Swift Billing Solutions

Updated November 2026

HIPAA Compliance Checklist

for Medical Billing Companies

Practices: use this to vet your billing partner. Billing teams: treat every unchecked box as a gap to close. The proposed HIPAA Security Rule overhaul is not final (HHS now targets July 2027), so the current rule is what you are measured against today.

1. Business Associate Agreements

- [ ] Signed BAA with every client before any PHI is shared
- [ ] Subcontractor BAAs: clearinghouse, statement vendor, cloud storage, answering service, collections
- [ ] Breach notification window defined in writing
- [ ] PHI return or destruction terms at contract end
- [ ] Yearly review of all active BAAs

2. Privacy and Security Officers

- [ ] Named Privacy Officer and Security Officer with written duties
- [ ] Clear contact point for client privacy questions and incidents

3. Risk Analysis and Risk Management

- [ ] Documented risk analysis covering every system that holds ePHI
- [ ] Remediation plan with owners and target dates
- [ ] Evidence that fixes were completed
- [ ] Refreshed yearly and after major changes

4. Written Policies and Procedures

- [ ] Minimum necessary rules for each billing role
- [ ] Acceptable use, device, email/fax, remote work and sanctions policies
- [ ] Records kept at least six years
- [ ] Annual review with dated changes

5. Access Controls

- [ ] Unique login for every staff member in every system and portal
- [ ] MFA on PM/EHR, clearinghouse, email and remote access
- [ ] Role-based, least-privilege access
- [ ] Same-day access removal at exit or role change
- [ ] Audit logs reviewed on a schedule

6. Encryption and Secure Transmission

- [ ] Encrypted laptops, workstations, servers and backups
- [ ] Encrypted EDI, email with PHI and file transfers
- [ ] No PHI in personal email, messaging apps or unapproved cloud folders

7. Workforce Training

- [ ] HIPAA training at hire and at least yearly
- [ ] Phishing awareness included
- [ ] Confidentiality agreements and training records kept six years

8. Remote and Offshore Teams

- [ ] Remote work policy: private workspace, no printing, secure network or VDI
- [ ] Same training, access controls and monitoring as on-site staff
- [ ] Team locations disclosed to clients and reflected in the BAA

9. Physical Safeguards

- [ ] Controlled office access
- [ ] Locked storage for paper EOBs and mail
- [ ] Shredding or certified destruction; clean-desk rule

10. Incident Response and Breach Notification

- [ ] Written incident response plan with named roles
- [ ] Four-factor risk assessment documented for every incident
- [ ] Client notified within BAA window, never later than 60 days
- [ ] Incident log kept six years

11. Contingency Planning

- [ ] Tested backups, one copy offline or immutable
- [ ] Disaster recovery plan with realistic recovery times
- [ ] Backup route for claims if the clearinghouse goes down

12. Patient Billing and Collections

- [ ] Identity verified before discussing balances
- [ ] Minimum necessary detail in voicemails, emails and statements
- [ ] Secure patient payment channels
- [ ] Records requests routed to the practice promptly

13. Offboarding and Data Return

- [ ] Client system and portal access revoked on the last day
- [ ] PHI returned or destroyed with written certification
- [ ] Clean handoff of open AR and pending appeals

General information only, not legal advice. Consult a healthcare attorney or compliance professional about your obligations.

swiftbillingsolutions.com | (888) 315 0532 | Info@swiftbillingsolutions.com

Questions to Ask Before You Hire a Billing Company

Vague answers aren't proof of a problem, but they're a reason to keep asking.

Ask this	A good answer sounds like
When was your last security risk analysis?	A specific date in the past year, and a walk-through of what was found and fixed
Will you sign our BAA, or provide yours?	Yes, before any data is shared, with breach notice and data return terms
Which subcontractors will touch our data?	A named list, with a BAA in place for each
Does every biller get their own login?	Always, with MFA and no shared credentials
Where is your team, and how are remote staff secured?	A direct answer on locations, plus specific remote-work controls
How fast will you report a suspected breach?	A number of days written into the BAA, well under 60
How do you train your staff?	At hire and every year, with records they can show you
What happens to our data if we part ways?	Returned or destroyed with certification, access cut on day one

Notes and follow-ups

Want a second set of eyes on your billing?

Swift Billing Solutions offers a free practice revenue audit. Flat 3% of monthly collections, no setup fees, no long-term contracts.
swiftbillingsolutions.com | (888) 315 0532