GUESS COMPLIANCE CONSULTING LLC.

Compliance made simple – for small and medium-sized healthcare teams

GUESS COMPLIANCE CONSULTING LLC PRESENTS

Compliance Confidence Assessment™ + Implementation Workbook

For Small and Mid-Size Healthcare Practices

Turn your compliance gaps into a practical action plan. This workbook helps you prioritize risks, build accountability, and create a defensible compliance program over the next 90 days.

Use this workbook after completing the Operational Compliance Readiness Checklist

GAP ANALYSIS | **90-DAY ROADMAP** | **5 TEMPLATES** | **AUDIT PREVENTION**

Operational Compliance for Growing Healthcare Teams

GuessComplianceConsultingLLC.com

Section 1: What Your Gaps Actually Mean

Every unchecked item on your scorecard is not just a missing policy. It is a specific operational exposure. This section translates your gaps into language regulators use so you understand exactly what is at risk and why it matters.

Missing or Outdated Security Risk Analysis	HIGH RISK
What OCR Expects	What OCR expects: A current, documented SRA that reflects your actual systems, workflows, and vendors. Not a template from three years ago. A living evaluation tied to your operational calendar.
Operational Impact	Operational impact: Without a current SRA, you cannot demonstrate that you identified your risks. OCR has cited the absence of a risk analysis as the primary finding in the majority of HIPAA enforcement actions. This is not a technicality. It is the foundation everything else is built on.

Incomplete Business Associate Agreement Inventory	HIGH RISK
What OCR Expects	What OCR expects: A complete, current inventory of every vendor that creates, receives, maintains, or transmits protected health information on your behalf. Agreements must reflect what is actually happening today, not what existed at signing.
Operational Impact	Operational impact: Vendor services expand. Ownership changes. New data-sharing arrangements develop. An agreement that covered a narrow scope two years ago may no longer reflect the relationship. That gap is your liability, not your vendor's.

Role-Based Access Controls Not Documented	HIGH RISK
What OCR Expects	What OCR expects: Documented access profiles for every staff role specifying which systems and record types that role requires. Access logs reviewed on a regular schedule.
Operational Impact	Operational impact: Informal access is one of the three most common operational gaps in growing practices. Someone needs temporary access and gets it. The problem resolves but the access stays. Access logs capture all of it. When an investigation opens, the logs are evidence.

Training Records Incomplete	MEDIUM RISK
What OCR Expects	What OCR expects: Documentation of what was covered, who received it, when, and how it connects to the specific workflows and scenarios in each role. Generic annual awareness training alone does not meet the standard.
Operational Impact	Operational impact: A phishing attack compromised 45 employee email accounts at one healthcare organization, exposing nearly 190,000 patients. OCR's investigation found insufficient workforce training and monitoring. The settlement was $600,000. The training records told the story.

Policies Do Not Match Workflows	MEDIUM RISK
What OCR Expects	What OCR expects: Policies that reflect how the organization actually operates today, reviewed within the past 12 months, with documented evidence of review.
Operational Impact	Operational impact: A policy gets written when the practice opens. Then the EHR changes. A new platform gets added. Staff turns over. The workflow evolves but the policy stays where it was. Staff work around the parts that no longer fit. What the policy says and what the practice does are no longer the same thing. That gap is visible in an audit.

No Documented Incident Response Process	HIGH RISK
What OCR Expects	What OCR expects: A documented process that specifies what to do, in what order, and who is responsible from the moment a potential incident is discovered. A documented four-factor breach risk assessment process.
Operational Impact	Operational impact: How an organization responds to an incident often matters more than the incident itself. Regulators rarely penalize organizations for isolated mistakes when there is evidence of structured response. They penalize organizations for lack of documentation, patterns of inaction, and repeated issues without correction.

Vendor Oversight Stops at Contract Signing	MEDIUM RISK
What OCR Expects	What OCR expects: Ongoing monitoring of vendor compliance obligations, not just at contract signing. A clear process for what happens if a vendor experiences a breach or fails to meet their BAA obligations.
Operational Impact	Operational impact: Signed agreements are the beginning. Operational oversight is the requirement. Vendor services change. Subcontractor arrangements develop. Ownership transfers. The BAA must reflect what is actually happening, and someone in your organization must be watching.

