ahia
Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org Journal of the Association of Healthcare Internal Auditors Vol. 45, Number 2, 2026

Maintaining Business Continuity After a Natural Disaster

Learn from a compliance officer's real-life perspective

page 9

High-Stakes Deception

A healthcare internal auditor's guide to business email compromise

page 16

Follow the Money

Evaluate enterprise risk across the healthcare revenue chain

page 21

Face the Future with Confidence®

From insight to action in enterprise margin assurance

How Protiviti's Enterprise Margin Solutions support insight into margin performance

Healthcare organizations face sustained margin pressure amid growing clinical, operational and regulatory complexity. Internal Audit plays a critical role in validating whether margin improvement initiatives are well governed, data driven and delivering sustainable results.

Protiviti's Enterprise Margin Solutions (EMS) combine advanced analytics, selective use of AI and automation-enabled audit techniques with deep healthcare expertise. EMS helps Internal Audit identify where margin is at risk, validate management's improvement initiatives and independently assess whether analytics, automation and AI are appropriately governed and delivering measurable value.

KEY CAPABILITIES

- **Margin Risk and Leakage Identification**: AI-enabled analytics identify revenue leakage, payment variability, cost misalignment and underperforming initiatives.
- **Validation of Opportunity and Impact:** Benchmarking and claims-level analytics validate assumptions, prioritization and projected financial impact.
- **Automation and AI Enablement and Governance:** Evaluating where automation and AI are used, where opportunity exists and whether capabilities are governed and delivering value.
- **Technology Value and Analytics Maturity:** Assessing how effectively EHR, ERP, financial systems, analytics, AI and automation are embedded into workflows.

Scan here to learn how Protiviti brings deeper insight to Internal Audit and across the enterprise.

protiviti®

Global Business Consulting

contents

Vol. 45, Number 2

FROM THE EDITOR

Is This for Real?

By Jen Conley

"I've got to know. Is this for real? Oh, woah."
– lyrics by O'Bryan

I'm an HGTV junky who recently visited Laurel, Mississippi, the site of *Home Town*, a home renovation and design reality television series. Since the show's 2016 premiere, I've been enamored with the idea of the picturesque small town with tree-lined streets, charmingly restored Craftsman-style homes, and a vibrant downtown. But, because I'm an auditor at heart, I had to find out for myself if it's for real. Similarly, our *New Perspectives* authors help us figure out what's for real.

Few reality shows push the boundaries of bad behavior like Bravo's *Real Housewives*. But a franchise expansion into the real organizations of ethical collapse could keep pace. In a four-part series, Marianne Jennings explains how ethically failed companies have been following the same script for more than 20 years. In this installment, she introduces us to bigger-than-life Chief Executive Officers and the supporting characters who allow their bad behaviors to thrive.

Business email compromise (BEC) fraud is all about fooling employees about what, and who, is real. It's a scam that continues to hit healthcare organizations. Unlike reality TV stars, BEC scammers prefer quiet anonymity. Vic Hartman explains how BEC happens and what controls should be implemented and audited to prevent it. Among other insights, Vic helps us understand the legal reality of who bears the liability of BEC fraud and the importance of a timely response.

When AHIA members prepare to address fraud and other risks, they can rely on the Marketing Committee to keep them informed about available resources and upcoming events. In her Chair column, Heather Zundel introduces us to some members of this committee and their evolving work.

For audit planning and metric reporting, auditors commonly categorize risks as financial, operational, IT, or compliance. But in real life, enterprise risks do not confine themselves to neatly defined silos. This is especially true across the healthcare revenue cycle. The writers team from RubinBrown shows auditors how to follow the money through the full revenue cycle so they don't unwittingly limit their risk assessments.

continued on page 8

NEW PERSPECTIVES
Published by AHIA, Inc.

FROM THE CHAIR

Meet the AHIA Marketing Committee

By Heather Zundel

AHIA has great educational events coming up, including free-to-members webinars and Tech Talks. Our biggest event of the year, the 2026 AHIA Annual Conference, will be held virtually August 24-28, so you can join from anywhere. With so much happening across AHIA and plenty of news to share, our Marketing Committee plays an essential role in keeping members informed and engaged. I recently connected with committee volunteers to ask them a few questions about their work.

Q: What should readers know about the committee?

A: The Marketing Committee has an interesting history as it was first a social media subcommittee under the Membership and Awards Committee (MAC), until it formed as a standalone committee. Our purpose is to elevate AHIA's presence, strengthen engagement, and ensure that members clearly understand the value AHIA delivers throughout the year.

Our committee focuses on:

- Marketing strategy and campaigns: We help develop, implement, and monitor marketing initiatives across AHIA's owned, shared, and paid channels. This includes member emails, website content, social media (LinkedIn), digital marketing partnerships/advertising, and conference promotions.
- Social media management:
  - We curate monthly Industry News posts on LinkedIn to keep members informed about emerging risks, regulatory developments, information technology, and healthcare audit trends.
  - We participate as a Champion for the National Cybersecurity Alliance Cybersecurity Awareness Month campaign, and other awareness campaigns throughout the year.
  - We help support Talley (AHIA's contracted association management company) in creating posts for other committees (e.g., Publications, Certifications, MAC, Virtual Learning, Roundtables & Regionals) when needed.
- Website oversight: We monitor the AHIA website to advise Talley on keeping it functional, easy to use, and updated in appearance.
- Marketing materials quality control: We ensure that all AHIA marketing materials remain current, visually consistent, and aligned with modern design and social standards.

Marketing committee members are excited to engage with membership via conference posts, industry news posts, and more.

Q: Marketing Committee members were a high-energy cheer squad for the 2025 annual conference. Could you remind us of some of the activities you led? We'd also like to hear how you'll engage members during the 2026 virtual conference.

A: For the 2025 Annual Conference, a Marketing Committee liaison was added to the Conference Committee to:

- Develop and schedule a multi-month LinkedIn campaign to highlight speakers, sessions, and the overall theme
- Create preconference engagement content to build anticipation and spotlight sponsors
- Coordinate with the Conference Committee and Talley to ensure consistent messaging and branding
- Provide giveaways for the Exhibitor Passport Card, trivia night, new member breakfast, and LinkedIn engagement contests
- Support sponsor visibility and amplify member engagement
- Coordinate a trivia night (see photos below), hosted by one of our committee members, and LinkedIn engagement contests

For the upcoming 2026 AHIA Annual Conference, we're focusing on:

- Exploring new formats for virtual attendee engagement, such as spotlights on content tracks, what to expect posts, and interactive polls on LinkedIn
- Delivering engagement-driven content across LinkedIn and Cadmium (our event platform)
- Ensuring messaging consistency and strong sponsor visibility in a virtual setting

We're still coming up with engaging online contests and are open to suggestions!

Q: What else is the Marketing Committee working on that members should know about? What should members watch for?

A: If they're not already followers, they should check out our LinkedIn page (linkedin.com/company/ahia), where we post industry news articles and updates about webinars, roundtables, conferences, certification, and other benefits of AHIA. Members should watch for new images/graphics and more consistent LinkedIn posting.

We are excited to engage with membership via conference posts, industry news posts, and more. We hope members will follow our page, like, share, and engage with content to help make our posts visible to our followers.

"In business, words are words, explanations are explanations, promises are promises, but only performance is reality."
- Harold S. Geneen, former president and CEO of ITT

Why do you volunteer?

The Marketing Committee lets me use my creative and strategic skills to help strengthen AHIA's voice and support members. My favorite part is collaborating with a talented, energetic group across AHIA who care deeply about advancing the profession and telling AHIA's story in meaningful ways. - Vicky Gabbai, Marketing Committee Chair

I volunteer for the Marketing Committee/AHIA to give back to the community while expanding my professional network. Through my involvement, I've developed valuable skills such as effective communication, strategic thinking, and collaboration. These experiences enhance my professional growth and contribute meaningfully to my career development. My favorite part of serving on the committee is knowing we are helping increase awareness of AHIA to the broader profession. - Brandon Passon, Marketing Committee Member

Q: Are you looking for more volunteers? Who should readers contact?

