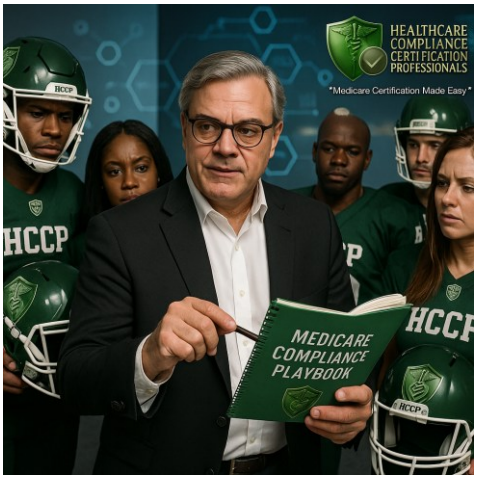
HEALTHCARE COMPLIANCE CERTIFICATION PROFESSIONALS

"Medicare Audit Readiness"

Hospice Executive

Medicare Certification & Audit Compliance

Playbook



Strategic Objective

To ensure Medicare certification and audit success by aligning leadership, staff, and processes with the Centers for Medicare & Medicaid Services (CMS), the Health Insurance Portability and Accountability Act (HIPAA), and the National Institute of Standards and Technology (NIST) frameworks.

This playbook serves as a high-level strategic guide for compliance leadership.

Developed by: Healthcare Compliance Certification Professionals, (HCCP) 2025

"Medicare Audit Readiness"

PLAY 1

Build A Compliance-Ready Team Structure

Objective: Establish a strong internal team with defined roles and responsibilities to lead Medicare certification, HIPAA, and CMS compliance efforts across the organization.

Key Actions:

- Appoint a Compliance Officer and/or Program Manager to oversee the Medicare certification process.
- Designate key functional roles: Privacy Officer (HIPAA), Security Officer (NIST), Risk Officer (SRA), and Clinical Director (CMS CoPs).
- Align each role with specific regulatory responsibilities based on NIST SP 800-171.
- HIPAA Security Rule, and CMS Conditions of Participation.
- Engage a Senior Medicare Certification Advisor or vCISO to guide organizational structure, policy alignment, and strategic oversight.
- Establish a recurring leadership meeting structure (monthly, quarterly) to review certification progress, audit risk, and documentation readiness.

Outcome:

A structured compliance leadership team capable of guiding the organization through audit readiness, regulatory alignment, and Medicare certification with confidence and clarity.

HEALTHCARE COMPLIANCE CERTIFICATION PROFESSIONALS

"Medicare Audit Readiness"

PLAY 2

Conduct Compliance Gap Analysis & Certification Readiness Review

Objective: Evaluate the organization's current compliance posture and identify gaps across HIPAA, CMS Conditions of Participation, and NIST requirements.

Key Actions:

- Conduct a HIPAA Security Risk Assessment (SRA) to evaluate technical, physical, and administrative safeguards.
- Map operations to CMS Conditions of Participation (42 CFR Part 418).
- Perform a NIST SP 800-171 gap analysis for information system controls and audit readiness.
- Review existing documentation including policies, procedures, training logs, and audit records.
- Identify critical vulnerabilities and prioritize remediation based on risk impact and Medicare readiness.

Outcome:

A comprehensive baseline assessment of compliance risk, regulatory gaps, and certification preparedness that informs future remediation planning.

"Medicare Audit Readiness"

PLAY 3

Launch Compliance Governance Framework

Objective: Establish a formal structure to oversee and manage regulatory compliance across clinical, technical, and administrative areas.

Key Actions:

- Initiate a Governance Committee or Compliance Council with representation from leadership, clinical, IT, and legal.
- Define Committee Charters and Responsibilities—clarify oversight authority, reporting requirements, and compliance domains under review (e.g. HIPAA, CMS CoPs).
- Develop and Maintain a Compliance Calendar with recurring activities such as policy reviews, risk assessments, training, and audits on a monthly, quarterly, and annual basis.
- Assign Accountability by Function: designate roles such as Privacy Officer (HIPAA), Security Officer (NIST SP), and Compliance Officer (CMS CoPs).
- Ensure Senior Advisor Involvement: include a Senior Medicare Compliance Advisor or vCISO in committee operations, strategy development, and audit prep.

