2026 COMPLIANCE RESOURCE

MedSpa & Wellness Security Checklist

Is your patient data truly protected? Use this checklist to find out.

Aligned with HIPAA Security Rule, FTC Health Breach Notification Rule & 2026 State Privacy Updates

If you run a medspa, aesthetic clinic, wellness studio, or any health-adjacent business, you are collecting Protected Health Information (PHI). That means federal law requires you to safeguard it. Most small practices are unknowingly non-compliant, and a single breach or audit can result in fines ranging from **$100 to $50,000 per violation**.

This checklist walks you through the 7 critical areas of data security your business must address in 2026.

Did you know?	The average cost of a healthcare data breach in 2025 reached $10.9 million, the highest of any industry for the 14th year in a row. (IBM Cost of a Data Breach Report)

SECTION 01

HIPAA Required Safeguards

- [ ] You have completed a formal HIPAA Risk Analysis within the past 12 months.
  Required by 45 CFR §164.308(a)(1). Not optional — this is the foundation of compliance.
- [ ] You have a written HIPAA Privacy Policy on file and staff has signed acknowledgment.
  Covers how PHI is collected, used, and disclosed.
- [ ] You have a written HIPAA Security Policy covering electronic PHI (ePHI).
  Must address administrative, physical, and technical safeguards.
- [ ] You have a designated HIPAA Privacy Officer (even if that's you).
  Requiredunder45CFR§164.530(a).Canbeanowner,manager,orexternal consultant.

- [ ] You have a documented Breach Notification Procedure.
  Intheeventofabreach,youmustnotifyaffectedpatientswithin 60 days.
- [ ] All staff who handle patient data have received HIPAA training in the last 12 months.
  Trainingmustbedocumentedwithdatesandsignatures.

SECTION 02

Business Associate Agreements (BAAs)

A Business Associate Agreement is a legally required contract between your practice and any third-party vendor that handles your patient data. Missing BAAs are one of the most common HIPAA violations found during audits.

- [ ] Your Electronic Health Record (EHR) or booking software provider has a signed BAA on file.
  Examples: Jane App, Aesthetic Record, Zenoti, PatientNow, Vagaro.
- [ ] Your email platform has a signed BAA if you communicate patient information via email.
  StandardGmailorOutlookareNOTHIPAAcompliantwithoutaBAAandencryption.
- [ ] Your payment processor has a signed BAA if payment data is linked to health records.
- [ ] Any cloud storage service (Google Drive, Dropbox, etc.) used for patient files has a BAA.
  You must use the HIPAA-compliant business tier — not a personal account.
- [ ] Your telehealth or virtual consultation platform has a signed BAA.
  FaceTime,Zoom(free),andstandardvideotoolsarenotHIPAAcompliant.
- [ ] You have a current log of all vendors with PHI access and their BAA status.
  This inventory should be reviewed at least annually.

SECTION 03

Device & Network Security

- [ ] All devices that access patient data are password protected and use screen lock.
  iPads, laptops, phones, front desk computers — all of them.
- [ ] Your clinic Wi-Fi network is separate from the guest/client network.
  Never run patient data systems on the same network available to the public.
- [ ] All workstations have up-to-date antivirus and security software installed.
- [ ] Automatic software updates are enabled on all devices used for business.
  Outdatedsoftwareisthe#1entrypointforransomwareattacks
- [ ] Multi-factor authentication (MFA) is enabled on all business email and software accounts.
  MFA blocks over 99% of automated credential attacks.

- [ ] You have a policy for what happens when an employee leaves — accounts are disabled immediately.
  Failuretooffboardstaffaccessisa leadingcauseof internaldatabreaches.
- [ ] No patient records are stored on personal devices without encryption and remote wipe capability.