A: The Marketing Committee is seeking volunteers to support initiatives that strengthen our brand, enhance member communications, and expand our digital presence. Volunteers may assist with one or more of the following activities:

- Keeping AHIA marketing materials current
  - Help ensure AHIA materials reflect the latest branding, design standards, and social media best practices
  - Review and update member facing content such as the AHIA website, webinars, TechTalk materials, *New Perspectives* articles, and other publications
- Supporting marketing for prospective members
  - Assist with creating and improving website and LinkedIn content aimed at attracting new members (it's a plus if you dabble in Canva or love creating images!)
  - Help ensure messaging clearly communicates the value of AHIA membership
- Branding guide coordination and awareness
  - Support coordination related to the AHIA branding guide (this is currently maintained by Talley).
  - Help increase awareness of branding requirements across AHIA committees.
  - Serve as a resource or liaison to other committees on proper branding of their materials.
- Online advertising and revenue initiatives
  - Assist in AHIA's efforts to increase revenue through online advertising
  - Support coordination with MultiView (digital publishing and marketing company) related to AHIA.org web ads, retargeting, and newsletter advertising
  - Work with the AHIA website administrator to identify and evaluate appropriate ad placements
- Creating images and visual content using Canva or other creative tools

These opportunities are flexible and can be tailored to volunteers' interests, availability, and skill set. Interested volunteers can contact Vicky Gabbai, Marketing Chair (vgabbai1@jhu.edu) or use the Connected Community Volunteer form.

I appreciate that the Marketing Committee is continually exploring new ways to elevate AHIA's voice and improve communication, engagement, and the member experience. The committee members appreciate every AHIA member who engages with their content, shares posts, or provides input. If you have ideas to share, please reach out to the Marketing Chair. **NP**

Interested in volunteering?

Find AHIA committee charters and membership rosters at https://ahia.org/committees/. Learn about and respond to committee volunteer opportunities at https://community.ahia.org/new-page2/volunteer-pages-bucket.

The committee members appreciate every AHIA member who engages with their content, shares posts, or provides input.

Is This for Real?

continued from page 4

Hopefully, most of us will only ever have to imagine if our healthcare organizations could function during a major natural disaster. But the harsh reality is that the frequency and severity of natural disasters keep increasing. To help us prepare for the worst, Jeff Pigott offers a real-life, first-hand reflection on what it took to endure Hurricane Ian. He knows that healthcare business continuity takes more than policies and emergency preparedness plans. He offers his knowledge, and even a checklist, to help mitigate this risk.

Finally, I want to share the exciting news that *New Perspectives* recently won a 2026 Azbee Awards of Excellence National Silver Award. You can take a second look at Sonda Kunzi's award-winning article in this issue.

The Azbee Awards honor the best in B2B media, recognizing outstanding work by business, trade, association, and professional publications. More than 740 entries were judged by experienced B2B editors, freelancers, designers, and journalism professors. They agreed that Sonda did a fantastic job explaining how auditors can close the gap between behavioral health service documentation and revenue integrity. Here are more details on the winning article and publishing team, including our behind-the-scenes editing and graphics team.

Category: All Content - How-To Article
Title of Entry: Behavioral Health Billing Compliance
Sonda Kunzi, Author; Jen Conley, Editor in Chief; Leslie Shivers, Editor; Steve Dunn, Design and Graphics

Please join me in congratulating and thanking Sonda, Leslie, and Steve for their outstanding contributions to *New Perspectives*!

If you're wondering whether Laurel, Mississippi, lived up to my *Home Town* hype, it did—mostly. Its vibrant downtown closed at five pm, and the charming historic district is quite small. But I was enchanted all the same. Really. **NP**

"The first responsibility of a leader is to define reality. The last is to say thank you. In between the two, the leader must become a servant and a debtor."
– Max De Pree, businessman and writer

About *New Perspectives*

New Perspectives (NP) is a refereed and peer-reviewed journal that focuses on up-to-date information, trends and issues in the healthcare industry and the internal auditing profession. Practical guidance is provided on risks and controls that can be applied by internal audit professionals in their jobs.

NP is published quarterly in an electronic format. Issues are accessed by online viewing or through download. See the NP archives at https://ahia.org/new-perspectives-archive/ (login required).

For author guidelines or to submit an article, please contact Jen Conley at 801-803-2361 or Jen.ahia.np@gmail.com.

Yearly subscription rates, including postage, are $100, payable in U.S. funds. No refunds or cancellations. Send publication and subscription inquiries, address changes and other inquiries to: Association of Healthcare Internal Auditors, Inc., 19 Mantua Road, Mount Royal, NJ 08061 USA. Phone 856-554-1083 or email, *info@ahia.org*.

Maintaining Business Continuity After a Natural Disaster

Learn from a compliance officer's real-life perspective

By Jeff Pigott

Business continuity audits should evaluate how organizations care for people—not just how they preserve operations. Living through Hurricane Ian showed me that regulatory compliance, ethical leadership, and workforce resilience are inseparable during a crisis.

Business continuity often involves policies, risk assessments, and emergency preparedness plans. When disaster strikes, teams test those documents in real time—under pressure, uncertainty, and loss. Hurricane Ian reminded me that compliance obligations do not pause during crises; they intensify.

This article reflects on maintaining business continuity during Hurricane Ian from the perspective of a healthcare compliance officer. It highlights regulatory responsibilities, operational constraints, and audit lessons that continuity leaders can apply in healthcare and other regulated industries.

Regulatory expectations do not stop for disasters

Healthcare organizations that participate in Medicare and Medicaid must maintain comprehensive emergency preparedness programs. Federal regulations under 42 CFR Part 482 require all-hazards risk assessments, emergency plans, communication protocols, and training and testing programs. These requirements apply not only to hospitals but also to rural health clinics (RHCs) and federally qualified health centers (FQHCs), which also comply with applicable federal, state, and local emergency preparedness rules.

Could it happen to you?

Rebuild by Design's Atlas of Accountability shows that 95.5% of U.S. residents live in counties with recent disaster declarations. Page one of their Atlas of Accountability Fact Sheet, presented at Appendix B, details disaster declarations across county and congressional districts from 2011 to 2024.

From an audit perspective, emergency preparedness is not a paper exercise. Regulators expect plans to be executable, scalable, and responsive to real world conditions—conditions that rarely follow forecasts or assumptions.

Organizational context: Scale matters in crisis

At the time of Hurricane Ian, I served as Vice President of Compliance and Internal Audit at Lee Health in Fort Myers, Florida. The system included multiple acute care hospitals, specialty hospitals, a children's hospital, a rehabilitation hospital, and more than 100 outpatient sites. Approximately 14,000 employees and more than 900 physicians supported those operations.

This scale magnified every operational decision during the storm. Auditors evaluating business continuity should consider organizational size, geographic dispersion, and dependency on workforce availability as core risk factors.

Preparation: What plans often miss

Lee Health established core preparedness capabilities before Ian, including an incident command structure, staff training, evacuation planning, communication protocols, resource management, and continuity plans for critical services. Technology supported many of these controls, but the storm quickly proved that teams also needed durable manual alternatives.

Hurricane Ian revealed that even well designed plans may not fully address:

- Rapidly shifting forecasts
- Geographic isolation
- Staffing constraints
- Communication failures
- Financial strain during extended outages

Teams make hundreds of time-sensitive decisions during an event.

For auditors, this underscores the importance of stress testing emergency plans against worst case scenarios rather than likely ones.

To prepare for that kind of disruption, leaders must define and document a decision tree before a crisis. Teams make hundreds of time-sensitive decisions during an event: they shut down services, alter workflows, redirect patients, adjust staffing, and approve emergency purchases. When leaders pre-authorize thresholds and delegations, they reduce delays and keep decisions consistent across sites.

Auditors can test this readiness by reviewing training records, drill outcomes, downtime job aids, and incident command logs from prior events. They can also observe functional exercises that force teams to operate without normal tools—no shared drives, limited email, and degraded electrical and/or phone service. When staff cannot demonstrate a manual workflow for registration, medication administration, or documentation, auditors should flag the gap as an operating risk, not just a training preference.

Compliance teams should also plan for privacy and security during downtime. Staff may rely on paper notes, ad hoc phone calls, and improvised workspaces during an evacuation or unit consolidation. Leaders should provide clear guidance on minimum necessary disclosures, secure storage for paper records, and controlled access to patient information when normal badge systems and cameras fail.

Forecasting: Risk versus reality

In the days leading up to landfall, official forecasts focused attention on Tampa Bay, with Fort Myers largely absent from early National Hurricane Center statements. Less than 24 hours before full impact, Ian's path shifted south and compressed the organization's decision timeline.

Auditors should recognize that reliance on forecasts alone can create a false sense of security, and organizations should avoid designing continuity around forecast precision. Leaders need clear triggers—such as expected wind fields, storm surge probabilities, or utility pre-shutoff notices—that prompt early actions even when the exact track remains uncertain. Early action buys time for staffing, supply staging, clinical service adjustments, and patient movement.

