QUICK REFERENCE

Compliance Checklists Quick Reference

The five compliance regimes most small businesses encounter — plus the essentials of each.

Which Rules Apply to You?

Answer yes or no. Every yes points to a specific compliance regime.

- ✓ **Do you accept credit or debit cards?** → You must follow **PCI DSS**
- ✓ **Do you handle medical or health information?** → You must follow **HIPAA**
- ✓ **Do you have significant business with customers in California?** → **CCPA / CPRA** may apply
- ✓ **Do you have customers in Europe?** → **GDPR** likely applies
- ✓ **Are you a public company or material vendor to one?** → **SEC cyber disclosure rules** apply
- ✓ **Have you had a security incident that exposed customer data?** → State breach-notification laws apply

Answered "no" to everything? You still have basic duties to protect customer data — but you are not in a formal compliance regime.

PCI DSS Essentials (for businesses taking cards)

- ✓ **Never write down full card numbers** — not on paper, spreadsheets, emails, or chat
- ✓ **Use a real payment processor** (Square, Stripe, PayPal, bank merchant services) — do not try to store cards yourself
- ✓ **Keep payment terminals secure** — lock them up, watch for tampering
- ✓ **Use strong Wi-Fi** — WPA2/WPA3, change router default password, separate payment network from guest Wi-Fi
- ✓ **Dedicated payment computers** — do not use the same machine for email or web browsing
- ✓ **Annual self-assessment** — your processor sends a questionnaire every year; complete it honestly

Cost for a small merchant: typically $0 to $500 per year.

HIPAA Essentials (for healthcare entities and business associates)

- ✓ Limit access to medical records — only people whose job requires it
- ✓ Keep records locked or password-protected at rest
- ✓ Train employees on HIPAA annually — document the training
- ✓ Written privacy and security policies
- ✓ Business Associate Agreements with every vendor who touches PHI
- ✓ Breach notification plan — 60 days max to notify affected individuals

State Breach Notification Basics

Every U.S. state now has a breach notification law. The timelines and triggers vary, but the common pattern:

- Trigger: unauthorized acquisition of personal information that is not encrypted
- Timeline: typically 30–90 days after discovery (some states as fast as "without unreasonable delay")
- Who to notify: affected individuals, state attorney general (in many states), sometimes credit bureaus
- Safe harbor: if the data was fully encrypted, notification may not be required — but only if the decryption key was not also taken

SEC Cyber Disclosure Rule (Public Companies)

- ✓ **Material incidents:** Form 8-K within 4 business days of determining materiality
- ✓ **Annual disclosures:** describe cybersecurity risk management, strategy, and governance in the 10-K
- ✓ **Board oversight:** disclose which board committee oversees cyber risk and the management expertise assessing it

The "Compliance is the Floor" Principle

Compliance alone will not protect you. These rules are the legal minimum — often written years after the attacks they try to prevent. Real security posture comes from continuous governance: board attention, tabletop exercises, vendor oversight, and a culture that rewards reporting.