Outcome:

A centralized governance structure that enables leadership to track progress, enforce accountability, and continuously mature the organization's compliance posture in alignment with federal mandates.

"Medicare Audit Readiness"

PLAY 4

Update & Align Policy Infrastructure

Objective: Align all operational documents and policy artifacts with CMS survey requirements, HIPAA safeguards, and NIST 800-171 security standards.

Key Actions:

- Review and update HIPAA-related policies including access control, breach notification, incident response, and encryption.
- Ensure policies reflect CMS Conditions of Participation (CoPs) and NIST SP 800-171 controls.
- Align SOPs with CMS survey expectations, including care planning, documentation practices, and patient rights.
- Apply version control and ensure all policies are approved by the governing board or executive leadership.
- Maintain a centralized policy repository accessible to staff and compliance auditors.

Outcome:

A fully updated and audit-ready policy framework that demonstrates regulatory alignment and facilitates real-time document production during Medicare certification or compliance review

"Medicare Audit Readiness"

PLAY 5

Execute Technical & Risk Controls

Objective: Enforce cybersecurity and risk management best practices to protect patient data, ensure operational integrity, and meet HIPAA, CMS, and NIST expectations.

Key Actions:

- Implement Multi-Factor Authentication (MFA) across all systems accessing ePHI or sensitive operational data.
- Establish routine patch management protocols and remove unsupported/end-of-life (EOL) software.
- Conduct internal technical control reviews covering access control, encryption, audit logging, and secure configuration baselines.
- Monitor and log user and system activity per HIPAA §164.312 and NIST SP 800-53 AU-2 (Audit Events).
- Maintain and update a centralized risk register with remediation tracking and risk scoring based on likelihood and impact.

Outcome:

A hardened technical environment and evidence-based risk management program that supports ongoing compliance and demonstrates due diligence during audits or investigations.

"Medicare Audit Readiness"

PLAY 6:

Prepare Certification Binder & Audit Toolkit

Objective: Organize all essential compliance documentation into an easily accessible, audit-ready binder for real-time production during CMS or Medicare-related audits.

Key Actions:

- Use the HCCP Certification & Compliance Packages as your binder's structural foundation.
- Include all documentation for HIPAA policies, Security Risk Assessments, training logs, and incident history.
- Align documentation to CMS Conditions of Participation and HIPAA audit protocol requirements.
- Organize materials in a digital or physical binder with a clear index and attestation log.
- Prepare documentation for rapid retrieval, categorized by policy area and compliance domain.

Outcome:

A fully organized, certification-ready audit binder that ensures your organization can confidently and efficiently respond to auditor requests, demonstrate ongoing compliance, and defend Medicare funding.

"Medicare Audit Readiness"

PLAY 7:
Mock Audits & Tabletop Exercises

Objective: To prepare staff and leadership for real-time audit scenarios by conducting mock audits and tabletop exercises that simulate Medicare survey conditions, ensuring rapid response capability, audit readiness, and staff confidence.

Key Actions:

- Develop realistic audit scenarios aligned with CMS survey protocols.
- Script tabletop exercises based on previous audits or OCR findings.
- Assign roles for executives, compliance leads, and clinical staff.
- Facilitate timed walk-throughs of survey interviews and documentation requests.
- Use standardized forms and audit checklists from the HCCP Toolkit.
- Capture gaps in audit responses and document retrievability.
- Repeat exercises quarterly or before scheduled CMS visits.

Outcome:

Hospice organization demonstrates increased audit preparedness and team response cohesion. Mock audits reduce anxiety, identify weaknesses in documentation practices, and solidify internal command structure. Leaders and staff become proficient in navigating Medicare survey demands in real-time, reducing the risk of citations and funding disruptions.

"Medicare Audit Readiness"

PLAY 8:

Pre-Certification Final Review

Objective: Validate the organization's full readiness before CMS certification or survey by conducting a comprehensive internal review.