Auditors can evaluate this capability by reviewing how leaders set triggers, who approves escalation steps, and how quickly teams execute them. A strong program documents time-stamped decisions, shows consistent criteria across facilities, and demonstrates that leaders can reverse or scale decisions safely as conditions change. A weak program depends on informal judgment that varies by leader and site.

The event: Making compliance decisions under extreme conditions

On September 28, 2022, Hurricane Ian made landfall near Fort Myers as a Category 4 storm and caused catastrophic damage. Nearly all of Lee County lost power. Water systems suffered damage and contamination risks. Communications infrastructure failed across large areas, which reduced situational awareness, slowed coordination, and forced leaders to run hospitals like field operations. Teams managed sanitation workarounds, secured potable water, and controlled access to clinical spaces when building conditions degraded. Leaders also balanced immediate clinical needs against longer-term safety concerns, such as infection control, waste disposal, and environmental hazards.

Technology risk intensified during the response. Power instability and limited connectivity can interrupt electronic health records, telemetry, and identity systems. When teams switch to manual workarounds, they often create new privacy and security exposure through paper records, unsecured devices, and improvised communications. Compliance and IT leaders should plan for this shift and provide clear guardrails that keep care moving while limiting avoidable exposure.

As another audit example, test whether emergency purchasing controls work under crisis speed. Select a sample of storm-related purchases (for example, fuel deliveries, water, temporary services, and critical supplies) and trace each item from request to approval to receipt. Confirm that leaders used documented emergency authorities, captured vendor terms, and reconciled invoices after operations stabilized. When teams bypass normal procurement systems, auditors should verify that leaders still prevented duplicate ordering, controlled price spikes, and documented why they chose each vendor under constrained conditions.

Supply chain constraints also reshaped control expectations. Leaders needed fuel, water, food, linens, pharmaceuticals, and contracted services at the same time vendors faced road closures and their own outages. A mature continuity program pre-identifies emergency suppliers, establishes receiving locations, and sets purchasing controls that remain workable during a crisis. Auditors should confirm that emergency purchasing still requires accountability, documentation, and post-event reconciliation.

As the hurricane advanced, Lee Health experienced loss of water pressure and sanitation systems, contaminated community water supply, sporadic cellular communication, and storm surge that impacted hospital facilities.

Compliance leaders supported real-time decisions about patient acuity, evacuation feasibility, resource allocation, and regulatory obligations while leaders protected patient safety and workforce well-being. We focused on two disciplines: We helped teams act decisively, and we helped them document decisions clearly enough to withstand post-event scrutiny.

Evacuation: Continuity of care when moving patients

In the immediate aftermath, Lee Health coordinated with local, regional, and national partners to evacuate patients to hospitals across Florida and neighboring states. We evacuated Golisano Children's Hospital first, including 67 NICU infants transferred within 24 hours without an adverse event. We then evacuated two additional hospitals and moved more than 400 patients over several days.

Evacuation requires more than transportation. Teams must maintain patient identification, medication continuity, clinical handoffs, and accurate documentation while conditions change minute by minute. Leaders also need current transfer agreements and clear criteria that define when they shelter in place versus evacuate, especially for high-acuity units such as NICUs, ICUs, and behavioral health.

Auditors can test evacuation readiness by requesting transfer logs, bed-tracking records, receiving facility confirmations, and time-stamped decisions from incident command. They should also test how the organization protects patient information during transfers and how it reconciles paper documentation back into systems after normal operations resume. Those artifacts demonstrate whether the organization can execute continuity of care, not just describe it in policies.

From an audit perspective, evacuation performance depends on controls that remain functional during crisis conditions:

- Coordinate with external partners and activate mutual-aid and transfer agreements quickly
- Maintain decision logs and patient movement documentation that leaders can review and defend later
- Sustain minimum clinical, privacy, and safety controls while teams operate on manual processes

When auditors scope continuity, they should include evacuation as a cross-functional process that touches clinical operations, IT, privacy, facilities, transportation, and external communications. Teams can only execute safely when staff responsible for each function understand their role and share the same operational picture.

Workforce resilience: Learn from history

Leaders carried a critical lesson from Hurricane Irma in 2017. During the aftermath of that storm, some leaders terminated employees who could not report to work quickly, which triggered reputational damage and rehiring issues. During Ian, leadership committed to more flexibility and communicated that commitment clearly.

The organization's relief efforts restored operational capacity. When employees lose housing, transportation, childcare, or basic supplies, attendance policies alone cannot restore

A weak business continuity program depends on informal judgment that varies by leader and site.

Communications infrastructure failed across large areas, which reduced situational awareness, slowed coordination, and forced leaders to run hospitals like field operations.

staffing. Leaders must address practical barriers so staff can return safely and sustainably.

Workforce continuity also requires structured controls: leaders must track who is available, redeploy staff across sites, confirm credentials and competencies, and manage fatigue during extended response periods. Auditors can test these controls by reviewing staffing rosters, redeployment records, just-in-time training materials, and evidence that leaders monitored rest cycles and safety incidents.

Things that were done differently after Hurricane Ian that provided audit opportunities:

- Paid all employees for three weeks regardless of work status
- Reimbursed insurance deductibles for damaged vehicles
- Provided transportation assistance
- Offered legal and FEMA claim support
- Supplied basic necessities such as scrubs, food, and transportation support

Auditors should treat workforce resilience as a core continuity objective. If the organization cannot locate staff, communicate expectations, provide basic support, and redeploy qualified personnel, every other continuity control degrades quickly. Effective programs plan for workforce disruption with the same rigor they apply to power, water, and IT.

Community impact: External dependencies extend organizational risk

Hurricane Ian disabled television and radio stations and disrupted a meaningful portion of regional wireless infrastructure, which complicated efforts to locate and support employees and to coordinate logistics across the community.

Leaders often underestimate how quickly external dependencies fail. Roads close, fuel becomes scarce, and vendor delivery routes collapse. Even when a facility remains structurally sound, it can lose practical access to supplies, staff, and information. Continuity planning must therefore include the community environment, not just the enterprise footprint.

Auditors can add value by mapping the organization's external dependencies—power, water, fuel, roads, telecom, and public messaging—and by verifying practical workarounds for the first 72 hours. Teams should maintain alternate communications methods (i.e., text messages have a better chance of reaching recipients than a phone call when cellular networks may be compromised), offline contact directories, and predefined rally points. They should also document which leaders coordinate with emergency management and how they share updates internally.

Auditors should incorporate community infrastructure and utility dependencies into continuity risk assessments.

Be better prepared: Lessons for auditors and compliance leaders

Auditors add the most value when they translate a disaster story into testable criteria. After Ian, I returned to the same question: Would our controls still work if we lost power, clean water, and reliable communications for days? Most organizations answer that question with policies. Strong organizations answer it with practiced behaviors, delegated authority, and evidence that leaders can make ethical decisions under pressure.

- Audit the first 72 hours: Test how teams operate before outside support restores utilities, logistics, and staffing.
- Control emergency purchasing: Enable rapid procurement while preserving documentation, approvals, and post-event reconciliation.
- Map community dependencies: Validate workarounds for fuel, water, roads, and telecom so continuity does not collapse when the community fails.
- Close the loop: Run an after-action review with owners, deadlines, and retesting so the organization confirms improvement before the next event.

These lessons apply beyond hurricanes and beyond healthcare. Floods, wildfires, cyber incidents, and prolonged utility failures create the same continuity challenge: Leaders must protect people and information while they sustain critical services with fewer resources and less certainty.

Conclusion

Hurricane Ian reinforced the role compliance officers and auditors play during crises. We do not enforce rigid rules in a vacuum; we help leaders make ethical, defensible decisions while operations degrade. We also help teams preserve evidence and tell an accurate story later, when regulators, boards, insurers, and communities ask what happened and why.

Organizations measure preparedness by how they perform under worst-case conditions, not by how polished their binders look during calm weather. Leaders should build programs that work when utilities fail, communications fragment, and staff face personal loss. Auditors can reinforce this mindset by testing operating effectiveness, not just policy completeness. The checklist at Appendix A reflects lessons informed by Hurricane Ian.

To strengthen continuity now, start with three actions: 1) validate decision triggers and delegated authorities, 2) run a functional downtime exercise that forces manual operations, and 3) confirm that evacuation, communications, and workforce support plans produce usable documentation. These steps build readiness and give leadership credible assurance before the next event tests the organization.

Jeff Pigott is Compliance Director and Privacy Officer at Summit Medical Group in Knoxville, Tennessee. He has 40 years of experience, including 30 in healthcare. You can contact him at pigottjeffrey@gmail.com or on LinkedIn.

Evacuation performance depends on controls that remain functional during crisis conditions.

