



THE NEW COMPLIANCE ERA: SURVIVING THE CMS CRACKDOWN

TABLE OF CONTENTS

Introduction	03
Seven Steps to Safeguard Your Organization	05
1. Complete an Internal Compliance Risk Assessment	06
2. Strengthen Clinical Documentation Practices	07
3. Evaluate Referral Source Relationships Carefully	08
4. Invest in Workforce Education and Competency Validation	09
5. Strengthen Internal Auditing and Monitoring Systems	10
6. Make Cybersecurity and Data Governance a Priority	11
7. Create a Culture of Ethical Operations and Transparency	13
Internal Compliance Risk Assessment	15
Axxess Tool Kit for Compliance	16
Axxess Business Intelligence	18
Axxess Training and Certification Resources	19
References	20

INTRODUCTION

The recent federal moratorium on new home health and hospice agency enrollments represents one of the most significant regulatory actions the federal government has taken against the post-acute care industry in years. Announced by the Centers for Medicare & Medicaid Services on May 13, 2026, the [nationwide six-month moratorium](#) temporarily stops new home health and hospice agencies from enrolling in Medicare. The action was implemented as part of a broader federal anti-fraud initiative targeting what CMS describes as widespread fraud, waste and abuse within the industry.

For current home health organizations already enrolled in Medicare, the moratorium does not stop operations or reimbursement. Existing agencies can continue providing care, billing Medicare, admitting patients and operating normally as long as they remain compliant with federal and state regulations. However, CMS has made clear that oversight will intensify during the moratorium period.

CMS has stated it will intensify investigations, site visits, claims reviews, ownership scrutiny and data analytics during the moratorium period. Agencies should expect closer examination on eligibility documentation, billing patterns, referral relationships, ownership structures and compliance programs. In high-risk states such as California, Texas, Arizona, Nevada, Georgia and Ohio, providers may face even greater regulatory attention due to previously identified fraud concerns (Fig. 1).

Operationally, the moratorium may create both opportunities and challenges for established agencies. Because no new competitors can enter the Medicare market during the freeze, current providers may temporarily experience reduced market competition and increased referral opportunities. Hospitals, physicians and discharge planners may rely more heavily on established organizations that already have Medicare certification and proven compliance histories.

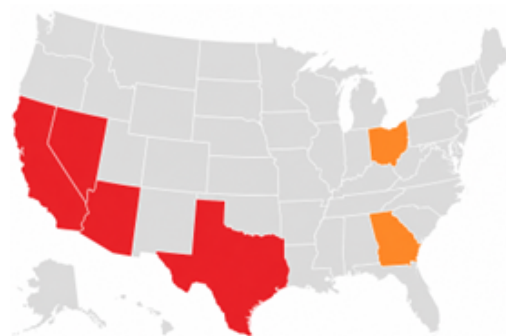


Fig. 1 - High Risk States

INTRODUCTION

At the same time, the moratorium raises concerns about access to care, workforce expansion and future growth. Industry leaders warn that blocking new agencies could [reduce care availability in rural and underserved communities](#) where provider shortages already exist. Existing agencies may experience higher patient volumes, staffing pressures and increased demand for services.

The moratorium also affects mergers, acquisitions and ownership transitions. [Certain ownership changes](#) that require new Medicare enrollment approval may now be delayed or denied during the moratorium period. Organizations pursuing expansion strategies, de-novo locations or restructuring transactions must carefully evaluate regulatory risk and timing.

Most importantly, the moratorium sends a clear message that compliance has become a strategic priority for survival and growth in home health care. Agencies must strengthen internal auditing, documentation accuracy, eligibility verification, coding integrity and staff education. Organizations with strong compliance cultures, transparent operations and effective leadership will likely be better positioned to withstand increased federal scrutiny.

Overall, while the moratorium does not shut down existing home health agencies, it fundamentally changes the regulatory environment. Current providers must prepare for more aggressive oversight, stricter enforcement and a healthcare landscape where operational integrity and compliance readiness are more important than ever.



