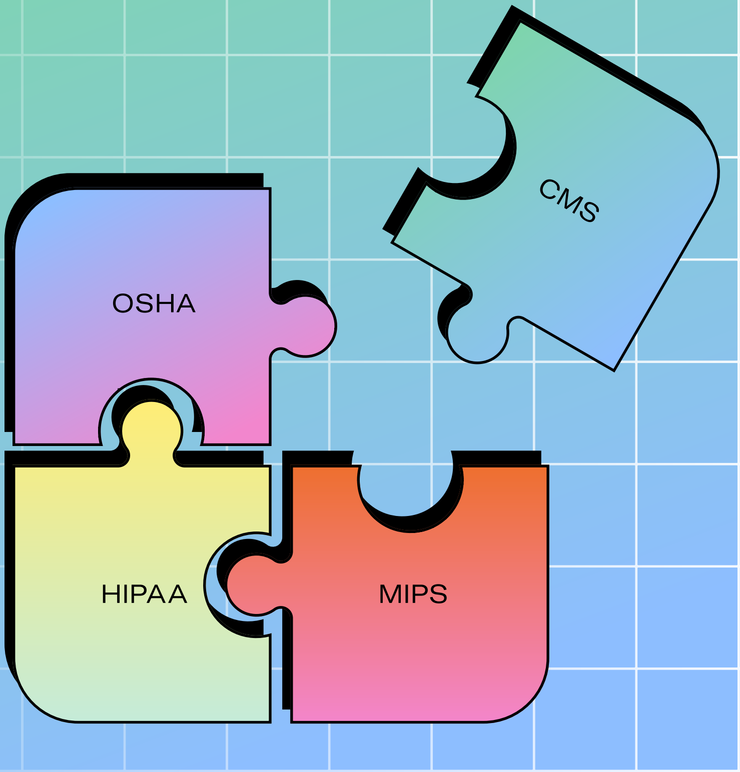
Athelas
Powered by Commure

THE MID-MARKET HEALTHCARE COMPLIANCE TOOLKIT

Navigating Regulatory Challenges with Confidence



Compliance Isn't an Afterthought; It's the Bedrock of Your Practice.

For mid-market medical groups (50—200 providers), staying compliant isn't just about avoiding fines, it's about protecting patient trust, securing reimbursements, and enabling growth.

A single HIPAA violation can cost **$50,000+ per incident.**

A MIPS penalty can wipe out up to **9% of Medicare revenue.**

And CMS audits are becoming **more frequent, detailed, and unforgiving.**

Yet most mid-market practices don't have full-time compliance officers. You're wearing multiple hats—overseeing operations, managing revenue, and now, interpreting complex regulations.

This Mid-Market Healthcare Compliance Toolkit gives you exactly what you need: clear guidance, and technology-backed strategies to simplify HIPAA compliance, navigate CMS regulations, and build a culture of accountability, without overwhelming your team. And don't miss the Athelas HIPAA Audit Checklist and three complete, fillable templates at the end of this white paper to get an idea of where you stand.

SECTION 1: Key Regulations Impacting Mid-Market Practices

Here are the core rules keeping administrators up at night—and what they mean for your organization:

Regulation	What It Covers	Mid-Market Impact
HIPAA	Privacy, security, breach notification	Every patient record, email, and text must be encrypted and tracked
MIPS / MACRA	Quality reporting, cost, improvement activities	Up to ±9% Medicare payment adjustment
CMS Interoperability Rules	Patient access to records, API standards	Must provide data within 48 hours of request
No Surprises Act	Good faith estimates, dispute resolution	Required for all self-pay and out-of-network billing
OSHA & CLIA	Workplace safety, lab standards	Annual training and documentation required

Start with HIPAA and MIPS—they account for more than 80% of audit triggers in mid-sized medical groups.

SECTION 2: Common Compliance Dangers *(and How to Get Around Them)*

Even well-intentioned practices fall into these traps:

Outdated Policies

Fix: *Review HIPAA policies annually using the HIPAA Policy Update Checklist (included in your toolkit).*

Untrained Staff

Fix: *Run quarterly 15-minute compliance huddles. Use our Staff Training Slide Deck—ready to present.*

Unsecured Communication

Fix: *Prohibit unencrypted email for PHI. Use secure messaging platforms with audit logs instead.*

Incomplete Risk Assessments

Fix: *Complete the Annual Security Risk Assessment Template (takes under 2 hours).*

Poor Documentation

Fix: *Log every training, breach drill, and policy review. Store in a centralized, encrypted folder accessible only to leadership.*

Confidence Boost

Practices that document every compliance action reduce audit penalties by ***up to 60%.***

SECTION 3: Technology’s Role in Simplifying Compliance

You don’t need a full compliance department—***just the right digital tools.***

Modern platforms can automate much of your compliance workload:

Secure Data Management

Automatic encryption, access controls, and full audit trails for every user action.

Automated MIPS Reporting

Pulls quality metrics directly from your EHR—no manual spreadsheets.

Breach Detection Alerts

Flags unusual data access before it becomes a reportable incident.

EHR-Agnostic Integration.

Works seamlessly with Epic, Cerner, and athenahealth—no workflow disruption.

Real-Time Eligibility & Prior Authorization

Reduces billing errors that commonly trigger CMS audits.

Case Example: *One 120-provider group cut audit prep time from 40 hours to 4 using automated compliance dashboards.*

SECTION 4: Your 90-Day Compliance Implementation Roadmap

This phased plan helps your team go from reactive to proactive—fast.