Appendix A

Auditor Checklist: Business Continuity and Emergency Preparedness

This checklist is designed to help auditors evaluate whether an organization's emergency preparedness and business continuity program is operationally effective—not merely compliant on paper.

1. Regulatory compliance and governance

- ☐ Does the organization maintain a documented emergency preparedness program that meets Medicare and Medicaid Conditions of Participation, including all-hazards risk assessments, emergency plans, communication plans, and training/testing programs?
- ☐ Are emergency preparedness requirements clearly extended to all applicable entity types (e.g., hospitals, RHCs, FQHCs), with evidence of compliance across the enterprise?
- ☐ Is executive leadership formally involved in emergency preparedness governance and activation decisions?

2. Risk assessment and planning assumptions

- ☐ Does the organization's risk assessment account for forecast uncertainty, including rapidly shifting disaster paths and incomplete early warnings?
- ☐ Are plans stress-tested against worst-case scenarios rather than most likely events (e.g., loss of utilities, water contamination, infrastructure failure)?
- ☐ Does the plan address risks related to geographic isolation, staffing shortages, and communication failures?

3. Command center and incident management

- ☐ Is there a documented command center structure with clear activation criteria and escalation protocols?
- ☐ Is there evidence that the command center can be partially or fully activated in advance of an event based on emerging risk signals?
- ☐ Are roles and responsibilities clearly defined for compliance, legal, operations, and clinical leadership during emergencies?

4. Communication resilience

- ☐ Does the organization maintain redundant communication methods to operate during widespread cellular, broadcast, and internet outages?
- ☐ Is there a documented process for locating and accounting for employee safety when traditional communication channels fail?
- ☐ Are communication protocols tested under conditions that simulate infrastructure failure?

5. Patient care continuity and evacuation

- ☐ Are patient evacuation plans documented, scalable, and coordinated with external agencies and receiving facilities?
- ☐ Is there evidence of decision-making criteria for assessing patient acuity and prioritizing evacuations during emergencies?
- ☐ Are evacuation outcomes tracked, including adverse events, to support post-incident review and regulatory scrutiny?

6. Workforce resilience and ethical considerations

- ☐ Does the emergency plan explicitly address workforce impact, including transportation, housing loss, and personal hardship?
- ☐ Are policies in place to prevent punitive employment actions that could create legal, ethical, or reputational risk following disasters?
- ☐ Are financial assistance programs (e.g., payroll continuation, deductible reimbursement, transportation support) governed by documented internal controls?

7. Infrastructure and utility dependencies

- ☐ Does the organization assess dependency on community utilities such as water, power, sewage, and communications infrastructure?
- ☐ Are contingency plans documented for operating with limited or contaminated water supply and reduced fire suppression capability?
- ☐ Is generator capacity, duration, and maintenance validated against extended outage scenarios?

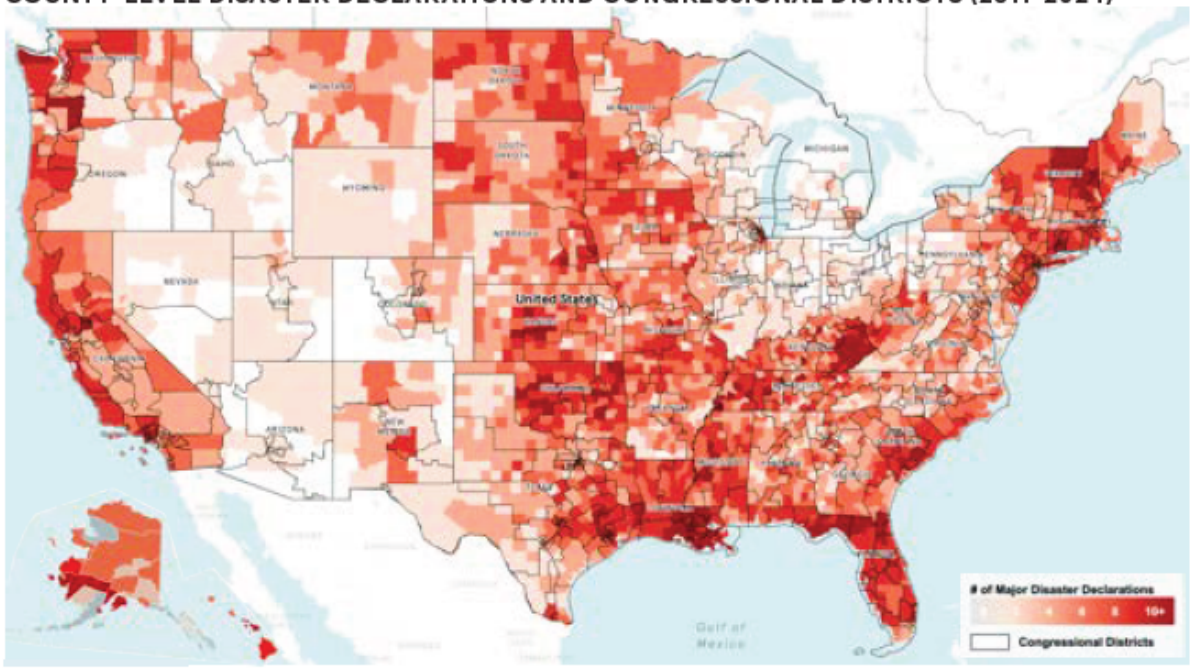
8. Post-event review and continuous improvement

- ☐ Is there a formal post-incident review process to identify gaps, document lessons learned, and update emergency plans?
- ☐ Are emergency preparedness lessons shared across the organization and incorporated into training and drills?
- ☐ Does leadership acknowledge that emergency preparedness requires flexibility and judgment beyond written plans?

Appendix B

ATLAS OF ACCOUNTABILITY

COUNTY-LEVEL DISASTER DECLARATIONS AND CONGRESSIONAL DISTRICTS (2011–2024)



As extreme weather continues to impact the U.S., Rebuild by Design launches the Atlas of Accountability, a mapping tool designed to help communities and policymakers understand their localized, climate-fueled exposure to extreme weather disasters. The tool builds on Rebuild by Design's 2022 report, "Atlas of Disaster," which analyzes county-level extreme weather disaster declarations and post-disaster federal assistance. The analysis highlights the urgency of bipartisan cooperation and the need to unite across the urban-rural divide.

99.5% OF CONGRESSIONAL DISTRICTS include a county that received a major disaster declaration for extreme weather between 2011 and 2024, amounting to $117.9 BILLION in federal post-disaster assistance from FEMA and HUD CDBG-DR.

FINDINGS

80% OF STATES	EXPERIENCED 10 OR MORE MAJOR DISASTER DECLARATIONS
28 STATES	HAD EVERY COUNTY IMPACTED BY A MAJOR DISASTER DECLARATION
39 DISASTERS	CALIFORNIA HAD THE HIGHEST COUNT IN THE U.S., SOME OF WHICH INCLUDED DECLARATIONS FOR TRIBAL GOVERNMENTS
22 DISASTERS	WASHINGTON COUNTY IN VERMONT, RECORDED THE HIGHEST NUMBER OF MAJOR DISASTER DECLARATIONS
HIGHEST PER CAPITA	STATES WITH THE HIGHEST PER CAPITA POST-DISASTER ASSISTANCE SPAN ACROSS BOTH POLITICAL AFFILIATIONS: LOUISIANA, HAWAII, NEW YORK, VERMONT AND NEW JERSEY.

NP

High-Stakes Deception

A healthcare internal auditor's guide to business email compromise

By Victor Hartman, JD, CPA/CFF, CFE

While internal auditors are accustomed to focusing on issues such as revenue cycle management, HIPAA compliance, and clinical quality controls, healthcare enterprises must also address a significant fraud risk: business email compromise (BEC). According to the FBI's 2023 figures, BEC has resulted in over $55 billion in global losses.

For healthcare organizations—which manage massive capital expenditures for medical equipment, navigate complex insurance reimbursements, and maintain sprawling vendor networks—the risk is very real. Unlike a standard ransomware attack that locks down a system for a noisy ransom, BEC is a quiet fraud. It relies on the deception of a trusted relationship to redirect a legitimate payment to a fraudster's bank account.

For the internal auditor, BEC represents a breakdown in the most fundamental of internal controls: the verification of identity and the integrity of payment instructions. This article provides a deep dive into the mechanics of these attacks, the legal frameworks governing liability, and a roadmap for auditing the healthcare environment against this evolving threat.

Attack vectors: Spoofing vs. hacking

In a healthcare setting, BEC usually targets the accounts payable (AP) department or the treasury function. To audit these risks, one must first distinguish between the two primary attack methods: spoofing and hacking.

