eBOOK · HIPAA

Business Associate Agreements in 2026: What Changed and What You Must Update

The 2026 HIPAA NPRM introduces new mandatory BAA terms. Is your template still compliant?

18 pages · PDF · Updated May 2026 · **goironfort.com**

What Is a BAA and Why Does It Matter?

A Business Associate Agreement (BAA) is the contract required by HIPAA between a covered entity and any vendor (business associate) that accesses, uses, or discloses protected health information on their behalf. Without a valid BAA, neither party is compliant — and both are exposed to OCR penalties.

New BAA Requirements Under the 2026 NPRM

24-Hour Incident Notification

BAs must notify covered entities within 24 hours of discovering a security incident involving ePHI. This is a significant compression from "without unreasonable delay" (previously interpreted as up to 60 days).

Subcontractor Chain Accountability

BAs must contractually require their subcontractors (sub-BAs) to meet equivalent security standards. The originating BA is accountable for the entire downstream chain.

Termination Rights

CEs must have contractual right to terminate the BAA immediately upon discovering a material violation by the BA — including security control failures and unauthorized disclosures.

Annual Security Review Obligation

BAs must conduct and document an annual security review of their ePHI-handling operations and provide summary results to covered entities upon request.

BAA Compliance Checklist

Review each existing BAA against these requirements:

- Incident notification timeline updated to 24 hours
- Subcontractor accountability clause included
- Termination rights for material violations specified
- Annual security review obligation included
- Data return / destruction obligations on termination
- Permitted uses and disclosures of PHI clearly defined
- Safeguards appropriate to PHI sensitivity level
- Sub-BA agreement requirement included
- Audit rights for covered entity included
- Updated effective date reflecting 2026 NPRM changes

BAA Lifecycle Management with Iron Fort

Iron Fort's BAA module tracks every agreement — creation, execution, renewal dates, and termination. Automated alerts notify you 90/60/30 days before expiry. Subcontractor chain mapping identifies all downstream BAs. Book a demo at **goironfort.com/demo**.