Compliance Program Readiness Checklist

A practical compliance review tool for healthcare practices, ASCs, and office-based surgical settings

Purpose
Use this checklist to evaluate whether your organization has a practical compliance infrastructure for HIPAA, privacy, cybersecurity, OSHA, infection control, CLIA, credentialing, personnel documentation, audits, corrective actions, and ongoing regulatory readiness.

How to Use This Checklist
Complete the assessment annually, before major operational changes, after leadership changes, and before audits, surveys, or accreditation reviews. Track open items in the action plan and maintain documentation of completion.

1. Compliance Governance and Accountability

☐	Checklist item	Notes / owner
☐	Designate a compliance owner or committee with authority to coordinate compliance activities and report concerns.	
☐	Document responsibilities for OSHA, HIPAA, CLIA, infection control, credentialing, labor documentation, accreditation, privacy, cybersecurity, and corrective actions.	
☐	Maintain a written compliance plan or operating framework tailored to the practice, ASC, or office-based surgical setting.	
☐	Create a compliance calendar with recurring audits, trainings, policy reviews, license renewals, drills, and committee reviews.	
☐	Define reporting pathways for staff questions, concerns, incidents, privacy issues, safety events, and suspected violations.	
☐	Document leadership review of compliance risks, corrective actions, open issues, and closure evidence.	
☐	Confirm compliance activities are practical, assigned, tracked, and reviewed instead of left as static documents.	

2. HIPAA, Privacy, and Cybersecurity Readiness

☐	Checklist item	Notes / owner
☐	Complete and document a HIPAA Security Rule risk analysis covering systems, ePHI, users, vendors, threats, vulnerabilities, and safeguards.	
☐	Review access controls, unique user IDs, MFA where appropriate, password standards, termination procedures, encryption, backups, and device management.	
☐	Confirm business associate agreements are in place for vendors that create, receive, maintain, or transmit PHI on behalf of the organization.	
☐	Review website forms, chat tools, online scheduling, analytics, pixels, AI tools, email systems, texting, and marketing platforms for PHI/privacy exposure.	
☐	Maintain policies for privacy, security, breach response, minimum necessary access, patient rights, workforce sanctions, and incident reporting.	
☐	Conduct HIPAA/privacy/security training and maintain completion records.	
☐	Test breach response workflows, contact lists, documentation templates, and reporting escalation procedures.	

3. OSHA, Infection Control, and Safety

☐	Checklist item	Notes / owner
☐	Maintain OSHA, bloodborne pathogen, hazard communication, sharps safety, PPE, exposure control, and workplace safety documentation.	
☐	Confirm SDS access, labeling, chemical inventory, exposure response, eyewash needs, emergency procedures, and safety signage.	
☐	Document annual OSHA/safety training, infection control training, exposure follow-up, and competency review.	
☐	Review hand hygiene, PPE use, environmental cleaning, sterilization/high-level disinfection, instrument processing, and biological monitoring where applicable.	
☐	Track vaccinations, TB screening, respiratory protection, fit testing, or other employee health requirements when applicable to the setting.	
☐	Maintain logs for injuries, exposures, sterilization, equipment checks, temperature monitoring, emergency drills, and corrective actions.	
☐	Conduct routine safety rounds and document findings, responsible owners, deadlines, and closure evidence.	

4. CLIA, Laboratory, and Clinical Documentation

☐	Checklist item	Notes / owner
☐	Confirm CLIA certificate status, testing menu, waived/non-waived test classification, and certificate renewal dates.	
☐	Maintain laboratory policies, quality control logs, calibration/maintenance logs, proficiency testing when applicable, and personnel competency records.	
☐	Review specimen handling, labeling, result reporting, abnormal result follow-up, and documentation processes.	
☐	Confirm clinical documentation supports services provided, coding, billing, patient communication, consent, and follow-up.	
☐	Monitor documentation gaps, unsigned notes, missing consents, incomplete orders, and inconsistent follow-up workflows.	
☐	Assign responsibility for periodic chart audits and follow-up corrections.	
☐	Document audit results, education provided, corrective actions, and ongoing monitoring.	

5. Credentialing, Licensure, and Personnel Files

☐	Checklist item	Notes / owner
☐	Maintain current licenses, certifications, registrations, DEA/CDS where applicable, malpractice coverage, and expiration tracking.	
☐	Confirm credentialing and privileging processes for providers, anesthesia personnel, surgical staff, and allied health professionals where applicable.	
☐	Review OIG LEIE and other exclusion/sanction checks before hire/engagement and on a recurring schedule.	
☐	Maintain employee and contractor files with required onboarding, training, job descriptions, competency records, acknowledgments, and evaluations.	
☐	Review labor documentation, wage/hour practices, employee classifications, workplace policies, and required postings with qualified advisors as needed.	
☐	Track missing or expired documents and escalate deficiencies before they become survey, payer, or operational risks.	
☐	Document ownership for personnel file maintenance and periodic audits.	

6. Audit, Incident Response, and Corrective Action

☐	Checklist item	Notes / owner
☐	Create an audit schedule based on risk, including privacy, security, OSHA, infection control, documentation, billing, credentialing, vendor, and facility readiness reviews.	
☐	Define incident categories, reporting timeframes, investigation steps, documentation standards, and escalation requirements.	
☐	Use a corrective action log to track findings, root cause, responsible owner, deadline, evidence of completion, and follow-up review.	
☐	Review trends from complaints, incidents, infections, privacy issues, documentation gaps, billing errors, and staff concerns.	
☐	Prepare leadership summaries showing open risks, overdue items, audit results, and corrective action progress.	
☐	Update policies, training, workflow, forms, or technology controls when recurring issues are identified.	
☐	Maintain evidence of closure for all corrective actions and follow-up monitoring.	

Final Review and Action Plan

Priority	Gap / risk identified	Responsible party	Target date

Resource Use Note

This resource is provided for general business and compliance education only. It is not legal, medical, accounting, tax, financial, regulatory, accreditation, or clinical advice. Requirements vary by state, payer, specialty, facility type, accreditation body, and scope of services. Organizations should consult qualified legal, compliance, privacy, financial, clinical, accreditation, and professional advisors regarding their specific obligations and risk profile.