In a spoof attack, the fraudster does not actually infiltrate an organization's network. Instead, they create a look-alike domain. For example, if your primary surgical supply vendor uses the domain *@hartman.com*, a fraudster might register *@hartmann.com*.

When this attack is successful, it constitutes both a social engineering and an information technology failure. The audit function can test both social engineering awareness and the IT function. For example, the auditor can assess whether email filters are configured to flag external sender warnings or whether the organization uses DMARC (Domain-based Message Authentication, Reporting, and Conformance) to prevent unauthorized use of a domain. Social engineering can be evaluated with penetration testing and employee acknowledgement of social engineering training.

Unlike a standard ransomware attack that locks down a system for a noisy ransom, BEC is a quiet fraud.

By gaining control of a vendor's sales or accounts receivable email account, the attacker can send legitimate-looking invoices from a trusted source.

A hack attack is more dangerous than a spoof attack because there are fewer warning signals. The fraudster compromises a vendor's email system rather than the healthcare organization's own network. By gaining control of a vendor's sales or accounts receivable email account, the attacker can send legitimate-looking invoices from a trusted source. This part of the fraud is particularly challenging because the healthcare organization has limited oversight or control over its external vendor's security protocols.

Once inside the vendor's email system, the fraudster's modus operandi is to be patient. They do not send an immediate "wire money now" request. Instead, they set up an email folder, often a hidden RSS feed or auto-forwarding rules, where they can anonymously review emails. The fraudster then learns the healthcare organization's payment cycles, the names of the signing authorities, and the typical invoice phrasing. When an email containing a high-value invoice (e.g., for new medical components or pharmaceutical supplies) is received, they respond with a change of banking instructions email from the vendor's compromised account.

The anatomy of an email account takeover

An email account takeover is at the heart of many forms of fraud, including BEC. Probably the most common method is a real-time phishing attack, known as the adversary-in-the-middle attack. Here, the fraudster may send an email that entices the victim to click a link for a Microsoft 365 Security Check. After the click, the victim is unwittingly communicating directly with the fraudster and provides their Microsoft credentials, including the two-factor authentication (2FA, also known as multifactor authentication or MFA) code that is obtained as part of the ruse. Simultaneously, the fraudster is using the credentials to log in to the victim's email account. Other techniques include 2FA bombing and session cookie theft.

An IT strategy to prevent email account takeover is to use phish-resistant 2FA (such as hardware keys) for high-risk treasury roles, or "Impossible Travel" logs, which detect an out-of-area login (such as a foreign country) followed by the legitimate user at the company office. The audit function can test for the presence and functioning of these protocols.

Definitions

What is DMARC?

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol designed to stop email fraud and phishing. It gives domain owners control over how their email should be authenticated and what should happen if a message fails those checks (e.g., rejected, quarantined, or delivered). DMARC works alongside SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to ensure that only authorized senders can use the domain. It doesn't replace antivirus or firewalls, but it adds an essential layer of protection.

What is an RSS feed?

RSS stands for *really simple syndication or rich site summary*, depending on who you talk to. An RSS feed is a web feed that allows applications and their users to access automatic website or content updates. RSS feeds rely on simple text files, extracting important information from XML (extensible markup language). Simplified, streamlined content is then input into an RSS reader, which converts text files into digital updates. Through this process, an RSS feed makes it possible to turn simple information, such as a content's title description, into a steady stream of new content pieces.

What is session cookie theft?

Session cookie theft, also known as session hijacking, is a type of attack where the attacker intercepts or steals a user's session cookie (a small piece of data that a website sends to your computer, allowing the website to remember information about your session, such as login details, preferences, or items in your shopping cart) to gain unauthorized access to an active web session. Since session cookies store authentication details, attackers who hijack them can impersonate the legitimate user. This allows them to bypass login credentials and gain access to sensitive data, applications, or accounts.

The legal reality: Who bears the risk of loss?

When a $500,000 payment meant for a medical device manufacturer ends up in a fraudster's account in Hong Kong, who is responsible? The healthcare provider is now incentivized to attempt to shift the loss to a bank or its vendor. The result will depend on the application of the Uniform Commercial Code 4A-207 and common law.

When the case is healthcare provider v. bank, UCC 4A-207, known as the Mismatch Rule, often serves to protect the bank. This is perhaps the most critical legal concept for a healthcare auditor to understand. When a healthcare provider sends a wire or an ACH, they provide both an account name (e.g., General Medical Supplies, Inc.) and an account number. Under UCC 4A-207, the receiving bank may rely entirely on the account number, and the bank is not required to verify that the name on the account matches the account number.

Although increasingly controversial, the purpose of the Mismatch Rule is to enable automated processing of mass transactions without human intervention. Unless the bank had actual knowledge of the discrepancy at the time of the deposit (which is difficult, but possible, to prove), the bank is not liable.

The Mismatch Rule is also at the heart of most BECs, because the fraudster directs funds to a bank account number belonging to another unwitting victim, likely involved in a romance or work-from-home scam that the fraudster controls.

When the healthcare organization completes the wire or ACH transfer instructions naming its vendor as the recipient of the funds but provides the bank account number of the account the fraudster controls, the vendor's name will not match the account holder's name. The bank will pay the fraudster, and the payor will likely suffer the loss. The importance of knowing this rule is that the payor must conduct due diligence at the front end to ensure the payee's name and account number match.

When the case is healthcare provider v. vendor, the health-care provider's chances of success are increased. The outcome will depend on a court's application of common law principles, such as the imposter rule or the least-cost avoider.

The loss typically falls on the party that was in the best position to prevent the fraud. For example, if a hospital's AP clerk received a change-of-bank email request with obvious red flags (typos, an odd tone, a foreign bank account for a domestic vendor) and failed to call the vendor, the hospital likely bears the loss.

Alternatively, if the vendor's email was hacked and the fraudster sent the instructions from the vendor's actual server, in an attempt to shift liability the hospital could argue that the vendor's poor cybersecurity was the proximate cause.

The healthcare provider's defense against the BEC is to ensure that rigid protocols are in place for the Vendor Master File (VMF). The internal audit function should focus on the presence and functioning of the following types of controls:

1. Out-of-band verification (The Golden Rule): Any request to change banking instructions must be verified by phone to a known number in the VMF. Never use the phone number provided in the email requesting the change.
2. Dual control: Does the system require one person to input a change to a vendor's ACH/wire instructions and a second person (ideally a supervisor) to approve it?
3. The "penny test" / micro-deposits: For new high-value vendors, consider a policy of sending a nominal amount (e.g., $1.00) and confirming receipt verbally before sending the full balance.
4. Vendor communication policy: Proactively inform your vendors that your organization never changes payment instructions via email without a formal, multistep verification process.

The 72-hour financial fraud kill chain and response protocol

In healthcare, we talk about the Golden Hour for trauma patients. In BEC, a victim can rely on the FBI's Financial Fraud Kill Chain, but they must act quickly. In fact, the FBI reports a 70% success rate if the BEC is reported within 72 hours.