Compliance Responsibilities Not Assigned	MEDIUM RISK
What OCR Expects	What OCR expects: Every compliance-sensitive function has a named individual responsible for it. Not a department. Not a role title. A specific person.
Operational Impact	Operational impact: When nobody owns it, everybody assumes someone else is watching. That assumption is where gaps build quietly over time. In a growing practice, proximity disappears as the team expands. The informal standard that kept things consistent in a small team does not scale. Formal assignment is what replaces it.

Policy Reviews Not Documented	MEDIUM RISK
What OCR Expects	What OCR expects: Documented policy reviews with dates, names, and any changes made. An audit trail that demonstrates ongoing maintenance rather than static storage.
Operational Impact	Operational impact: If you cannot produce documentation, the assumption is that it did not happen. A binder full of undated policies sitting in a drawer is not a compliance program. It is a collection of documents. The documentation of review is what creates the evidence of a functioning program.

Monitoring Activities Not Performed Consistently	MEDIUM RISK
What OCR Expects	What OCR expects: A cadenced oversight schedule. Quarterly billing reviews. Monthly documentation spot checks. Regular policy reviews tied to operational changes.
Operational Impact	Operational impact: Compliance oversight is a rhythm, not an event. The practices that hold up under scrutiny are not the ones that reviewed everything once a year. They are the ones that never went more than a quarter without looking. Episodic compliance creates the gaps that systematic monitoring would have caught.

Section 2: Gap-to-Action Matrix

Use this matrix to prioritize your remediation efforts. High risk gaps should be addressed before medium risk gaps regardless of how easy or difficult they are to close. Column four is your accountability column. Fill it in before you close this workbook.

Compliance Gap	Risk Level	Address First?	Owner	Target Date	Status
Missing or Outdated Security Risk Analysis	HIGH	Yes	_____	_____	Not Started
Incomplete BAA Inventory	HIGH	Yes	_____	_____	Not Started
No Documented Incident Response Process	HIGH	Yes	_____	_____	Not Started
Role-Based Access Controls Not Documented	HIGH	Yes	_____	_____	Not Started
Training Records Incomplete	MEDIUM	Next	_____	_____	Not Started
Policies Do Not Match Workflows	MEDIUM	Next	_____	_____	Not Started
Vendor Oversight Stops at Contract Signing	MEDIUM	Next	_____	_____	Not Started
Compliance Responsibilities Not Assigned	MEDIUM	Next	_____	_____	Not Started
Policy Reviews Not Documented	MEDIUM	Next	_____	_____	Not Started
Monitoring Not Performed Consistently	MEDIUM	Next	_____	_____	Not Started

Rule: Do not let ease determine order. A medium-risk gap that takes 30 minutes to close does not move ahead of a high-risk gap that takes three weeks. Risk level determines sequence. Capacity determines pace.

Section 3: 90-Day Compliance Roadmap

This roadmap gives you a structured sequence for closing gaps across three months. Each month builds on the one before it. Do not skip ahead. The foundation work in Month 1 determines whether Months 2 and 3 hold.

MONTH 1 — Governance and Foundation

The first month is about establishing the structural foundation. Everything else depends on this work being done first.

- ☐ **Complete or update your Security Risk Analysis** — High
  This is the foundation document that everything else references. It must reflect your current systems, vendors, and workflows.
- ☐ **Assign compliance responsibilities by name** — High
  Every compliance-sensitive function needs a specific person, not a department or a title. Document the assignments.
- ☐ **Audit your BAA inventory** — High
  Pull every vendor that touches protected health information. Confirm current agreements exist and reflect the current scope of each relationship.
- ☐ **Document your incident response process** — High
  Write the process before you need it. Specify what to do, in what order, and who is responsible from the moment an incident is discovered.

Month Notes / Owner: _____

MONTH 2 — Workforce and Access

Month 2 addresses the human and system access layer. This is where informal practices get formalized and training records get current.

- ☐ **Conduct a role-based access audit** — High
  Review every staff role. Document what access each role requires. Identify and remove access that no longer aligns with current role responsibilities.
- ☐ **Review and update workforce training records** — Medium
  Document what was covered, who received it, when. Connect training to actual workflows and scenarios, not just general HIPAA awareness.