Raianne Melton, BSN, RN

Senior Director of Clinical Services
Axxess



Seven Steps to Safeguard Your Organization

Home health agencies should respond to the current federal enforcement climate with immediate, proactive compliance and operational strategies designed to reduce regulatory, financial and reputational risk. The recent CMS moratorium and broader fraud enforcement initiatives make it clear that agencies must move beyond reactive compliance and adopt a culture of continuous oversight, documentation integrity and clinical accountability.

-
- 1 Complete an Internal Compliance Risk Assessment
 - 2 Strengthen Clinical Documentation Practices
 - 3 Evaluate Referral Source Relationships Carefully
 - 4 Invest in Workforce Education and Competency Validation
 - 5 Strengthen Internal Auditing and Monitoring Systems
 - 6 Make Cybersecurity and Data Governance a Priority
 - 7 Create a Culture of Ethical Operations and Transparency

Step 1

Complete an Internal Compliance Risk Assessment

Leadership teams should review billing practices, referral patterns, admission trends, utilization data and documentation quality to identify areas that could trigger payer scrutiny. Particular attention should be given to diagnoses supporting homebound status, skilled need documentation, plan-of-care compliance, face-to-face encounter requirements and physician certification accuracy. Agencies with unusually high utilization, rapid census growth or outlier billing patterns are more likely to attract federal attention.

ACTION STEPS:

- Perform an immediate internal audit of billing practices, referral sources, admissions, utilization trends and documentation quality.
- Review charts for documentation supporting homebound status, skilled need, plan-of-care compliance, face-to-face encounter requirements and physician certification accuracy.
- Identify unusual patterns such as rapid census growth, high utilization or billing outliers and escalate them for leadership review.
- Prioritize corrective actions for the highest-risk findings and assign clear accountability, deadlines and follow-up monitoring.

WHAT TO AVOID:

- **Ignoring outlier trends** in utilization, admissions or billing that could draw payer or regulator attention.
- **Incomplete, vague or inconsistent documentation** related to home-bound status, skilled services or physician certifications.
- Assume rapid growth or concentrated referral activity will go unnoticed if **supporting compliance controls are weak.**
- **Delaying corrective action** when internal reviews reveal risk areas that could trigger audits, denials or investigations.

Step 2

Strengthen Clinical Documentation Practices

Documentation remains the single most important defense during audits or investigations. Clinicians must clearly demonstrate medical necessity, skilled services, patient eligibility, functional limitations and measurable progress toward goals. Templates and cloned documentation should be minimized, as regulators increasingly use data analytics to identify repetitive charting patterns. Regular chart audits should be performed to ensure consistency between assessments, visit notes, OASIS documentation and claims submissions.

ACTION STEPS:

- Leverage [Axxess Training & Certification](#) platform to expedite staff training.
- Train clinicians to document medical necessity, skilled services, patient eligibility, functional limitations and measurable progress in patient-specific terms.
- Reduce reliance on templates by requiring individualized narratives that reflect each patient's condition, response to care and goals.
- Perform regular chart audits to confirm consistency across assessments, visit notes, OASIS documentation and submitted claims.
- Provide timely feedback and corrective coaching when documentation gaps, contradictions or repetitive charting patterns are identified.

WHAT TO AVOID:

- Cloned, generic or repetitive charting that **fails to show the patient's unique condition, needs and response to treatment.**
- **Inconsistencies between assessments,** visit notes, OASIS entries and claims unresolved.
- **Vague descriptions** of skilled need, functional limitations or progress **that cannot support audit review.**
- **Delaying chart review and correction** when patterns of weak or repetitive documentation begin to appear.

Step 3

Evaluate Referral Source Relationships Carefully

Federal investigators continue to focus heavily on improper financial relationships, inducements and referral arrangements. Agencies should ensure all marketing practices comply with the federal Anti-Kickback Statute and Stark Law requirements.