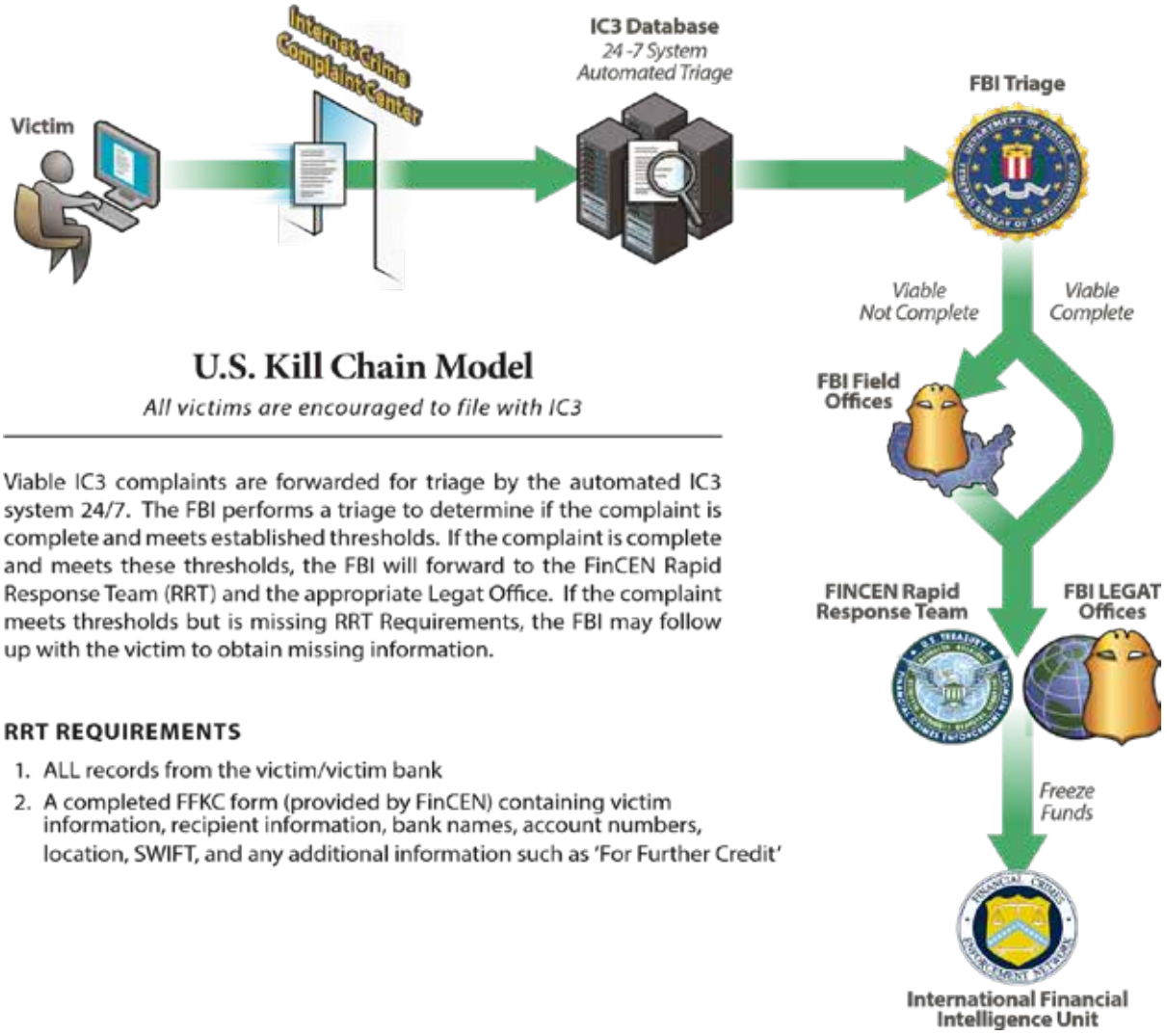
The loss typically falls on the party that was in the best position to prevent the fraud.

NON-LAW ENFORCEMENT SENSITIVE

F B I · C Y B E R

International Kill Chain Process

The International Financial Fraud Kill Chain (FFKC) is a partnership between federal law enforcement and financial entities whose purpose is to freeze fraudulent funds wired by victims. International FFKC requests are coordinated through the Financial Crimes Enforcement Network (FinCEN) Rapid Response Team (RRT) and law enforcement entities. Victims are urged to file a complaint with IC3.gov as soon as the fraud is discovered.



U.S. Kill Chain Model

All victims are encouraged to file with IC3

Viable IC3 complaints are forwarded for triage by the automated IC3 system 24/7. The FBI performs a triage to determine if the complaint is complete and meets established thresholds. If the complaint is complete and meets these thresholds, the FBI will forward to the FinCEN Rapid Response Team (RRT) and the appropriate Legat Office. If the complaint meets thresholds but is missing RRT Requirements, the FBI may follow up with the victim to obtain missing information.

RRT REQUIREMENTS

1. ALL records from the victim/victim bank
2. A completed FFKC form (provided by FinCEN) containing victim information, recipient information, bank names, account numbers, location, SWIFT, and any additional information such as 'For Further Credit'

The future of BEC auditing lies in continuous monitoring.

Victim's role in incident response:

- Immediate bank contact: Ensure the financial team knows to contact the bank's security/fraud department, not a general customer service line.
- Hold harmless agreement: Banks are often hesitant to freeze accounts for fear of liability. The victim organization should be prepared to sign a hold harmless agreement if requested by the bank.
- IC3.gov and the FBI: Filing an IC3 report is not just for statistics; it generates a case number that the FBI's Recovery Asset Team (RAT) uses to trigger the financial fraud kill chain protocols with foreign banks.
- Engage legal counsel: Instruct legal counsel to aggressively demand detailed facts around the bank's transfer of funds that may later be used to seek legal recourse.

The intersection of BEC and HIPAA

If the healthcare provider's email account is hacked, as it is in some variants of the BEC, or if it is hacked as part of an email or bank account takeover fraud, this becomes a double-headed disaster. If a fraudster compromises an email account to redirect a payment, they also have access to every email in that inbox. If that inbox contains protected health information (PHI)—such as patient billing records, clinical trial data, or insurance claims—the financial fraud is now also a HIPAA breach.

Internal auditors should also focus on whether its organization's procurement and financial departments are practicing good inbox hygiene and not storing sensitive PHI in their email indefinitely. Automated deletion policies for old emails can significantly reduce the blast radius of a BEC compromise.

Continuous monitoring and the future of AI

The future of BEC auditing lies in continuous monitoring. Rather than an annual audit of the VMF, internal audit functions should advocate for software that uses AI to flag anomalies in real time.

- Sentiment analysis: AI can detect if an email from a longtime vendor's CFO suddenly shifts in tone, urgency, or vocabulary—common indicators of a hack attack.
- Geo-fencing: Monitoring for logins from countries where the organization has no business interests.
- Name matching: While banks aren't required to match names with account numbers under UCC 4A-207, some modern fintech solutions and confirmation of payee services (common in the UK and Australia) are beginning to bridge this gap.

Conclusion

While ransomware often captures headlines, the BEC has quietly become a $55 billion global threat, posing a serious risk to healthcare organizations. Unlike noisy cyberattacks that lock down systems, BEC is a patient fraud that relies on the deception of trusted relationships to divert legitimate payments.

By distinguishing between spoofing (look-alike domains) and hacking (direct vendor account takeover), internal auditors can identify critical gaps in their organization's defenses. Because these attacks often exploit a lack of control over third-party vendor security, they represent a fundamental breakdown in the integrity of payment instructions. Effectively auditing this risk requires a shift in focus—moving beyond standard compliance to rigorously testing both social engineering defenses and the technical filters intended to catch these sophisticated predators. **NP**

Victor Hartman, JD, CPA/CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting, internal investigations, and fraud mitigation consulting. He previously served as an FBI Special Agent. He is also an Adjunct Professor at Georgia State University. Vic can be reached at 404-369-0616 and Vic@HartmanFirm.com.

"There are some things you learn best in calm, and some in storm." - Willa Cather

FEATURE

Follow the Money

Evaluate enterprise risk across the healthcare revenue chain

By Julie Hardy, MSA, CRCE, RHIA, CCS, CCS-P, Jesse Parker, CPA, and Robert Rudloff, CISSP, CISA, QSA

Healthcare organizations don't experience financial, compliance, and cybersecurity risks in isolation. They experience them through the same workflows, systems, and data that drive reimbursement. At the center of that convergence is the flow of money: from patient access and documentation to billing, payment, and ultimately financial reporting.

Breakdowns in the revenue chain flow rarely stay contained; a single issue can cascade from operational inefficiency to regulatory exposure and even to data vulnerability. For internal auditors, this means we need to avoid evaluating risk in silos. These processes must be understood as an interconnected chain where financial integrity, compliance obligations, and data security are tightly linked. Following the money, therefore, is not just about revenue; it is about understanding how risk moves across the enterprise.

Revenue cycle risk

The revenue cycle is often viewed as an operational function. While it does contain many operational processes, it is actually a central point of enterprise risk. Financial performance, regulatory compliance, and data security all intersect within revenue cycle processes, systems, and data.

For internal auditors, the objective is not just to identify discrete risks, but to understand how those risks connect and compound. Breakdowns in one area rarely remain isolated. They move downstream, often increasing in impact. Effective oversight requires an end-to-end view of how revenue is captured, processed, and reported.

The revenue cycle as an interconnected process

The revenue cycle spans the full lifecycle of a patient encounter, starting with scheduling and registration and ending with final payment. Each phase introduces risk, and each depends on the integrity of the prior step.

1. Front-end processes establish the foundation for reimbursement. Errors in eligibility, demographics, or authorization often surface later as denials or write-offs.
2. Mid-cycle activities translate clinical services into billable events. Documentation, coding, and charge capture present significant compliance and financial risk. Errors at this stage can result in improper payments or missed revenue.
3. Back-end processes determine whether revenue is realized. Claims submission, denial management, and collections directly affect cash flow and financial reporting.

These functions are often managed in silos, but the risk doesn't stay that way; issues upstream tend to carry through and get worse as they move downstream.

Core revenue cycle risk areas

Several risk domains consistently result in exposure within the revenue cycle.

