Third-Party Vendor Compliance Checklist

2026 Readiness Note: This checklist has been updated for healthcare vendor oversight, HIPAA business associate review, cybersecurity supply chain risk, exclusions screening, data privacy, AI/automation tools, and incident-response expectations. It is not a substitute for legal, privacy, security, payer, or accreditation advice.

Purpose

Use this checklist before engaging, renewing, or expanding work with vendors, contractors, consultants, billing companies, credentialing support, IT vendors, marketing partners, suppliers, staffing agencies, management companies, AI or automation vendors, software platforms, cloud services, and other third parties. The goal is to identify who is acting on your behalf, assess risk before engagement, document due diligence, define expectations in writing, and monitor performance over time.

How to Use This Checklist

- Complete the inventory before signing, renewing, expanding, or materially changing a vendor relationship.
- Assign each third party a risk level based on services, access, location, payment structure, regulatory exposure, technology access, data access, patient impact, and operational importance.
- Scale due diligence to risk. Higher-risk relationships require deeper review, stronger documentation, contractual protections, and ongoing monitoring.
- Determine whether the vendor is a HIPAA business associate, subcontractor business associate, technology service provider, clinical vendor, financial vendor, or general operational vendor.
- Document every decision, red flag, approval, contract requirement, security review, privacy review, and follow-up item in a centralized file.

1. Third-Party Inventory

Done	Checklist item	Notes / owner
[ ]	Create or update a centralized list of all third parties used by the organization.	
[ ]	Record the third party's legal name, DBA name, address, website, primary contact, tax identifier, and support contact information, when applicable.	
[ ]	Identify the type of service provided and the department, location, facility, specialty, or practice area supported.	
[ ]	Record the internal hiring/requesting person and the internal owner responsible for ongoing oversight.	
[ ]	Identify where the contract, certificate of insurance, due diligence file, security review, business associate agreement, and audit records are stored.	
[ ]	Document owners, principals, key personnel, subcontractors, offshore support, parent companies, and related entities, when applicable.	
[ ]	Record where work or service is performed and whether work is onsite, remote, offshore, cloud-based, multi-state, or performed through subcontractors.	
[ ]	Track contract dates, renewal dates, termination rights, insurance expirations, BAA dates, security review dates, license expirations, and review cadence.	

2. HIPAA, Data Access, and Business Associate Classification

Done	Checklist item	Notes / owner
[ ]	Determine whether the third party creates, receives, maintains, transmits, stores, hosts, supports, analyzes, or accesses PHI, ePHI, patient information, images, billing data, claims data, or appointment information.	
[ ]	Determine whether the third party is a HIPAA business associate, a subcontractor business associate, a workforce-equivalent contractor, or a vendor with incidental or no PHI access.	
[ ]	Confirm that a business associate agreement is signed before PHI/ePHI access begins, when required.	
[ ]	Identify data flows, system connections, integrations, API access, remote access, cloud storage, user accounts, file transfers, and support access.	
[ ]	Apply minimum necessary access and document role-based access expectations.	
[ ]	Review whether the vendor uses analytics, website tracking, advertising pixels, patient communication tools, AI tools, call recording, chatbots, transcription, or automation that could collect or transmit health-related data.	
[ ]	Document whether data is stored, processed, backed up, or supported outside the United States or outside the primary service location.	
[ ]	Confirm return, deletion, retention, backup destruction, and transition procedures for PHI/ePHI at termination.	

3. Risk Assessment and Prioritization

Done	Checklist item	Notes / owner
[ ]	Determine whether the third party performs a critical business, clinical, financial, compliance, technology, cybersecurity, safety, or patient-facing function.	
[ ]	Identify whether the third party has access to patient information, employee information, financial data, systems, credentials, facilities, supplies, controlled areas, medical devices, or connected equipment.	
[ ]	Assess whether the third party can bind the organization contractually, financially, clinically, operationally, or through payer or government submissions.	
[ ]	Review whether the service involves government approvals, licensing, payer enrollment, credentialing, accreditation, inspections, certifications, claims submission, or regulatory reporting.	
[ ]	Evaluate whether the third party handles billing, coding, collections, revenue cycle, refunds, claims, payments, banking, purchasing, or controlled expenses.	
[ ]	Assess cybersecurity and operational resilience risk, including network connectivity, remote access, cloud hosting, software dependencies, incident response, backup capability, downtime risk, and business continuity impact.	
[ ]	Classify each third party as low, medium, or high risk, with written rationale for the assigned risk level.	
[ ]	Prioritize high-risk third parties for enhanced due diligence, security review, privacy review, contract protections, and more frequent monitoring.	