- [ ] **Review access logs for the past 90 days**
  Identify any access events that do not align with expected role-based behavior. Document the review and any corrective actions taken. **High**

- [ ] **Conduct a policy review against current workflows**
  Walk through each policy and compare it to how the practice actually operates today. Document what changed, what was updated, and when. **Medium**

Month Notes / Owner:

MONTH 3 Monitoring and Sustainability

Month 3 builds the ongoing oversight rhythm that keeps the work from Month 1 and Month 2 from eroding over time.

- [ ] **Establish a quarterly compliance review schedule**
  Put it on the operational calendar. Not when it is convenient. On a fixed schedule that repeats. Compliance oversight is a rhythm, not an event. **Medium**

- [ ] **Build a vendor monitoring process**
  Create a process for reviewing vendor compliance obligations on an ongoing basis. Include subcontractor arrangements. Schedule annual BAA reviews. **Medium**

- [ ] **Document a policy review cycle**
  Tie policy reviews to the operational calendar and to specific triggers: new system, new vendor, new staff role, new service line. **Medium**

- [ ] **Complete a compliance program review with leadership**
  Bring the work from the past 90 days to leadership. Document what was reviewed, what was addressed, and what is in progress. **Medium**

Month Notes / Owner:

Section 4: Working Templates

These five templates give you a starting framework for the most critical compliance functions. They are designed to be filled in, adapted to your practice, and maintained as living documents. A template in a drawer is not a compliance program. A completed, dated, regularly reviewed template is.

Template 1: Compliance Oversight Log

Use this log to document compliance oversight activities on an ongoing basis. Date every entry. Name every reviewer.

Date	Activity Reviewed	Findings / Notes	Action Required	Reviewer

Template 2: Policy Review Tracker

Document every policy review with dates, reviewers, and changes made. An undated policy is an unreviewed policy in the eyes of a regulator.

Policy Name	Last Reviewed	Reviewed By	Changes Made	Next Review
			Yes / No / Notes:	
			Yes / No / Notes:	

_____	_____	_____	Yes / No / Notes: _____	_____
_____	_____	_____	Yes / No / Notes: _____	_____
_____	_____	_____	Yes / No / Notes: _____	_____
_____	_____	_____	Yes / No / Notes: _____	_____
_____	_____	_____	Yes / No / Notes: _____	_____

Template 3: Vendor Inventory Log

Every vendor that touches protected health information belongs in this log. Review it quarterly. Update it immediately when a vendor relationship changes.

Vendor Name	Service Type	BAA on File	BAA Date	Last Reviewed	Notes
		Yes / No			
		Yes / No			
		Yes / No			
		Yes / No			
		Yes / No			
		Yes / No			
		Yes / No			
		Yes / No			

Template 4: Annual Compliance Calendar

Compliance oversight is a rhythm, not an event. Use this calendar to build recurring review activities into your operational schedule.

Frequency	Activity	Owner	Completed
Monthly	Review access logs for unusual activity		☐
	Check for unresolved compliance concerns		☐
	Review any incidents from the prior month		☐
Quarterly	Review billing documentation for consistency		☐
	Audit a sample of records against policies		☐
	Review vendor compliance status		☐
	Update compliance oversight log		☐

Annually	Complete or update Security Risk Analysis		■
	Review and update all HIPAA policies		■
	Review all Business Associate Agreements		■
	Complete workforce compliance training		■
	Conduct leadership compliance review		■
Triggered	New system or EHR platform added		■
	New vendor or subcontractor engaged		■
	Staff role change or termination		■
	Potential incident or breach		■
	Regulatory update affecting operations		■

Template 5: Incident Review Worksheet

Important: Complete this worksheet for every potential incident, regardless of whether you believe it constitutes a reportable breach. The documentation of the review is what demonstrates compliance maturity. Complete it. Date it. File it.

Date Incident Discovered:

Date This Worksheet Completed:

Completed By (Name and Role):

Description of What Occurred:

Systems or Records Involved:

Staff Members Involved:

Four-Factor Breach Risk Assessment

Complete all four factors. Document your assessment for each.

