Vendor HIPAA and BAA Readiness Checklist

Questions to answer before a vendor handles protected health information. Pair with your own BAA and legal review.

Vendor	Service	Business owner	Date

DATA

- [ ] We know exactly what PHI the vendor will create, receive, keep or send
- [ ] The vendor only gets the minimum PHI needed for the service
- [ ] We know where the data will be stored and in which countries

AGREEMENT

- [ ] A business associate agreement is signed before any PHI is shared
- [ ] It limits use and disclosure of PHI to the service
- [ ] It requires safeguards and breach reporting with a set time frame
- [ ] It covers subcontractors who touch PHI
- [ ] It covers return or destruction of PHI at the end of the contract

SECURITY

- [ ] Encryption in transit and at rest
- [ ] Access controls and multi-factor sign-in
- [ ] Audit logs we can request
- [ ] Recent security assessment or certification provided (for example SOC 2 or HITRUST)
- [ ] Incident response contact named

Notes and open items

Reviewed by (privacy or compliance)	Approved by	Date

Reference: HHS publishes sample business associate agreement provisions at hhs.gov.

Generic template from Actari (actarihealth.com). Adapt it to your organization's policies, regulations and scope of practice. Not clinical, legal or compliance advice.