

Checklist: 5 Must-Have Features of a Compliance Solution for Healthcare Providers

A Practical Guide for Healthcare CISOs, Compliance Officers, Risk Managers, and IT Leaders

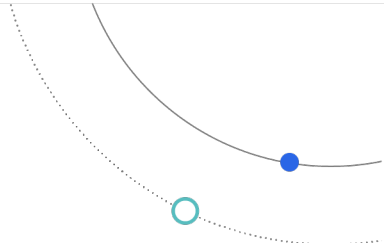
Why This Checklist Matters:

Healthcare compliance isn't just a regulatory requirement, it's essential for protecting patient trust, avoiding costly breaches, and ensuring long-term organizational resilience.

Today's environment demands continuous visibility, proactive risk management, and automated audit readiness, especially with HIPAA, HITECH, CMS, OCR, and emerging state privacy mandates tightening requirements year after year.

- Gartner predicts that by 2026, 70% of healthcare organizations will shift to continuous compliance monitoring.
- IDC Health Insights reports that proactive compliance strategies can reduce penalties by up to 50% and cut breach costs significantly.

This checklist is your guide to selecting a modern compliance solution, one that not only protects but strengthens your healthcare organization in a rapidly evolving world.



Checklist: 5 Must-Have Features

1

Continuous Compliance Monitoring and Evidence Collection

Why It's Critical:

Healthcare organizations face heightened scrutiny from regulators like OCR, CMS, and HHS, who now expect continuous oversight—not just once-a-year audits. Compliance failures often stem from outdated controls, poor documentation practices, or failure to detect drift in administrative or technical safeguards. Without ongoing monitoring and continuous evidence collection, it becomes nearly impossible to demonstrate compliance during a breach investigation or surprise audit. This can result in costly penalties, reputational damage, and a loss of patient trust. A modern compliance program must enable healthcare leaders to maintain visibility across hybrid environments and confidently answer, "Are we in compliance—right now?"

Checklist Items

- Real-time monitoring: Track administrative, technical, and physical safeguards to maintain continuous alignment with HIPAA and CMS expectations.
- Collect and maintain continuous evidence: Ensure consistent gathering and storage of proof demonstrating adherence to the HIPAA Security Rule.
- Evaluate and address compliance gaps: Review findings regularly to detect and resolve misalignments before they escalate.

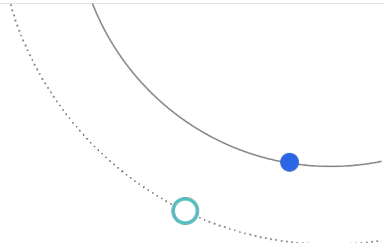
2

Proactive Risk Identification and Mitigation

Why It's Critical:

In today's healthcare landscape, risks evolve rapidly—from ransomware and phishing attacks to IoMT vulnerabilities and third-party vendor exposures. If these threats are not proactively identified and addressed, they can lead to major compliance violations and catastrophic data breaches. Relying solely on scheduled audits or compliance checklists leaves critical gaps, especially as threat actors target healthcare due to its valuable patient data and often complex, aging infrastructure. Proactive risk identification allows organizations to stay ahead of both attackers and auditors, reducing the likelihood of adverse outcomes and ensuring resilient, regulatory-aligned operations.

According to Forrester, proactive risk identification and mitigation are the single largest factors influencing whether a healthcare breach results in minor operational impacts—or full-blown legal, financial, and reputational crises.



Checklist Items

- Perform regular, risk-based compliance assessments aligned to HIPAA, HITRUST, and NIST CSF.
- Identify gaps in vendor agreements, cloud configurations, and endpoint protections.
- Prioritize mitigation efforts based on real-world threat impact and business risk.

3

Integrated Security and Compliance Automation

Why It's Critical:

Manual compliance processes are no longer sustainable in a healthcare environment defined by high alert volumes, cross-functional system dependencies, and limited internal resources. Tasks like evidence collection, control validation, and documentation are essential—but when done manually, they are time-consuming, inconsistent, and error-prone. As the volume of data increases and regulatory expectations intensify, automation becomes critical for ensuring policy enforcement, streamlining audit prep, and maintaining accurate reporting. With automation in place, healthcare organizations can shift focus from administrative busy work to strategic oversight, while reducing the risk of noncompliance caused by human error or oversight.