Coding and billing integrity

Coding errors remain a primary source of compliance risk. Inaccurate code selection, modifier use or leveling can result in improper payments. Overpayments create audit and recoupment or clawback risk. Underpayments reduce revenue and are often not recovered.

The greater concern is systemic error. Gaps in provider education, inconsistent policies, or weak feedback loops can produce sustained patterns of noncompliance. Internal audit should focus on both error rates and root causes.

Auditors need to avoid evaluating risk in silos.

Following the money is not just about revenue; it is about understanding how risk moves across the enterprise.

Denials and revenue leakage

Denials are a visible indicator of revenue cycle breakdowns, but they are rarely the root problem. Many denials originate upstream, including missing authorizations, documentation gaps, or payer-specific requirements.

Organizations also vary in how effectively denials are worked. Limited resources, poor prioritization, or lack of analytics can result in avoidable write-offs. Over time, this creates significant revenue leakage.

Data integrity and system dependence

Revenue cycle performance really comes down to how cleanly data moves across systems, including electronic health records (EHRs), billing platforms, and all the interfaces in between. Configuration errors, mapping issues, or interface failures can result in systemic discrepancies.

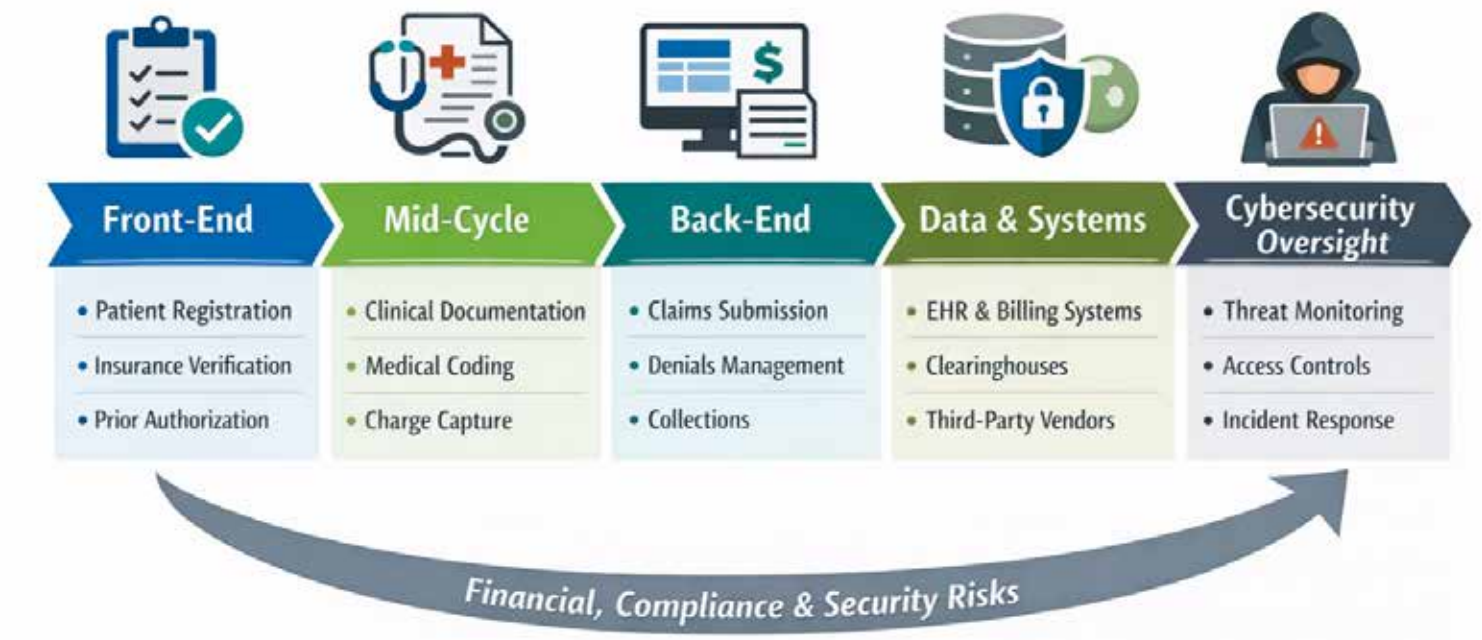
These issues are often difficult to detect and may persist for extended periods. For example, incomplete charge capture or incorrect payer mapping can lead to underbilling or underpayment.

Third-party and vendor risk

Outsourced coding, billing, and credentialing functions introduce additional risk. Vendors may vary in control maturity, compliance practices, and security posture.

A vendor issue, whether operational or cybersecurity-related, can directly affect revenue and compliance. Oversight is often limited, with insufficient visibility into vendor controls. Internal audit should assess both performance and compliance monitoring.

Revenue cycle: End-to-end risk flow



Cybersecurity considerations within the revenue cycle

Revenue cycle systems contain high-value data, including protected health information (PHI) and financial information, which make them a valuable target for cyber criminals. Three factors that make these systems especially attractive are:

- Revenue disruption: potential to immediately disrupt revenue, creating financial pressure on the organization
- PHI: these systems contain dense concentrations of protected health information, which cyber criminals can use or sell
- Cash: many of these platforms have banking, routing, and payment information within the records, providing cyber criminals with additional sources of money

Key areas of exposure include:

- Clearinghouses and transaction intermediaries
- Automation tools, including remote process automation (RPA)
- Remote access environments supporting distributed teams

A cybersecurity event can halt claims processing, delay billing, and interrupt cash flow. The impact may include operational disruption, financial loss, regulatory reporting, and reputational damage.

For internal audit, revenue cycle and cybersecurity cannot be evaluated separately. Control gaps often exist at the intersection of systems, users, and workflows.

Operational signals of cyber risk

Revenue cycle disruptions are often the first visible sign of a cybersecurity event. Cyber criminals usually use compromised accounts to gain access, so the IT security team may only see normal traffic, even if the criminal is active within the system. Billing and revenue cycle staff may observe changes to payment methods, banks, account numbers, or payment addresses. Unusual changes may be linked to a compromise that hasn't caused any cyber alerts. Signals warranting a closer look include:

1. Sudden claim failures not explained by payer system maintenance or scheduled downtime
2. Unusual spikes in claims rejections or edit overrides, particularly when rejection codes do not align with typical denial patterns
3. Interface outages between the EHR, practice management system, clearinghouse, or payment platforms
4. Vendor connectivity anomalies, especially involving third-party clearinghouses or revenue cycle management (RCM) platforms
5. Unusual user access patterns, such as after-hours activity, unfamiliar account usage, or bulk data queries in billing systems
6. Unexplained changes in payment routing or banking information within remittance files or payer portals

In 2024, a clearinghouse processing billions of transactions was compromised by a ransomware group (see Change Healthcare sidebar). When their systems went offline the impact cascaded across the entire revenue chain: eligibility verification stopped, prior authorizations stalled, and claims did not get processed.

An American Hospital Association (AHA) survey about the event of nearly 1,000 hospitals found that 94 percent reported financial impact, and one-third reported that more than half of their revenue was disrupted. Providers resorted to manual workarounds that increased error rates and created reconciliation burdens lasting through multiple billing cycles.

This demonstrates how a single third-party failure can disrupt the entire revenue cycle. A single point of failure in a clearinghouse relationship can halt operations across an entire organization—and the operational signals described above were among the first indicators that something was wrong.

The Change Healthcare Breach

Rick Pollack, President and CEO of the AHA, stated that "the Change Healthcare cyberattack is the most significant and consequential incident of its kind against the U.S. healthcare system in history." And Congress members have said that "the breach of Change was tantamount to targeting the health care system in its entirety."

The revenue cycle is actually a central point of enterprise risk.

For internal auditors, the objective is not just to identify discrete risks, but to understand how those risks connect and compound.

Connecting risk across the revenue cycle

In practice, risks are sequential and compounding. A documentation issue can lead to coding errors, resulting in overpayment and subsequent audit exposure. A system disruption can delay claims, increase denials, and affect cash flow.

The role of internal audit

Internal audit functions should move toward an integrated approach to revenue cycle risk. Key elements include:

- End-to-end process evaluation, from access through payment
- Coordination across revenue cycle, compliance, and IT functions
- Use of data analytics to identify patterns and anomalies
- Evaluation of controls across the revenue cycle

Combining data sources such as coding results, denial trends, and system activity can reveal risks that are not visible in isolation.

Continuous monitoring is also increasingly important. Given transaction volume, periodic reviews may not be sufficient. Dashboards, key risk indicators, and automated alerts can improve timeliness and responsiveness.