MONTH 1

Assess & Organize

Complete the Security Risk Assessment Template (included)

Update HIPAA policies and Business Associate Agreements

Conduct staff training using the included Compliance Training Slides

MONTH 2

Automate & Secure

Enable secure messaging and two-factor authentication for all logins

Turn on automated eligibility checks and MIPS data capture

Set up real-time breach monitoring alerts

MONTH 3

Test & Document

Run a mock CMS audit using your provided checklist

Compile all documentation in your Compliance Binder (digital or physical)

Schedule quarterly review meetings and assign owners for follow-up actions

The Athelas Advantage: Compliance Built In

Athelas delivers HIPAA-compliant RCM, EHR, and Ambient AI Scribe—all on one secure platform. With Athelas, compliance isn't a separate project—it's part of your daily workflow.

Baked-in protections include:

- **End-to-end encryption and role-based access**
- **Automatic audit logs for every transaction**
- **Real-time MIPS data aggregation**
- **Secure, EHR-integrated AI scribe**
- **No long-term contracts**

Book a demo with Athelas to see how we help practices like yours simplify regulatory adherence—without adding new systems or staff.

Sources

1. MGMA: *Compliance and Risk Management Benchmarks* (2024)
2. HHS Office for Civil Rights: *HIPAA Audit Protocol* (2025)
3. CMS: *MIPS 2025 Final Rule Summary*
4. KLAS Research: *RCM Services for Mid-Market Providers* (2025)
5. Health Affairs: *Financial Impact of Compliance Failures* (2024) https://www.healthaffairs.org/doi/10.1377/hlthaff.2023.0156

Template 1: Annual Risk Assessment Worksheet

~2 hours to complete

Help your practice complete the Annual Security Risk Assessment mentioned in Section 2 and Month 1 of the roadmap—identifying and prioritizing potential HIPAA and CMS compliance risks.

Category	Assessment Question	Risk Level *(Low/Med/High)*	Mitigation Action	Owner	Due Date
HIPAA Security	Are all PHI storage systems encrypted and access-controlled?	High ▾			
HIPAA Privacy	Are staff trained on minimum necessary access?	Medium ▾			
Technical Safeguards	Is two-factor authentication active for all logins?	Low ▾			
Administrative Safeguards	Do we have current Business Associate Agreements (BAAs) on file?	Low ▾			
CMS / MIPS	Are quality measures auto-captured from the EHR without manual edits?	Low ▾			
Incident Response	Is there a breach response plan tested within the last 12 months?	Low ▾			
Documentation	Are audit logs automatically generated and stored securely?	Low ▾			

Add your total “High” risk items. If you have more than 3, schedule a leadership review within 30 days and apply mitigation actions using your Compliance Binder.

Template 2: Quarterly Staff Compliance Training Log

Ensure staff are up to date on HIPAA, MIPS, and safety protocols—and that every session is documented to reduce audit penalties.

Quarter	Q1	Q2	Q3	Q4
Date				
Topic / Module	**HIPAA refresher:** Secure Messaging & PHI Handling	**CMS / MIPS:** Documentation Accuracy & Timely Reporting	**OSHA / CLIA:** Safety & Lab Standards	**Cybersecurity Drill:** Phishing Response Simulation
Trainer				
Attendance %				
Key Takeaway or Update				
Follow-Up Action				
Completion Verified By				

Store signed attendance sheets or digital completion reports in your encrypted Compliance Binder. Upload your slide deck to a shared folder so staff can review asynchronously.

Template 3: Annual Policy Review Tracker

Maintain all key compliance policies current, approved, and properly distributed.

Policy Name	Last Review Date	Reviewer	Required Update? *(Y/N)*	Notes/ Changes	Next Review Date	Distribution Verified?
HIPAA Privacy & Security Policy			Yes ▾			
Breach Notification Procedure			Yes ▾			
MIPS / Quality Reporting SOP			Yes ▾			
Business Associate Agreements (BAAs)			Yes ▾			
Secure Messaging Policy			Yes ▾			
OSHA / CLIA Compliance Manual			Yes ▾			

Reminders

- Schedule automatic review alerts every 12 months.
- Record approvals digitally (e-signature acceptable under HIPAA).
- Archive all retired versions securely—auditors may request prior policy versions.

Athelas HIPAA Audit Checklist

Use this checklist to assess your practice’s HIPAA readiness.

Administrative Safeguards

Risk Analysis completed within 12 months	Not Compliant ▾	
Documented Risk Management Plan exists	Not Compliant ▾	
HIPAA Security Officer designated	Not Compliant ▾	
Annual staff HIPAA training conducted	Not Compliant ▾	
Incident response plan documented	Not Compliant ▾	
Sanction policy in place	Not Compliant ▾	
BAAs on file for all vendors	Not Compliant ▾	

Physical Safeguards

Restricted facility access to PHI areas	Not Compliant ▾	
Workstations secured and auto-lock enabled	Not Compliant ▾	
Secure device/media disposal process	Not Compliant ▾	

Technical Safeguards

Unique IDs and password protocols	Not Compliant ▾	
Encryption of PHI at rest and in transit	Not Compliant ▾	
Quarterly audit log reviews	Not Compliant ▾	
Integrity controls prevent PHI alteration	Not Compliant ▾	
No unencrypted PHI transmission	Not Compliant ▾	

Athelas HIPAA Audit Checklist (cont.)

Organizational Requirements

Current HIPAA policies reviewed annually	Not Compliant ▾	
Documented workforce sanctions process	Not Compliant ▾	
Patient complaint process in place	Not Compliant ▾	
Documentation retained for 6 years	Not Compliant ▾	

Breach Notification

Breach assessment procedure defined	Not Compliant ▾	
Patients notified within 60 days	Not Compliant ▾	
Major breaches reported to HHS/media	Not Compliant ▾	
Breach logs maintained for 6 years	Not Compliant ▾	