Gartner notes that security and compliance automation can reduce operational security costs by up to 44%, while simultaneously improving regulatory outcomes.

Checklist Items

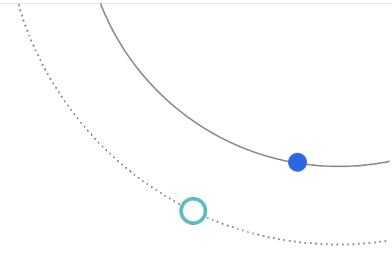
- Automate evidence collection, control checks, and policy enforcement.
- Ensure compliance activities are embedded across IT and security systems.
- Reduce audit preparation time by up to 50% through workflow standardization.

4

Expert Managed Services with Healthcare-Specific Compliance Knowledge

Why It's Critical:

Healthcare compliance isn't just technically complex, it's operationally unique. From PHI access monitoring and audit logs for EHR systems to breach notification rules under HIPAA and HITECH, providers face a web of interconnected regulatory demands that generalist service providers often overlook. Many compliance programs fail because they apply generic frameworks that don't account for care delivery workflows, clinical system integration, or the nuances of healthcare data flows. Partnering with a provider that understands the healthcare environment ensures not only technical alignment but also cultural and regulatory fit—driving better outcomes, faster audit response, and stronger organizational trust.



Checklist Items

- Partner with a provider experienced in HIPAA, HITECH, HITRUST, PCI DSS, GDPR, and state-specific privacy laws.
- Ensure 24/7 access to compliance professionals familiar with healthcare workflows and system integrations.
- Leverage regulatory liaison support and breach response expertise tailored to healthcare environments.

5

Scalable, Future-Ready Architecture

Why It's Critical:

As healthcare organizations adopt new technologies—from cloud-based EHRs to remote patient monitoring and AI diagnostics, their compliance solutions must keep up. Static, siloed tools cannot adapt to dynamic environments, resulting in security gaps and regulatory misalignment. New mandates like the California Privacy Rights Act (CPRA) and forthcoming OCR updates require healthcare IT systems to be more agile and extensible than ever before. A scalable compliance architecture ensures that as your environment grows—whether through mergers, cloud adoption, or digital health initiatives—your security and compliance posture evolves in parallel. Without it, organizations risk falling behind, retrofitting outdated systems, and increasing both cost and risk.

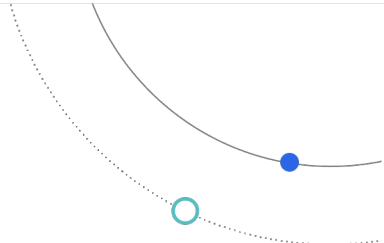
Checklist Items

- Ensure compatibility across cloud, on-premises, mobile, and hybrid environments.
- Adapt to new mandates like CPRA or upcoming OCR changes with modular compliance controls.
- Build compliance into digital transformation initiatives like remote care and AI-driven analytics.

The C1 Compliance & Risk Management Solution Suite: Built for Healthcare Leaders

At C1, we don't just help you meet compliance requirements – we help you transform compliance into a strategic advantage that protects patient trust, reduces operational risk, and supports healthcare innovation. Our Compliance & Risk Management Solution Suite is purpose-built for healthcare organizations navigating today's increasingly complex regulatory landscape.

Here's how we do it:



Advisory Services

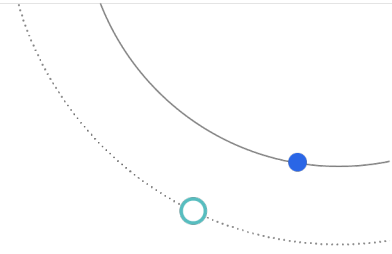
Strategic Risk Governance and Compliance Planning

- **Comprehensive Risk and Compliance Assessments**
Benchmark your current state against HIPAA, HITECH, HITRUST CSF, NIST CSF, 42 CFR Part 2, and other healthcare-specific frameworks.
- **Regulatory Gap Analysis**
Identify gaps in policies, technical controls, third-party vendor agreements, and physical security safeguards.
- **Compliance Program Design and Maturity Roadmaps**
Develop customized, phased roadmaps to move from reactive, audit-driven compliance to continuous, proactive risk governance.
- **Executive Board Reporting**
Deliver risk and compliance updates in business language for boards, C-suites, and regulatory bodies.
- **Third-Party Risk Management Strategy**
Assess and design governance programs that cover critical vendors, SaaS providers, and cloud partners to close high-risk exposure points.