4. Due Diligence Before Engagement or Renewal

Done	Checklist item	Notes / owner
[ ]	Confirm the third party has the experience, staffing, resources, qualifications, financial stability, and infrastructure required to perform the work.	
[ ]	Verify licenses, certifications, registrations, professional qualifications, accreditation status, and payer or government enrollment status, when applicable.	
[ ]	Check references, reputation, litigation history, sanctions, exclusions, disciplinary history, privacy/security history, billing integrity history, and publicly available background information when appropriate.	
[ ]	Screen relevant individuals and entities against the OIG List of Excluded Individuals/Entities and other applicable federal or state exclusion/debarment lists based on organizational policy and payer requirements.	
[ ]	Review ownership, conflicts of interest, referral relationships, compensation relationships, financial interests, and relationships with government officials, payer representatives, physicians, employees, or referral sources when relevant.	
[ ]	Request and review policies, attestations, or reports related to compliance, HIPAA, privacy, information security, incident response, anti-retaliation, conflicts of interest, ethical conduct, and subcontractor oversight when appropriate.	
[ ]	Review security documentation appropriate to the risk level, such as security questionnaires, SOC reports, penetration testing summaries, vulnerability management processes, disaster recovery capabilities, MFA, encryption, access controls, and backup practices.	
[ ]	Review insurance coverage, including general liability, professional liability, cyber liability, technology E&O, workers compensation, and other coverage relevant to the service.	
[ ]	Document red flags, escalation decisions, additional review steps, approvals, risk acceptance decisions, and final selection rationale.	

5. Written Due Diligence Process

Done	Checklist item	Notes / owner
[ ]	Maintain a written policy or standard operating procedure for third-party screening, approval, privacy review, security review, monitoring, renewal, escalation, and termination.	
[ ]	Define who is responsible for conducting due diligence, approving vendors, documenting results, managing BAAs, reviewing security risks, and monitoring performance.	
[ ]	Define risk categories and the minimum due diligence required for each category.	
[ ]	Identify red flags that require escalation before approval, renewal, or scope expansion.	
[ ]	Define how existing third parties will be reviewed and brought into the current process.	
[ ]	Document whether desktop review, questionnaires, reference checks, site visits, audits, mock reviews, cybersecurity review, privacy review, or enhanced review are required.	
[ ]	Maintain documentation of all due diligence performed, results reviewed, approvals issued, risk acceptance decisions, contract conditions, and corrective actions.	
[ ]	Establish a renewal and re-review schedule based on risk level, contract terms, data access, system access, incident history, and service criticality.	

6. Contract and Agreement Requirements

Done	Checklist item	Notes / owner
[ ]	Use a written agreement that clearly defines services, scope, deliverables, compensation, payment terms, performance expectations, service levels, and reporting obligations.	
[ ]	Require compliance with applicable organization policies, privacy expectations, security requirements, documentation standards, ethical conduct expectations, payer requirements, and accreditation expectations relevant to the services.	
[ ]	Include audit rights, record-retention expectations, cooperation obligations, documentation access, corrective action obligations, and termination rights for noncompliance or failure to meet contract requirements.	
[ ]	Include a business associate agreement when the vendor is a business associate and require subcontractor BAAs when subcontractors will handle PHI/ePHI.	
[ ]	Require appropriate training or certification of third-party personnel who work on the account, including privacy, security, compliance, safety, billing, or role-specific training when applicable.	
[ ]	Identify how concerns, questions, errors, incidents, data issues, suspected breaches, cybersecurity events, safety events, billing errors, or suspected violations must be reported.	
[ ]	Specify required notice of ownership changes, key personnel changes, subcontractor use, offshore support, location changes, data processing changes, system changes, or material changes affecting risk profile.	
[ ]	Specify acceptable payment methods, payment locations, invoicing detail, expense documentation, and prohibition of cash, off-book payments, unsupported reimbursements, and unusual payment arrangements.	
[ ]	Require approval before the third party uses subcontractors, sub-agents, offshore support, AI tools, new technology platforms, or other additional parties for the organization's work.	
[ ]	Include confidentiality, privacy, data security, minimum necessary, breach notification, incident response, data return/destruction, cyber insurance, anti-retaliation, conflict-of-interest, compliance, and cooperation provisions as appropriate for the relationship.	

7. Ongoing Oversight and Monitoring

Done	Checklist item	Notes / owner
[ ]	Assign an internal owner responsible for each third-party relationship.	
[ ]	Maintain a complete third-party file, including contract, due diligence records, BAA, insurance, licenses, security review, training records, audit notes, corrective actions, and renewal documentation.	
[ ]	Monitor performance according to risk level, service scope, financial exposure, patient impact, cybersecurity risk, data access, system access, and regulatory exposure.	
[ ]	Conduct periodic reviews of contract adherence, service quality, billing accuracy, documentation quality, privacy/security requirements, incident history, complaints, and operational performance.	
[ ]	Maintain an audit schedule for medium- and high-risk third parties.	
[ ]	Track ownership changes, legal concerns, sanctions, exclusions, insurance expirations, licensing changes, complaints, incidents, data events, security issues, and material changes in services.	
[ ]	Document corrective actions, follow-up deadlines, responsible parties, validation steps, and closure evidence.	
[ ]	Review high-risk third parties at least annually and before renewal, expansion, material scope changes, system integrations, or PHI/ePHI access changes.	

