The BAA Readiness Checklist

If you're signing BAAs, you should ask yourself one question: "Can we actually stand behind what we're signing?" Implement effective cybersecurity measures, and reduce the chance you'll ever have to make the worst call in healthcare: notifying a customer about a breach.

Before You Sign: The BAA Readiness Checklist

- □ Set PHI boundaries for your organization
  - □ Map where PHI enters your company (product, support, integrations)
  - □ Define where PHI is allowed to live (and where it's not)
  - □ Add guardrails so PHI doesn't drift into the wrong tools
- □ Turn BAA clauses into real security controls
  - □ Review the BAA and highlight anything tied to: safeguards, incidents, reporting, access, subprocessors
  - □ For each requirement, assign:
    - the control you'll use
    - an internal owner
    - the evidence you can produce
- □ Establish a credible minimum security baseline
  - □ Require MFA everywhere (especially admin access)
  - □ Enforce least privilege + remove access quickly when people leave
  - □ Maintain device/endpoint visibility across the team
  - □ Centralize monitoring + alerting so issues don't go unnoticed
  - □ Use operational security policies (not "rubber stamp" docs)
- □ Build an incident readiness plan
  - □ Define what counts as an "incident" internally
  - □ Create an escalation path + response process
  - □ Detect early and contain fast to avoid triggering notification clauses
- □ Put together a BAA-ready response kit
  - □ 1-page security overview
  - □ Incident response + escalation process
  - □ Subprocessors list
  - □ PHI boundary summary
  - □ Evidence you can share quickly (policies, controls, monitoring)

Quick Reality Checks

Are we "HIPAA compliant" if we have policies and a HIPAA certificate?

Not necessarily. HIPAA is underspecified—and BAAs are where customers expect you to have real, operational cybersecurity controls in place (not just paperwork).

Do I need to meet HITRUST requirements?

Not usually. HITRUST exists because HIPAA is underspecified. Start with a credible minimum and mature over time.

Can we negotiate the BAA?

Usually no. Big covered entities won't negotiate—and trying can be a red flag. It shows inexperience at best, and kills trust in your security posture at worst.

Is this about fines?

Fines are abstract. BAAs are where customer trust and breach-notification obligations become real.

How Zip Security helps you sign BAAs with confidence

Zip Security helps healthcare companies stay continually HIPAA compliant by implementing and maintaining the cybersecurity controls BAAs assume you already have—so when a customer sends over a BAA, you can sign it confidently without holding your breath.

Book a demo today to see how.