDIT CHECKLIST

For US & Canadian Doctors & Health Coaches

Your Quick Reference Guide to Compliance & Patient Trust

PART A: HIPAA COMPLIANCE AUDIT ✓

Patient Privacy & Consent

- ☐ I have reviewed all patient-related content for identifiability (name, age + condition = violation)
- ☐ Any patient testimonials/stories have written HIPAA-compliant consent forms signed and filed
- ☐ My consent forms specify WHERE content will be shared (website, LinkedIn, email, etc.)
- ☐ Consent forms are stored securely and retained for 6+ years
- ☐ I use composite case studies (combining features from multiple patients, no single person identifiable)
- ☐ Before/after photos have explicit written consent from the patient
- ☐ Patient reviews/testimonials don't mention specific health conditions
- ☐ I never share patient health information via unencrypted email or social media DMs

Secure Communication

- ☐ I use a secure patient portal for sensitive health information (not email or text)
- ☐ If I use email for patient communication, I use encrypted email services
- ☐ I don't discuss patient cases in social media comments or public channels
- ☐ My team doesn't share patient information via text, Slack, or unencrypted messaging

The HIPAA Compliance Checklist:
Avoid \$50,000 Penalties with This Simple Audit
freeyourhours.com

- ☐ All logins to patient information systems use strong passwords + 2FA
- ☐ I have a written data breach response plan in case of unauthorized access
- ☐ Patient data is encrypted both in transit and at rest

Account Security

- ☐ All social media and website passwords are unique and complex (12+ characters)
- ☐ Two-factor authentication is enabled on all accounts with patient/sensitive data
- ☐ I have a documented list of who has access to which accounts
- ☐ Inactive employees/team members have been removed from account access
- ☐ I monitor account activity regularly for suspicious logins
- ☐ No passwords are written down, stored in email, or shared verbally
- ☐ I log out after each session, especially on shared devices

Website & Data Security

- ☐ My website has SSL encryption (https://, not http://)
- ☐ I have a Privacy Policy posted that explains how patient data is handled
- ☐ Contact forms have a privacy notice explaining data use
- ☐ Patient data submitted through forms is stored securely
- ☐ I have a website backup system in case of data loss
- ☐ Regular security updates are applied to website and plugins
- ☐ I don't collect more patient information than necessary

Prohibited Content

- ☐ I don't make absolute medical claims ("cure," "guaranteed to work")
- ☐ I don't provide personalized medical advice via social media DMs or comments
- ☐ I include disclaimers where appropriate ("consult your healthcare provider")
- ☐ I don't diagnose conditions based on symptoms shared online
- ☐ I don't encourage patients to avoid recommended medical treatment
- ☐ I don't make comparative claims about superiority over other providers
- ☐ I don't share graphic medical images without clinical context

PART B: VISIBILITY & TRUST-BUILDING AUDIT

Professional Presence

- ☐ I have a complete, professional profile on LinkedIn
- ☐ LinkedIn headline clearly states my specialty and geographic service area
- ☐ My LinkedIn "Open to Work" section accurately reflects my services
- ☐ I have a professional website with current information about my practice
- ☐ Website includes my credentials, licenses, and areas of specialization
- ☐ Website has clear CTAs for scheduling or contacting me
- ☐ I claim my practice on Google Business Profile (for local visibility)
- ☐ My Google Business Profile has current hours, phone, address, and reviews enabled

Content Strategy

- ☐ I post educational content at least 2-3 times per week
- ☐ 80% of my content is educational/helpful (not promotional)
- ☐ 20% of my content includes practice information or success stories
- ☐ My posts address common patient concerns and questions
- ☐ I vary content formats (carousel, video, article, infographic)
- ☐ I use visuals (photos, graphics, videos) in most posts
- ☐ Posts include relevant keywords for my specialty
- ☐ I have a documented content calendar for the next 30 days

Engagement & Community

- ☐ I respond to comments and messages within 24 hours
- ☐ I engage with other healthcare professionals' content regularly
- ☐ I've encouraged patient reviews (with reminder to keep them non-medical)
- ☐ I have 3+ professional testimonials/recommendations on LinkedIn or website
- ☐ I share industry news and research relevant to my specialty
- ☐ I participate in relevant online communities or forums (appropriately)
- ☐ My email list (if applicable) has opt-in consent documented
- ☐ I send emails to my list regularly (newsletter, updates, educational content)

Trust Signals

- ☐ My credentials and licenses are clearly displayed on my website
 - ☐ Patient testimonials (with consent) are visible on my website
 - ☐ I have a clear "About Me" section with background and experience
 - ☐ I list my professional affiliations and memberships
 - ☐ I have a professional photo on all platforms (not generic or outdated)
 - ☐ My website includes patient FAQs addressing common concerns
 - ☐ I display any certifications or specialized training prominently
 - ☐ I have a clear privacy policy and data protection statement
-

PART C: QUICK WINS TO IMPLEMENT THIS WEEK

Compliance Priority (Do These First):

- ☐ Audit 5 oldest posts for HIPAA violations and remove/update as needed
- ☐ Check all social media passwords and enable 2FA on every account
- ☐ Create/update your Privacy Policy if you don't have one
- ☐ Document who has access to your accounts and remove anyone inactive
- ☐ Review one patient testimonial for compliance (ensure consent is documented)

Visibility Priority (Do These Second):

- ☐ Update LinkedIn headline to include specialty + geographic area
- ☐ Claim or optimize your Google Business Profile
- ☐ Schedule 4 educational posts for the next 2 weeks in advance
- ☐ Write 1 blog post or LinkedIn article addressing a patient pain point
- ☐ Identify 5 healthcare professionals in your field to follow and engage with
- ☐ Add a clear CTA (schedule appointment, contact form) to your website
- ☐ Request a patient review (remind them to keep it non-medical)

SCORING GUIDE

Count your ✓ marks:

- ☐ 45+ Checks: Excellent! You're HIPAA-compliant and visible. Focus on consistency.
 - ☐ 35-44 Checks: Good foundation! Implement Part C to strengthen both areas.
 - ☐ 25-34 Checks: Significant opportunity! Prioritize compliance first, then visibility.
 - ☐ Below 25: Start with Part A (compliance is non-negotiable). Don't sacrifice privacy for visibility.
-

RED FLAGS (Do These Immediately if You Have Any)

- ☐ ✗ Patient information shared via unencrypted email or DMs
- ☐ ✗ Patient testimonials without documented consent
- ☐ ✗ Website without https:// (not secure)
- ☐ ✗ Weak or shared passwords for accounts with patient data
- ☐ ✗ No Privacy Policy on website
- ☐ ✗ Discussing patient cases in social media comments

If you have any red flags: Consult with a healthcare compliance officer before continuing.

NEXT STEPS

For Compliance Issues:

→ Address immediately. HIPAA violations can result in fines up to \$50,000 per violation.

For Visibility:

→ Implement the Part C quick wins this week.

The HIPAA Compliance Checklist:
Avoid \$50,000 Penalties with This Simple Audit
freeyourhours.com

To Build a Sustainable System:

→ [Book a free 15-minute strategy call](#) to create a HIPAA-compliant content plan that actually works.

Use this checklist monthly to stay compliant and build patient trust.