ACTION STEPS:

- Review referral, marketing and service contracts with healthcare counsel.
- Analyze referral data for concentration patterns and spikes.
- Document business development activities and compensation structures carefully.
- Train leadership, marketers and referral-facing staff on compliance requirements.

WHAT TO AVOID:

- **Compensation, gifts or incentives tied to referrals or admissions**
- Ignoring concentrated or **financially motivated referral patterns**
- **Outdated or unclear contracts**
- Assuming **older referral relationships are still compliant without review**

Step 4

Invest in Workforce Education and Competency Validation

Agencies should invest in workforce education and competency validation. Staff members must understand current Medicare eligibility requirements, documentation expectations, fraud and abuse laws, HIPAA protections and survey readiness standards. Ongoing training should extend beyond clinicians to intake staff, billers, schedulers and marketers. Compliance education should be routine, measurable and documented.

ACTION STEPS:

- Develop a documented training program covering Medicare eligibility, documentation standards, fraud and abuse laws, HIPAA and survey readiness for all relevant roles.
- Validate competencies through testing, observation or case-based review and maintain records showing completion and follow-up.
- Extend compliance education beyond clinicians to include intake, billing, scheduling and marketing staff whose work affects agency risk.
- Track training completion, identify knowledge gaps and provide refresher education when policies, regulations or audit findings change.

WHAT TO AVOID:

- **Treating compliance education as a one-time orientation task** instead of an ongoing operational requirement.
- Limiting training to clinicians while **excluding staff in intake, billing, scheduling or marketing roles.**
- Undocumented or informal training that **cannot demonstrate staff competency during audits or surveys.**
- **Ignore recurring knowledge gaps or policy changes** that require immediate retraining and leadership follow-up.

Step 5

Strengthen Internal Auditing and Monitoring Systems

Effective agencies are using predictive analytics, utilization dashboards and compliance scorecards to identify trends before regulators do.

ACTION STEPS:

- Implement routine pre-bill audits, ADR tracking, denial analysis and PEPPER monitoring to identify compliance vulnerabilities early.
- Use dashboards, predictive analytics and compliance scorecards to monitor utilization, billing, documentation and operational trends.
- Establish a formal corrective action process with assigned owners, deadlines and follow-up validation when issues are identified.
- Report key risk indicators to leadership regularly so emerging patterns are addressed before they escalate into audits or payment issues.

WHAT TO AVOID:

- **Relying only on reactive reviews** after denials, ADRs or complaints have already exposed a problem.
- **Ignoring utilization or billing trends** simply because claim volume remains high or payments continue.
- **Incomplete corrective action plans** that lack ownership, deadlines or evidence of follow-through.
- **Keeping audit findings siloed from leadership** when trends may signal broader operational or compliance risk.

Step 6

Make Cybersecurity and Data Governance a Priority

As agencies increasingly adopt AI tools, remote monitoring and electronic documentation systems, leaders must ensure secure handling of protected health information and appropriate oversight of automated workflows. Weak cybersecurity practices can create both compliance and operational risk.

ACTION STEPS:

- Conduct and document a cybersecurity risk analysis that maps where electronic protected health information is created, stored, transmitted and accessed across AI tools, remote monitoring platforms, mobile devices and documentation systems.
- Strengthen technical safeguards by enabling multifactor authentication, role-based access, encryption for data at rest and in transit, routine patching and audit logging for systems handling protected health information.
- Establish governance for AI and automated workflows by defining approved use cases, human review checkpoints, output validation and clear accountability for decisions that affect documentation, care coordination or billing.
- Review vendors, business associates and connected technology partners to confirm security controls, breach notification obligations, access restrictions and contract terms align with HIPAA and organizational standards.
- Train staff regularly on phishing, password hygiene, secure remote access, appropriate use of AI tools and breach escalation procedures and test the incident response plan through tabletop exercises.