Key Actions:

- Conduct a cross-functional readiness walkthrough with compliance, clinical, and administrative leaders.
- Confirm certification binder readiness, ensuring all required documents are up-to-date and complete.
- Verify Security Risk Assessment (SRA) documentation reflects current operational risks and mitigation strategies.
- Review alignment of documentation with CMS Conditions of Participation (42 CFR §418) and HIPAA/NIST standards.
- Perform final policy reviews and confirm staff understanding of key compliance responsibilities.
- Simulate final audit interactions and survey readiness.

Outcome:

Organization leadership is fully prepared to engage with CMS surveyors, produce required documentation on demand, and demonstrate compliance with Medicare certification requirements.

"Medicare Audit Readiness"

PLAY 9:

Support CMS Survey & Real-Time Engagement

Objective: Provide confident, well-prepared representation during CMS certification audits by ensuring all compliance materials and leadership personnel are aligned for successful real-time survey engagement.

Key Actions:

- Assign a Senior Advisor to lead all audit meetings and documentation responses.
- Ensure audit documents are prepared in advance and organized within the Certification Binder.
- Deliver documentation to CMS surveyors via secure channels (e.g., encrypted email, secure file sharing).
- Designate internal representatives to answer CMS questions related to compliance, patient care, and operations.
- Maintain real-time communication between leadership, staff, and compliance team during the survey.
- Track and document all surveyor requests and responses provided.
- Establish a rapid response protocol to address any unforeseen compliance issues raised by CMS.

Outcome:

The organization will be fully prepared for real-time CMS audit interaction, capable of responding to requests efficiently, addressing surveyor concerns, and mitigating any immediate deficiencies—leading to a higher likelihood of successful Medicare certification.

"Medicare Audit Readiness"

PLAY 10:

Maintain Certification & Continuous Compliance

Objective: Sustain compliance maturity and certification status through proactive, ongoing risk, security, and governance practices. Ensure continued alignment with CMS (Centers for Medicare & Medicaid Services), HIPAA (Health Insurance Portability and Accountability Act), and NIST (National Institute of Standards and Technology) requirements.

Checklist:

- Schedule quarterly HIPAA Security Risk Assessments (SRAs).
- Review and update all compliance documentation (e.g., policies, procedures, training logs).
- Reassess technical controls and safeguards based on changes in NIST SP 800-171 and CMS protocols.
- Implement automated monitoring and alerting for system changes or threats.
- Engage governance team in quarterly strategy and compliance sessions.
- Update audit readiness binder quarterly with new evidence and artifacts.
- Provide refresher training to staff on HIPAA, CMS CoPs, and cybersecurity best practices.
- Perform internal spot checks and mock audits semi-annually.
- Track federal and state regulatory updates (CMS, OCR, ONC, etc.) and adjust compliance efforts accordingly.
- Maintain continuous collaboration with Senior Advisor or vCISO to support evolving compliance posture.

Outcome:

Maintains organizational certification status and ensures the facility is always audit-ready. Reduces risk exposure, builds compliance resilience, and protects continued Medicare funding through vigilant oversight and strategic adaptation.

HEALTHCARE COMPLIANCE CERTIFICATION PROFESSIONALS

"Medicare Audit Readiness"

PLAY 11:

Use The HCCP Compliance & Certification Packages

Objective: Align compliance strategy with the most appropriate Healthcare Compliance Certification Professionals (HCCP) service package to meet organizational readiness, risk posture, and audit demands.

Key Steps:

- Evaluate your organization's compliance maturity, staffing, and operational risk profile.
- Review all five HCCP Certification & Compliance Packages to determine the right fit.
- Use the selected package as a blueprint for compliance execution (Silver to Concierge).
- Incorporate package tools and checklists into audit preparations.
- Leverage the certification binder templates provided with each package tier.
- Ensure that assigned leaders (e.g., Senior Advisor, Compliance Officer) implement the service deliverables as scoped.

Outcome:

By selecting and utilizing the appropriate HCCP package, organizations gain structured guidance, documentation tools, and strategic support necessary to close compliance gaps, protect Medicare funding, and pass certification audits with confidence.