COMPLIANCE READINESS SELF-ASSESSMENT

Are You Ready for a Healthcare Compliance Review?

This assessment is based on the seven elements of an effective compliance and ethics program as outlined in the Federal Sentencing Guidelines.

Answer each question honestly. Score 1 point for each "Yes."

ELEMENT 1: Written Standards and Procedures

Do you have documented policies that guide compliant behavior?

- ☐ We have written HIPAA policies and procedures
- ☐ We have a method for determining when policies are needed and how to create them
- ☐ Our policies are accessible to all employees who need them
- ☐ Our policies are updated at least annually or when regulations change

Subtotal: _____ / 4

ELEMENT 2: Oversight by High-Level Personnel

Is there clear accountability for your compliance program?

- ☐ We have a designated Privacy Officer or Security Officer (or both)
- ☐ Our compliance officer has direct access to senior leadership
- ☐ Leadership demonstrates commitment to compliance (not just delegated to IT)
- ☐ Board or senior management receives regular compliance updates

Subtotal: _____ / 4

ELEMENT 3: Due Care in Delegation

Do you screen and authorize people who have access to sensitive data?

- ☐ We conduct background checks on employees handling PHI
- ☐ We have documented processes for granting and revoking system access
- ☐ We screen vendors and subprocessors before they handle PHI
- ☐ We have Business Associate Agreements (BAAs) with all relevant third parties

Subtotal: _____ / 4

ELEMENT 4: Effective Communication and Training

Do your people know what's expected of them?

- ☐ All employees who handle PHI have completed HIPAA training

- ☐ We maintain records of training completion with dates
- ☐ New hires receive compliance training during onboarding
- ☐ We provide annual refresher training or updates when policies change
- ☐ Employees know the reporting process for compliance concerns or incidents

Subtotal: _____ / 5

ELEMENT 5: Monitoring, Auditing, and Risk Assessment

Do you actively look for compliance problems?

- ☐ We have completed a formal HIPAA risk assessment in the past 12 months
- ☐ We maintain audit logs that track access to PHI
- ☐ We can demonstrate our audit logging capability on demand
- ☐ We review audit logs periodically to detect unauthorized access
- ☐ We have documented our technical safeguards (encryption, access controls, etc.)
- ☐ We conduct periodic security assessments or penetration testing

Subtotal: _____ / 6

ELEMENT 6: Enforcement and Discipline

Do you hold people accountable for compliance violations?

- ☐ We have documented disciplinary procedures for policy violations
- ☐ Our employees understand consequences of non-compliance
- ☐ We apply discipline consistently when violations occur

Subtotal: _____ / 3

ELEMENT 7: Response and Prevention

Can you respond effectively when things go wrong?

- ☐ We have a documented incident response procedure
- ☐ We know who to contact and what steps to take if a breach occurs
- ☐ We have a breach notification process (internal and external)
- ☐ We document incidents and use them to improve our program
- ☐ We have a process for investigating and remediating compliance issues

Subtotal: _____ / 5

YOUR TOTAL SCORE

Add up all subtotals: _____ / 31 points

SCORE INTERPRETATION

28-31 Points: ENTERPRISE-READY ✓

You have a mature compliance program. You're well-positioned to pass healthcare compliance reviews with confidence. Your program demonstrates the fundamental elements of effective compliance.

Strengths: You likely have strong documentation, clear accountability, and systematic processes.

Next steps:

- Consider third-party validation (SOC 2 Type II, HITRUST)
- Focus on continuous improvement and staying current with regulations
- Use your compliance maturity as a competitive differentiator

You can confidently address sophisticated compliance questions from your partners.

22-27 Points: NEARLY READY ⚠

You have a solid foundation but some gaps remain.

Common gaps at this level:

- Training records may be incomplete
- Risk assessments may be outdated
- Incident response procedures may lack detail
- Monitoring and auditing may be inconsistent

Next steps:

- Review your scores by element—which scored lowest?
- Prioritize closing gaps in Elements 1, 4, and 7 (most visible to auditors)
- Document what you're already doing (you may be more compliant than your documentation shows)
- Plan a 60-day sprint to reach enterprise-ready status

You have a comprehensive compliance program and are finalizing documentation of your processes.

15-21 Points: SIGNIFICANT WORK NEEDED

You have pieces in place but lack systematic approach. You need a structured 90-day program to get ready.

Common challenges at this level:

- Policies exist but aren't updated or accessible
- Training is ad-hoc rather than systematic
- No formal risk assessment process
- Limited monitoring and auditing
- Unclear accountability for compliance

Next steps:

- Don't start compliance reviews until you've strengthened your foundation
- Focus on Elements 1, 2, and 5 first (foundation of any program)
- Consider engaging a compliance consultant to accelerate your timeline
- Build a realistic 90-day roadmap with clear milestones

You're in the process of formalizing your compliance program and will be ready for review at the conclusion of the current build out phase.