Professional Services

Technology Enablement and Compliance Control Implementation

- **Deployment of Compliance-Enhancing Technologies**
Implement solutions for endpoint protection, cloud security, IoMT device monitoring, identity access governance, and continuous threat detection – all mapped to compliance controls.
- **Automation of Compliance Processes**
Integrate compliance evidence collection, audit documentation, policy enforcement, and incident reporting with platforms like Microsoft, Palo Alto Networks, Cisco, Armis, and ServiceNow.
- **Security Control Validation**
Perform detailed validation of technical and administrative safeguards to ensure readiness for HIPAA, HITECH, CMS, and OCR audits.
- **Policy Development and Documentation Support**
Create or refine healthcare-specific security and privacy policies, breach notification procedures, and acceptable use standards.
- **Incident Response Plan Development**
Align security incident response strategies to regulatory breach reporting requirements, including HIPAA and HITECH 60-day notification rules.



Managed Services

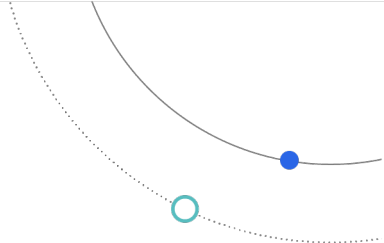
Continuous Protection, Monitoring, and Compliance Assurance

- **24/7 Compliance and Security Monitoring**
Monitor technical and administrative controls continuously to maintain regulatory readiness and detect compliance drift.
- **Real-Time Risk Reporting and Dashboards**
Deliver compliance status updates mapped to frameworks such as HIPAA, NIST CSF, and HITRUST CSF – with executive-level visibility and evidence on demand.
- **Audit Support and Documentation Readiness**
Maintain, curate, and organize audit-ready evidence libraries, compliance records, and risk treatment plans for internal and external audits.
- **Breach Response and Regulatory Notification Support**
Support rapid investigation, documentation, and regulatory engagement in the event of a breach impacting protected health information (PHI).
- **Continuous Improvement and Control Optimization**
Regularly tune, optimize, and adjust controls to align with evolving regulatory guidance, cyberthreats, and clinical innovation initiatives (telehealth, AI in healthcare, remote patient monitoring, etc.).

Enabled by Best-in-Class Technology Partners

C1's Compliance and Risk Management Solution Suite is enhanced by trusted partnerships with the world's leading technology innovators:

- **Palo Alto Networks** – Zero Trust enforcement, Precision AI™ threat detection, cloud security for HIPAA/HITECH environments
- **Cisco** – Secure network, endpoint, and identity solutions that integrate into compliance automation workflows
- **Microsoft** – Azure and Microsoft 365 security compliance alignment with Purview, Defender, and Entra solutions



Outcome-Focused, Risk-Driven, Healthcare-Ready

With C1, healthcare organizations can:

- Cut audit preparation time by up to **50%**
- Reduce breach-related costs by up to **30%**
- Decrease regulatory fine exposure by up to **40%**
- Free up compliance and security team resources to focus on innovation, patient outcomes, and digital health transformation
- Build long-term resilience and maintain patient trust

Ready to Strengthen Your Compliance Strategy?

Schedule Your Complimentary Compliance Readiness Assessment

Let's make proactive compliance your competitive advantage.

Learn more about how C1 can help you migrate your existing contact center to the cloud and take advantage of the latest CX innovations to give you a competitive edge. Learn more by visiting our website at: www.onec1.com/c1conversations or [contact us](#) for a consultation and demo.



C1, the global technology solutions provider, transforms businesses by creating connected experiences that shape the future. With more than 6,000 customers, C1 empowers industries through secure, innovative technologies, collaborating with leading partners to deliver total lifecycle solutions. Learn more at onec1.com.