SECTION 04

Patient Data Collection & Handling

- [ ] Your intake forms — paper or digital — only collect information that is clinically necessary.
  Collecting more data than needed increases your liability exposure.
- [ ] Digital intake forms are collected through a HIPAA-compliant platform.
  StandardGoogleFormsisNOTHIPAAcompliant for patient health data.
- [ ] Before/after photos are stored in a secure, access-controlled system — not in your phone camera roll.
  PhotosareconsideredPHIif linkedtoapatient'sidentity or treatment record.
- [ ] Patient records are retained according to your state's medical records retention law.
  Most states require 7–10 years. Check your specific state requirement.
- [ ] You have a documented process for patients to request, access, or delete their records.
  Required under HIPAA's Patient Rights provisions and 2026 state privacy laws.
- [ ] Physical patient files (if any) are stored in a locked cabinet with restricted key access.

SECTION 05

Website & Marketing Compliance

2026 Update:	The FTC finalized expanded enforcement of the Health Breach Notification Rule. Health apps and wellness platforms that share data with advertisers now face significant penalties.

- [ ] You have removed or audited any Meta Pixel, Google Analytics, or ad tracking tools on pages where patients submit health information.
  TheFTCandHHShavebothissuedwarnings that thesetoolsmayviolate HIPAAwhen used on health-related
- [ ] Your website has a current, accurate Privacy Policy that discloses how visitor and patient data is used.
- [ ] Online booking and contact forms use SSL encryption (your site URL begins with https://).

- [ ] You do not send appointment reminders or treatment details via standard unencrypted SMS without patient consent.
  Use a HIPAA-compliant messaging platform for clinical communications.
- [ ] Email marketing lists (newsletters, promotions) are kept separate from clinical patient records.
  Marketing data and medical data must not be commingled.

SECTION 06

Financial Data & PCI Compliance

- [ ] Your payment processing system is PCI-DSS compliant.
  If you accept credit cards, you are required to meet Payment Card Industry standards.
- [ ] Credit card numbers are never written down, stored in spreadsheets, or saved in email.
  This is both a PCI violation and a significant liability.
- [ ] You use a vetted, secure point-of-sale system — not a personal Venmo or CashApp for business payments.
  Personal payment apps do not carry business-grade fraud protection.
- [ ] Staff are trained to recognize and avoid phishing scams targeting payment data.
  Phishing is the #1 method used to compromise small business financial accounts.
- [ ] You conduct an annual review of who has access to your business financial accounts and software.

SECTION 07

Incident Response & Data Backup

- [ ] You have a written Data Breach Response Plan that outlines exactly what to do if patient data is compromised.
  Without a plan, the panic of a breach makes costly mistakes almost inevitable.
- [ ] Patient data is backed up automatically and stored in an encrypted, off-site or cloud location.
  Ransomware attacks encrypt your local files. Backups are your recovery lifeline.
- [ ] Backups are tested at least quarterly to confirm they can actually be restored.
  An untested backup is not a backup.
- [ ] You know your legal obligation: breaches affecting 500+ patients must be reported to HHS within 60 days.
  Smaller breaches must be logged and reported annually.
- [ ] You have cyber liability insurance that covers a data breach notification and response.
  General business insurance typically does NOT cover cybersecurity incidents.

YOUR RESULTS

What Your Score Means

Score Range	What It Means	Recommended Action
35–40 ✓	Strong Compliance Foundation	Schedule an annual review to stay current with regulation changes.
25–34 ✓	Moderate Risk — Gaps Present	Prioritize Sections with the most unchecked items immediately.
15–24 !	High Risk — Action Required	You are likely non-compliant. Seek a professional HIPAA audit now.
Under 15 !!	Critical Exposure	Your business is at serious risk of fines and breach liability. Act immediately

Not Sure Where to Start?

If this checklist revealed gaps in your practice's security, you're not alone and you don't have to figure it out on your own. I offer a personalized HIPAA Risk Assessment specifically for MedSpas and wellness businesses. You'll receive a clear, written report of your vulnerabilities and a prioritized action plan.. in plain English, no tech overwhelm.

Book your FREE 20-minute discovery call today.

This checklist is for informational purposes and does not constitute legal advice. Regulations referenced include the HIPAA Privacy Rule (45 CFR Part 164), HIPAA Security Rule, FTC Health Breach Notification Rule, and applicable 2026 state consumer privacy laws.

Lindsay Nichole Consulting | LindsayNicholeConsulting@gmail.com