Step 6

Make Cybersecurity and Data Governance a Priority

WHAT TO AVOID:

- **Using unapproved AI applications**, consumer messaging tools or personal devices to handle protected health information without documented security review and authorization.
- **Relying on shared logins**, weak passwords or broad user permissions that make it difficult to verify who accessed, changed or transmitted sensitive data.
- **Assuming automated outputs are accurate or compliant without human oversight**, especially when technology influences documentation, patient monitoring, coding or operational decisions.
- Onboarding vendors or digital tools **without evaluating business associate requirements**, data-sharing practices, breach response expectations and technical safeguards.
- **Treating cybersecurity as only an IT issue**; delaying risk remediation, staff training or breach response planning can quickly become both a compliance and patient care problem.

[cont]

Step 7

Focus on Preserving Mission-Driven Care

Agencies with engaged leadership, empowered compliance officers and strong interdisciplinary communication are better positioned to withstand scrutiny. Compliance should not be viewed as a department—it should be integrated into everyday clinical and operational decision-making.

ACTION STEPS:

- Demonstrate visible leadership commitment by reviewing compliance data regularly, discussing ethical expectations in operations meetings and reinforcing that compliance responsibilities apply to every department.
- Empower the compliance officer with direct access to leadership, authority to escalate concerns and resources to monitor risks, investigate issues and coordinate corrective actions.
- Create structured interdisciplinary communication channels such as regular compliance huddles, case reviews and cross-functional meetings that connect clinical, billing, intake, operations and leadership teams.
- Build accountability into daily workflows by incorporating compliance checks into hiring, onboarding, documentation review, referral management, billing oversight and incident follow-up.
- Encourage transparent reporting by maintaining non-retaliation practices, giving staff clear ways to raise concerns and tracking reported issues through resolution and leadership follow-up.

Step 7

Focus on Preserving Mission-Driven Care

WHAT TO AVOID:

- **Treating compliance as a stand-alone department** that is responsible for fixing issues without operational ownership from clinical, billing, intake and leadership teams.
- **Sidelining the compliance officer**, delay escalation of concerns or create reporting structures that weaken independent oversight.
- **Poor communication between disciplines** that allows documentation issues, billing risks, patient care concerns or survey findings to remain siloed.
- Tolerating retaliation, fear-based management or informal workarounds that **discourage staff from reporting concerns or disclosing problems early.**
- **Waiting for an audit**, denial trend or investigation before addressing ethical or operational weaknesses that leadership already sees emerging.

In the current environment, agencies that wait for an audit, investigation or payment suspension before acting may face significant financial and reputational consequences. Organizations that prioritize documentation integrity, operational transparency, compliance education and proactive monitoring today will be far better positioned to navigate increasing federal oversight and sustain long-term success in home health care.

Addendum A

Internal Compliance Risk Assessment

AREA	KEY INDICATORS	RISK LEVEL	ACTION
Billing and Utilization	Outlier billing patterns, rapid census growth, high utilization, ADRs, denials or PEPPER targets trending upward	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Conduct focused claims and utilization audit, validate documentation support and escalate outliers for leadership review
Clinical Documentation	Weak access controls, shared logins, unapproved apps, missing encryption, vendor oversight gaps or untested incident response plan	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Perform targeted chart reviews, retrain clinicians and require corrective documentation follow-up
Referral Source Relationships	Concentrated referrals, unusual admission spikes, unclear contracts or compensation tied to admissions or volume	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Review contracts and compensation models, analyze referral data and obtain legal/compliance review where needed
Workforce Training and Competency	Incomplete training records, recurring staff errors, inconsistent onboarding or role-based compliance gaps	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Update training matrix, validate competencies and assign refresher education for high-risk roles
Internal Auditing And Monitoring	No routine audit calendar, unresolved findings, limited dashboard visibility or delayed corrective action follow-up	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Implement monthly monitoring, track corrective actions to closure and report key indicators to leadership
Cybersecurity And HIPAA Risk	Weak access controls, shared logins, unapproved apps, missing encryption, vendor oversight gaps or untested incident response plan	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Perform security risk review, tighten access controls, confirm business associate safeguards and test breach response procedures
Leadership Oversight And Culture	Limited compliance reporting to leadership, siloed communication, weak escalation pathways or fear of reporting concerns	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Schedule leadership review of compliance metrics, reinforce non-retaliation and require cross-functional follow-up on identified risks