Factor 1	Nature and extent of the PHI involved
What type of information was involved? How sensitive is it? How much?	Assessment:

Factor 2	Who accessed or could have accessed the information
Was the recipient authorized? Is there evidence the information was actually viewed?	Assessment:

Factor 3	Whether the information was actually acquired or viewed
Is there evidence the information was accessed beyond what was authorized?	Assessment:

Factor 4	Extent to which risk has been mitigated
What steps were taken to reduce the risk of harm? Were notifications made?	Assessment:

Conclusion (Breach / Not a Breach / Further Review Required):

Corrective Actions Taken:

Policy Updates Made as a Result:

Reviewed and Signed By:

Section 5: Dr. Natasha's Audit Prevention Framework

This section is drawn from direct experience working with small and mid-size healthcare practices through compliance reviews, gap assessments, and remediation planning. The patterns here are not theoretical. They are what actually surfaces when an investigation opens or an audit request arrives.

What Triggers Investigations

Patient Complaints

The single most common trigger for OCR investigations in small practices is a patient complaint. A patient who feels their information was mishandled, shared without permission, or used inappropriately can file a complaint directly with OCR at no cost to them. The complaint triggers a desk review. The desk review triggers a document request. The document request reveals what you do and do not have.

Breach Reports

Every breach report filed with OCR triggers a review. For breaches affecting 500 or more individuals, OCR notification is required within 60 days of discovery and the breach is posted on the OCR Wall of Shame. But smaller breaches accumulate too. Patterns of small breaches are as likely to draw scrutiny as a single large one. The response documentation is what determines the outcome.

Business Associate Incidents

When a vendor experiences a breach that involves your patients' information, the investigation does not stop at the vendor. Regulators will review your BAA, your vendor oversight process, and your response. A vendor's breach is your compliance event. How prepared you are for that conversation starts long before the incident occurs.

Random Audits

OCR conducts random compliance audits of covered entities and business associates. Selection is not based on suspicion. It is based on a pool of organizations. When your name is pulled, you receive a document request with a response deadline. The organizations that handle random audits well are the ones that would have passed any audit on any day because their documentation reflects what they actually do.

Disgruntled Workforce Members

A staff member who leaves under difficult circumstances can file a complaint. A workforce member who feels retaliated against for raising a compliance concern can file a complaint. These complaints are investigated the same way patient complaints are. The organizations most exposed here are the ones that do not have a documented reporting culture that separates reporting from punishment.

Common Documentation Mistakes That Create Exposure

1 The SRA That Describes a Practice That No Longer Exists

A Security Risk Analysis completed three years ago during an EHR implementation is not a current SRA. If your systems have changed, your vendors have changed, or your workflows have changed, your SRA must reflect those changes. An outdated SRA is often worse than no SRA because it demonstrates that the organization knows what is required and chose not to maintain it.

2 Training Records That Document Attendance, Not Content

A sign-in sheet from an annual HIPAA training session is not a training record. A training record documents what was covered, who received it, when, what platform was used, and how it connects to the specific workflows of that staff member's role. Generic annual awareness training alone does not meet the standard. If a breach occurs and your training records cannot demonstrate role-specific content, the training records become a liability.

3 Policies With No Review History

A policy binder with no dates, no reviewer names, and no change log is a collection of documents. It is not evidence of a functioning compliance program. The review is what creates the compliance value. The documentation of the review is what creates the evidence. Both are required.

4 Incident Documentation That Starts After Mitigation

When something goes wrong, the most common mistake is beginning documentation after the organization has already taken corrective action. The documentation must begin from the moment the potential incident is discovered. What was observed, when, by whom, what was done first, what was preserved, what was assessed. Organizations that reconstruct incident documentation after the fact are creating a record that does not match the timeline. That inconsistency is noticed.

5 Access Logs That Are Collected But Never Reviewed

Having access logs is not the same as having access oversight. The log captures what happened. The review is what demonstrates that someone was watching. Access logs that sit unreviewed are evidence of a system that was collecting data without governance. When an investigation surfaces an access event that the organization could have identified through log review, the question becomes why no one was looking.

Operational Blind Spots

These are the compliance gaps that surprise even the practices that believe they are doing well. They are not the result of negligence. They are the predictable outcome of organizations that grew faster than their compliance structure.

1 The Practice That Grew Beyond Its Informal System

In a small practice, proximity maintains consistency. Everyone sees what everyone else does. There is an informal standard that holds things together even without formal structure. When the practice adds clinicians, expands services, or introduces new workflows, that proximity disappears. The informal system that worked for three people does not work for ten. The gaps that appear are not new failures. They are the natural result of growth that outpaced the compliance structure underneath it.

