

Healthcare Contract Compliance Checklist

25 key terms to review before approval, organized into 7 categories. A first-pass review aid for healthcare legal, contracts, compliance, privacy, and finance teams.

Use this checklist as a first-pass review aid across BAAs, physician arrangements, medical vendor and device agreements, clinical trial agreements, and the healthcare vendor portfolio. Sensitive questions should be routed to qualified counsel and the organization's privacy, security, and compliance functions.

Counterparty and Agreement Type

- ☐ **01** Counterparty legal entity confirmed and matched to onboarding records.
- ☐ **02** Agreement type identified, including BAA applicability, data processing agreement (DPA) applicability, and whether a master services agreement (MSA) governs.
- ☐ **03** Services scope documented and consistent across the BAA, MSA, and any addenda.

PHI and Data

- ☐ **04** Protected health information (PHI) or ePHI access defined, including create, receive, maintain, and transmit categories.
- ☐ **05** Permitted uses and disclosures limited to what the services require.
- ☐ **06** De-identification, data aggregation, and research uses spelled out where applicable.

Security, Breach, and Subcontractors

- ☐ **07** Administrative, physical, and technical safeguards consistent with the HIPAA Security Rule.
- ☐ **08** Breach notice timing, content, root-cause obligations, and cost allocation defined.
- ☐ **09** Subcontractor flow-down terms and approval or notice rights present.
- ☐ **10** Cybersecurity cooperation, including patching, updates, and incident assistance, defined for technology vendors and connected device manufacturers.

Audit, Records, and Return of Data

- ☐ **11** Audit rights, response timelines, scope of records confirmed, including regulatory inspection cooperation where applicable.
- ☐ **12** Recordkeeping and retention periods documented, including audit, compensation, and study records where applicable.
- ☐ **13** Post-termination return or destruction of PHI and confidential data, including certification.

Risk Allocation

- ☐ **14** Indemnification scope reviewed against the organization's preferred positions, including mutual versus one-way structure and subject injury responsibility in clinical trial agreements.
- ☐ **15** Limitation of liability caps and super-cap carve-outs consistent with the organization's risk thresholds.
- ☐ **16** Insurance types, limits, additional-insured, and certificate requirements confirmed.
- ☐ **17** Warranty and warranty disclaimer language reviewed for healthcare vendor and device agreements.

Physician Arrangements and Compensation

- ☐ **18** Physician arrangement type identified (medical director, employment, services, call coverage, consulting).
- ☐ **19** Services scope, duties, time commitments, and time-record obligations clear.
- ☐ **20** Compensation structure documented and routed through the organization's approval workflow, with terms sensitive to fair market value (FMV), Stark Law, and Anti-Kickback Statute flagged for compliance escalation.
- ☐ **21** Volume-based and value-based payment language flagged for compliance escalation.

Term, Operations, and Conflicts

- ☐ **22** Term, renewal, and termination triggers, including cure periods.
- ☐ **23** Service levels and support response for healthcare vendor, device, and SaaS agreements.
- ☐ **24** Conflicts between the BAA, DPA, MSA, security addendum, and vendor click-through terms reconciled, with order-of-precedence confirmed.
- ☐ **25** Escalation triggers documented for legal, privacy, security, compliance, finance, procurement, research administration, and clinical reviewers.

This checklist is review guidance for healthcare contracts teams. It is not legal advice. It is not a determination of HIPAA, Stark Law, Anti-Kickback Statute, FMV, FDA, HHS Office of Inspector General (OIG), Centers for Medicare & Medicaid Services (CMS), audit, or applicable privacy law requirements. Route sensitive privacy, security, regulatory, compensation, and research questions to qualified counsel and the organization's compliance functions.

Ready to turn this checklist into a repeatable, playbook-driven workflow? See [Contract Logix Review](https://contractlogix.com) at contractlogix.com.