Addendum B

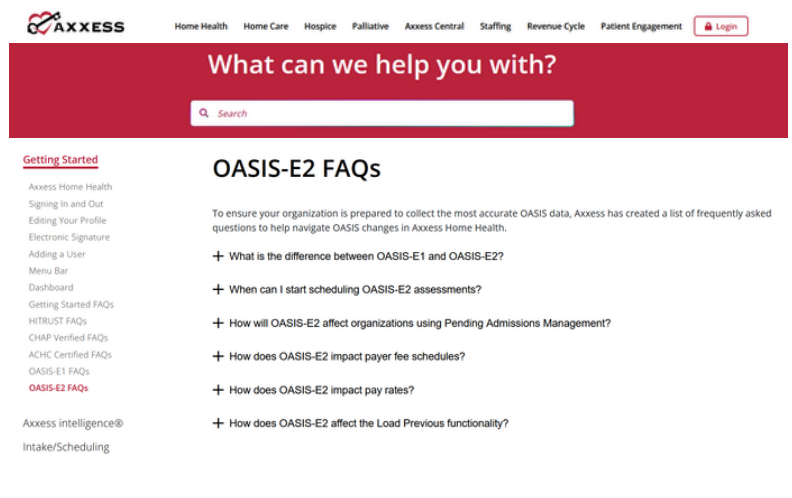
Axxess Tool Kit for Compliance

Axxess provides a robust suite of home health regulatory and compliance tools and assets that support home health organizations all in one location.

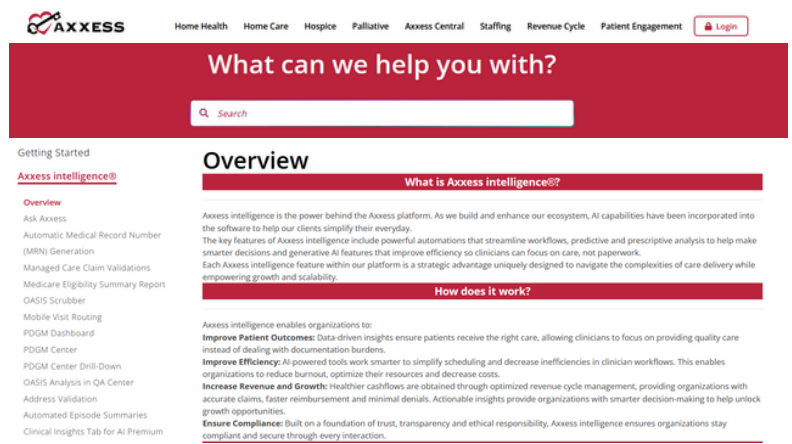
1 [Axxess HomeHealth Help Center](#)



2 [Axxess OASIS-E2 FAQs](#)



3 [Axxess intelligence®](#)