2 Informal Communication Channels

Operational teams are built for speed. That pressure for speed is valuable and it is also where safeguards quietly disappear. A text message sent from a personal phone to clarify a billing question. A patient note shared through a consumer messaging app for convenience. Each one feels like a time saver. Each one carries compliance exposure that begins the moment the message is sent. Workflow convenience becomes regulatory exposure. Every single time.

3 The Compliance Program That Existed in Someone's Head

Many small practices have a deeply knowledgeable person who carries the compliance function informally. They know the rules. They answer the questions. They catch the problems. When that person leaves, retires, or changes roles, the compliance knowledge leaves with them. There is no documentation trail. No policy framework. No oversight structure. The organization discovers the gap when it cannot answer a basic question during a review.

4 The BAA That Was Signed and Filed

A signed BAA is the beginning of a vendor compliance relationship. It is not the end. Vendor services expand beyond the original scope. Ownership transfers. New data-sharing arrangements develop. Subcontractors are added. The agreement sits in a file while the relationship it was designed to govern no longer reflects what is actually happening. The first time someone reviews it carefully is often during an incident.

5 Leadership Blind Spots

Practice leaders who are not in the day-to-day operational workflow often do not know what they do not know. Compliance is reported as fine because no one has surfaced a concern. No concern has been surfaced because there is no structured process for surfacing concerns. There is no structured process because no one built one. The compliance program that exists in leadership's understanding of the organization is not the same compliance program that exists in the day-to-day operations. That distance is where the most significant exposure lives.

Recommended Order of Operations

Use this sequence alongside your 90-day roadmap. The order is not arbitrary. High-risk gaps that are foundational to everything else come first. Sustainability work comes last because it requires the foundation to already be in place.

WEEKS 1–2 — Foundation First

- **Security Risk Analysis** — HIGH
  Everything else references this document. It must exist and be current before you build anything else on top of it.
- **BAA Inventory** — HIGH
  Identify every vendor that touches protected health information. Confirm agreements exist and reflect the current scope of each relationship.

WEEKS 3–4 — Structural Safeguards

- **Incident Response Process** — HIGH
  Write the process before you need it. Document what to do, in what order, and who is responsible from the moment an incident is discovered.
- **Compliance Responsibilities** — HIGH
  Assign every compliance-sensitive function to a named individual. Document the assignments. Distribute them.

MONTH 2 — Workforce and Access

- **Access Controls** — HIGH
  Audit every role. Document required access. Remove access that no longer reflects current role responsibilities. Review access logs.
- **Training Documentation** — MEDIUM
  Verify training records are current, role-specific, and reflect actual workflows. Close documentation gaps before they become findings.

MONTH 3 Monitoring and Sustainability

- [ ] **Monitoring Activities**
  Establish a cadenced oversight schedule. Quarterly billing reviews. Monthly documentation spot checks. Put it on the calendar and keep it there.
  MEDIUM

- [ ] **Policy Reviews**
  Walk every policy against current workflows. Document what changed and when. Create a review cycle tied to the operational calendar.
  MEDIUM

- [ ] **Vendor Oversight**
  Build an ongoing monitoring process. Schedule annual BAA reviews. Create a process for what happens when a vendor relationship changes.
  MEDIUM

The sequence matters. A monitoring program built on top of an incomplete risk analysis is monitoring the wrong things. A policy review conducted before compliance responsibilities are assigned has no owner. Follow the order. The 90 days compounds.

Next Steps

You now have a gap analysis, a prioritized action matrix, a 90-day roadmap, five working templates, and a framework built from direct compliance work with small and mid-size healthcare practices. The next step is moving from assessment to implementation.

> **The practices that get through audits and investigations are not the ones that had the most policies. They are the ones that can show, with documentation, that compliance was working before anyone came looking.**

Schedule Your Compliance Diagnostic	calendly.com/guesscomplianceconsulting-proton/compliancestrategycall

The Guesswork Ends Here™ HIPAA Compliance Template Kit

Templates, policies, checklists, logs, and a 30-day implementation roadmap. Everything in this workbook, expanded and ready to deploy in your practice.

GuessComplianceConsultingLLC.com
/the-guesswork-ends-here