8. Cybersecurity, Technology, and AI Vendor Review

Done	Checklist item	Notes / owner
[ ]	Identify whether the vendor provides cloud services, software, EHR/PM integrations, billing systems, scheduling systems, patient communications, analytics, AI tools, remote access, managed IT, backup, hosting, transcription, call recording, or connected-device support.	
[ ]	Document data types accessed, including PHI, ePHI, patient identifiers, financial data, credentials, employee data, operational data, or de-identified/limited data sets.	
[ ]	Confirm access controls, unique user IDs, MFA, role-based access, encryption, logging, monitoring, patching, vulnerability management, backup, disaster recovery, and incident response capabilities appropriate to the relationship.	
[ ]	Review whether the vendor uses customer data for model training, analytics, product improvement, benchmarking, marketing, resale, or third-party sharing, and prohibit or restrict uses that are not approved.	
[ ]	Require prior written approval before introducing AI, automation, subcontractors, offshore support, tracking technologies, pixels, cookies, data brokers, or new integrations that affect patient, employee, or business data.	
[ ]	Confirm security incident notification timelines, cooperation obligations, evidence preservation, corrective action duties, and post-incident reporting expectations.	
[ ]	Assess whether the vendor can support downtime procedures, data export, business continuity, service transition, and emergency operations if the system is unavailable.	

9. Third-Party Red Flag Review

Done	Checklist item	Notes / owner
[ ]	Lack of experience, qualifications, staff, infrastructure, financial stability, or resources to perform the work.	
[ ]	Refusal to provide ownership information, references, compliance attestations, required documents, security information, BAA terms, insurance, or audit access.	
[ ]	Unusually high fees, commissions, success fees, vague invoices, cash requests, off-book payments, unsupported reimbursements, or payment in an unrelated country.	
[ ]	Lack of detail about work to be performed, vague subcontractors, undisclosed offshore support, or unexplained additional parties introduced into the relationship.	
[ ]	Conflicts of interest, undisclosed relationships, family relationships with decision-makers, government officials, referral sources, payer representatives, or employees.	
[ ]	Prior criminal, civil, regulatory, exclusion, disciplinary, fraud, privacy, security, billing, kickback, patient safety, or questionable business practice history.	
[ ]	Use of shell companies, unclear corporate structure, inconsistent business records, or refusal to explain ownership or control.	
[ ]	Pressure to move quickly, bypass controls, avoid documentation, skip BAA review, ignore policy, or complete work without appropriate review.	
[ ]	Poor accounting records, opaque expenses, unsupported reimbursements, refusal to maintain records, or refusal to cooperate with audits.	
[ ]	Material misstatements, incomplete answers, inconsistent representations, hidden subcontractors, false information, or unexplained changes in onboarding materials.	
[ ]	Reluctance to disclose security practices, breach history, system architecture, incident response process, cyber insurance, or data retention/deletion practices.	

10.Final Review and Action Plan

Priority	Gap / risk identified	Responsible party	Target date

Resource Page Intro Copy

Use this checklist to evaluate third-party vendor risk before engaging, renewing, or expanding vendor relationships. It is designed to help healthcare practices, ASCs, and office-based surgical suites identify vendors, assess risk, document due diligence, strengthen contracts, monitor performance, and respond to red flags before they create operational, financial, compliance, cybersecurity, privacy, or reputational exposure.

Website CTA Copy

Need help organizing vendor oversight, documentation, contracts, privacy reviews, security reviews, or compliance workflows? Solstice Group can help evaluate third-party risk, build practical oversight systems, and strengthen operational accountability.

Source Note

This checklist is adapted for healthcare business and compliance use from third-party risk management concepts addressed in the Society of Corporate Compliance and Ethics handout, Third-Party Essentials: A Reputation/Liability Checkup When Using Third Parties Globally, by Marjorie W. Doyle, JD, CCEP-F, with input from Diana Lutz. It has been updated for healthcare vendor oversight using current compliance and risk-management concepts from HHS OCR HIPAA Security Rule guidance, HHS OIG compliance guidance and exclusions resources, HHS healthcare cybersecurity resources, and NIST cybersecurity supply chain risk management guidance.

Disclaimer

This resource is provided for general business and compliance education only. It is not legal, medical, accounting, tax, financial, regulatory, cybersecurity, privacy, or clinical advice. Organizations should consult qualified legal, compliance, privacy, cybersecurity, financial, accreditation, and professional advisors regarding their specific obligations and risk profile.