8-14 Points: BUILDING FOUNDATION

You're in early stages of compliance program development. You need 90-120 days of focused work before pursuing enterprise healthcare deals.

Critical gaps likely include:

- Missing or incomplete policies
- No designated compliance officer
- Limited or no formal training
- No risk assessment completed
- Inadequate monitoring and auditing
- Unclear incident response procedures

Next steps:

- Focus on the basics: Designate a compliance officer, draft core policies, conduct initial risk assessment
- Don't pursue enterprise deals yet—failed reviews damage your reputation
- Budget 3-4 months to build foundation before re-assessing

You're building your compliance program and are completing a comprehensive risk assessment and program build out.

WHAT'S MOST AT RISK?

Review your scores by element to identify priorities:

Element 1 (Standards & Procedures): ___/4

- **If you scored 0-2:** This is your #1 priority. You have no foundation. Write your core policies immediately.
- ***What healthcare buyers see:*** *"They don't know what they're supposed to be doing."*

Element 2 (Oversight): ___/4

- **If you scored 0-2:** No one is accountable for compliance. Designate a compliance officer now.
- ***What healthcare buyers see:*** *"Compliance is an afterthought, not a priority."*

Element 3 (Due Care): ___/4

- **If you scored 0-2:** You're not vetting people who access PHI. Critical security gap.
- ***What healthcare buyers see:*** *"They're careless about who handles our data."*

Element 4 (Training): ___/5

- **If you scored 0-3:** Your people don't know how to handle PHI properly.
- ***What healthcare buyers see:*** *"Their employees will cause a breach."*

Element 5 (Monitoring): ___/6

- **If you scored 0-3:** You can't prove what's happening in your systems.
- ***What healthcare buyers see:*** *"They're flying blind. They won't detect problems."*

Element 6 (Enforcement): ___/3

- **If you scored 0-1:** No consequences for violations. Policies are meaningless.
- ***What healthcare buyers see:*** *"Their compliance program is for show."*

Element 7 (Response): ___/5

- **If you scored 0-2:** You can't respond effectively to incidents.
- ***What healthcare buyers see:*** *"When something goes wrong, it will be a disaster."*

RECOMMENDED ACTION PLAN BY SCORE

Scored 22+: Focus on polish and validation

- Document any undocumented processes (you're likely doing more than you've written down)
- Update any policies older than 12 months
- Conduct refresher training on any new policies
- Consider formal validation (SOC 2, HITRUST, or third-party assessment)

Scored 15-21: Systematic improvement

- Prioritize Elements where you scored lowest
- Create 60-90 day improvement roadmap
- Focus on maturity across all elements
- Re-assess to track progress

Scored 8-14: Foundation building

- Designate compliance officer (Element 2)
- Write or update core policies (Element 1)
- Conduct initial risk assessment (Element 5)
- Implement basic training program (Element 4)
- Budget 90-120 days before pursuing enterprise deals

Scored 0-7: Ground-up program development

- Get leadership commitment and budget
- Hire or engage compliance expertise
- Build 6-month roadmap covering all seven elements
- Start with policies and accountability
- Don't pursue enterprise deals until you reach 15+ score

WHY THESE SEVEN ELEMENTS MATTER

Healthcare compliance reviews aren't checklists—they're evaluations of whether you have a **systematic approach** to protecting patient data.

The seven elements framework (from Federal Sentencing Guidelines) represents the core of a compliance program. If something goes wrong, having these elements in place demonstrates you were trying to do the right thing.

Healthcare buyers look for these elements because:

- They show compliance is systematic, not ad-hoc
- They demonstrate organizational commitment (not just IT doing their best)
- They indicate you'll detect and respond to problems
- They suggest you'll improve over time, not just "check boxes"

Missing these elements signals:

- The organization lacks maturity
- Compliance is not a priority
- Problems will be invisible until it's too late
- Risk of breach, fine, or regulatory action

NEXT STEPS

Want help interpreting your results or building an improvement plan?

Feel free to reach out for a no-pressure conversation about where you are and what makes sense for your situation.

Reach out to me at:

Phone: (509) 368-7411
Email: info@dangssolutions.com

METHODOLOGY NOTE

This assessment is based on the **Seven Elements of an Effective Compliance and Ethics Program** from the Federal Sentencing Guidelines for Organizations (§8B2.1). These elements are widely recognized as the foundation of effective compliance programs across industries, including healthcare.

While this assessment focuses on HIPAA compliance readiness, the seven elements framework applies to any regulatory compliance program.

This assessment is not:

- A guarantee of HIPAA compliance
- A substitute for legal counsel
- A formal audit or certification
- A comprehensive security assessment

This assessment helps you:

- Identify gaps in your compliance program
- Prioritize improvement efforts
- Prepare for healthcare compliance reviews
- Understand what "compliance-ready" actually means

2025 Dang's Solutions, LLC. This assessment is for educational purposes and does not constitute legal advice. Consult with qualified counsel for specific compliance guidance.