Axxess Tool Kit for Compliance

AXXESS INTELLIGENCE HIGHLIGHTS

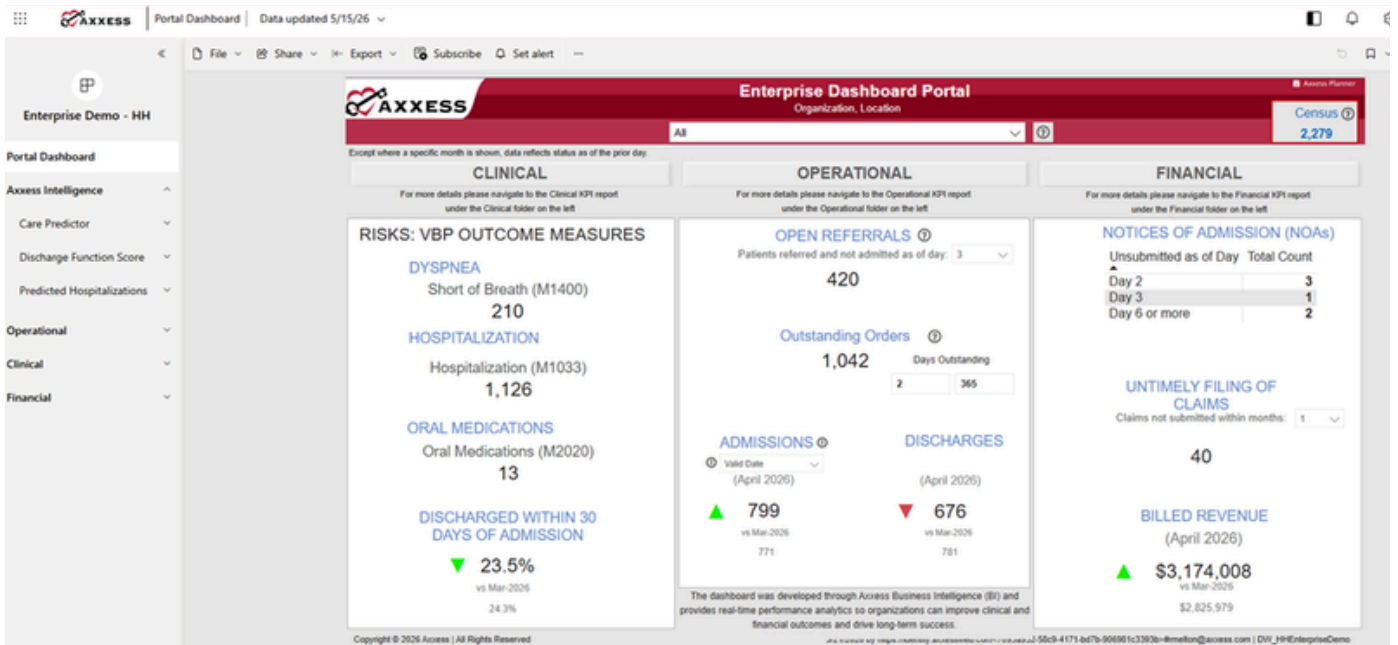
4 Axxess PDGM Center

5 Axxess QA Center OASIS Analysis



Addendum C

Axxess Business Intelligence



[Axxess Business Intelligence](#) (BI) is a healthcare analytics and reporting solution within the Axxess software ecosystem, designed primarily for home health, hospice and home care organizations. It transforms large volumes of clinical, operational and financial data into actionable insights to support better decision-making.

Talk To Our Team

Addendum D

Axxess Training and Certification Resources

[Axxess Training and Certification](#) directs your team for training, updates and industry knowledge.



The Maxim Memo

Serving up the freshest, most impactful industry news in the homecare and hospice world. Stay in the know with industry insights you can use.

[Read Now](#)

Resources

Engage with in-depth digital resources that can set you up for success.

[Learn More](#)

Blogs

Learn from industry thought leaders about a variety of care at home topics.

[Learn More](#)

Product Updates

Explore new and upcoming software features and product updates:

[Home Health](#)
[Home Care](#)
[Hospice](#)
[Palliative](#)

[Help Center](#)







HOPE

The Hospice Outcomes and Patient Evaluation (HOPE) goes into effect on October 1, 2025. Learn imperative strategies to ensure organizational success.

[Learn More](#)

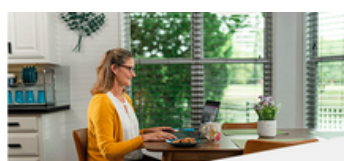





Regulatory Tools and Resources

Stay up to date with the regulatory changes that may affect the care at home industry.

[Learn More](#)





Blogs

Learn from industry thought leaders about a variety of home care topics.

[Learn More](#)

REFERENCES

- [Centers for Medicare & Medicaid Services](#)
- [American Hospital Association](#)