Common control dependencies can be audited to increase efficiency and reduce possible audit fatigue. Key areas of common controls include:

- Identity and access management: Billing systems require role-based access to patient data, payment portals, and payment functions. Weak control creates exposure that is both a billing integrity risk and cyber risk. Audit for separation of duties, roles, shared credentials, excessive privileges, and use of multifactor authentication (MFA).
- Automated edits and business rules: Claim scrubbing, coding validation, and payment posting rely on automated logic. The rules and process flow should be protected from change, monitored for changes, and audited annually to verify the processes are still accurate.
- Remote vendor access: Many organizations allow third-party billing vendors, coding companies, and technology providers to remotely access organizational systems. The access should be monitored and (if possible) only open during the required support period and then removed.
- Data transmission integrity: Encryption, secure file transfer, and data transmission should be regularly reviewed to verify they are still current and using the best available technology.

Proposed updates to the HIPAA Security Rule, published as a Notice of Proposed Rulemaking in January 2025, would formalize several of these controls as regulatory requirements, including mandatory MFA, encryption of ePHI at rest and in transit, 72-hour system restoration timelines, and annual technical asset inventories. Internal auditors should monitor rulemaking progress and assess current control maturity against these proposed requirements, regardless of whether the final rule is adopted as written.

In mid-2024, a major health system was compromised by a ransomware group after an employee downloaded a malicious file. The result was that every major technology system was shut down, clinicians reverted to paper, and ambulances were re-routed to other facilities whenever possible.

The incident severely disrupted the revenue cycle through delays in insurance verification, claims submissions, and payment processing. The incident illustrates how common control dependencies—in this case endpoint security, employee security awareness, and system access controls—simultaneously impacted operations, billing, and data protection. Internal audit needs to consider these common controls as part of the overall audit planning.

Internal auditors can help organizations build a cross-functional assessment to test the shared control dependencies and ensure these types of anomalies receive the same escalation rigor as cybersecurity alarms and alerts. We recommend audit plans verify that the organization has tested its incident response procedures against revenue cycle disruption scenarios using tabletop exercises or similar simulations, so operational, financial, and cybersecurity response actions are coordinated before an event occurs.

Control gaps often exist at the intersection of systems, users, and workflows.

Strengthening oversight

Organizations can improve revenue cycle oversight by focusing on a few practical areas:

- Align governance across revenue cycle, compliance, and IT
- Prioritize areas with both high financial impact and regulatory exposure
- Strengthen vendor oversight and accountability
- Invest in provider and staff education to address root causes
- Leverage analytics to improve visibility and decision-making

These efforts should align with overall risk tolerance and strategic priorities.

Follow the money

Revenue cycle processes generate the financial and utilization data that support broader reporting. Charges, payments, adjustments, and volumes flow directly into downstream financial structures.

Cost reporting relies on this data to allocate costs, support reimbursement, and meet regulatory requirements. As a result, weaknesses in the revenue cycle don't end at payment, they carry forward into how organizations represent financial performance.

Understanding the progression of revenue cycle effects from payment through financial reporting is critical. The same issues that affect revenue capture—data integrity, compliance, and system reliability—also influence cost reporting accuracy. The next step in following the money is to examine how these risks extend into cost reporting and how they are reflected in financial disclosures and reimbursement methodologies.

All cost reports are not created equal

While general cost reports may refer to internal, unaudited, or state-specific documents, Medicare Cost Reports (MCRs) are the primary, comprehensive source for authenticated financial, utilization, and cost data. Medicare-certified institutional providers are required to submit an annual MCR to a Medicare Administrative Contractor (MAC). The cost report contains provider information such as facility characteristics, utilization data, cost and charges by cost center (in total and for Medicare), Medicare settlement data, and financial statement data. CMS maintains the cost report data in the Healthcare Provider Cost Reporting Information System. This data is used to settle payments between CMS and hospitals and inform future Medicare payment rules.

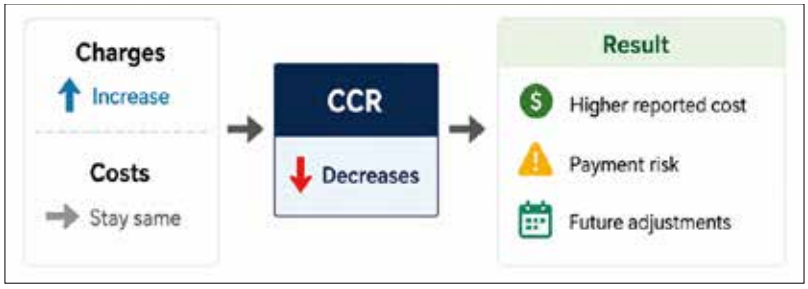
Key risk connection: Charges drive reported cost

Cost reporting relies on a foundational relationship: Charges → cost-to-charge ratio (CCR) → estimated cost.

There is an inverse relationship between the assigned chargemaster prices and the cost-to-charge ratio. If the underlying cost of inputs to provide a service does not increase, increases in the prices of services will result in a lower CCR.

Because CCR is derived from total costs and total charges, changes in pricing can shift the ratio even when underlying costs remain stable. This creates an inherent risk:

Impact of chargemaster changes on CCR



A single third-party failure can disrupt the entire revenue cycle.

- Increasing charges without a corresponding increase in cost → lower CCR
- Lower CCR applied to charges → distorted cost estimates

For internal audit, the key takeaway is that pricing decisions are influenced by reported cost and reimbursement outcomes, not just revenue.

Impact area 1: Outlier payments

Under the Medicare inpatient prospective payment system, outlier payments are designed to offset unusually high-cost cases. These payments rely on estimated costs derived from CCRs in the most recently settled Medicare cost report.

This introduces a timing disconnect. Claims are processed using CCRs that may be one to two years old, while chargemaster prices and operational costs may have changed significantly in the interim. When prices increase without a corresponding increase in cost, the actual CCR declines, but the CCR used for interim outlier calculations does not.

The result is a temporary distortion in reimbursement. Hospitals may receive higher interim outlier payments based on outdated CCRs, creating exposure when those amounts are later reconciled to current-period data. From an internal audit perspective, this raises several considerations:

- Whether chargemaster changes are evaluated for downstream reimbursement impact
- The level of coordination between revenue cycle and reimbursement functions
- The organization's ability to anticipate and manage settlement adjustments

Impact area 2: Cost-based reimbursement

The relationship between charges and CCR is even more direct for providers reimbursed on a cost basis, such as Critical Access Hospitals and certain rural facilities.

In these environments, Medicare reimbursement is based on allowable charges multiplied by the CCR. As with outlier payments, interim reimbursement relies on CCRs from prior-period cost reports, with final settlement occurring after submission of current-year data.

Changes to the chargemaster can therefore create misalignment between interim payments and actual costs. For example, increasing charges without a corresponding increase in cost reduces the CCR, but that change may not be reflected in interim rates. This can lead to overpayments or underpayments during the year, followed by reconciliation adjustments.

From an operational standpoint, this introduces variability in cash flow and increases reliance on interim rate adjustments to maintain alignment. Internal audit should consider whether organizations have processes in place to monitor these impacts and respond proactively when significant changes occur.

Impact area 3: Financial reporting and audit implications

Across both reimbursement models, a consistent risk pattern emerges: Revenue cycle inputs drive financial outcomes that are recognized later. Because reimbursement often relies on prior-period CCRs, current-period billing activity can distort interim payments and delay the recognition of actual financial performance.

This creates exposure in several areas, including balance sheet accuracy, cash flow predictability, and performance measurement. For example, settlement adjustments may significantly affect receivables or liabilities, while apparent changes in profitability may reflect pricing decisions rather than true operational performance.

For internal audit, this is a point of convergence between revenue cycle and financial reporting risk. Pricing decisions, charge capture practices, and billing patterns should be evaluated not only for compliance and revenue integrity, but also for their downstream impact on cost reporting and reimbursement accuracy.

Audit risk

These dynamics ultimately affect balance sheet accuracy, cash flow predictability, and performance reporting, reinforcing the need for alignment between revenue cycle and reimbursement functions.

Conclusion

Risk in the revenue cycle is not isolated; it is interconnected, compounding, and often delayed in how it surfaces.

Internal audit is uniquely positioned to connect these points, linking operational processes, financial outcomes, and system-level controls. Following the money provides that line of sight—turning fragmented risks into a cohesive view of enterprise exposure. **NP**

Julie Hardy, MSA, CRCE, RHIA, CCS, CCS-P, is a Partner in RubinBrown's Consulting Services Group. She has over 20 years of experience in the healthcare industry providing revenue cycle management, process improvement and operational optimization. Julie has helped to enhance provider financial performance while maintaining compliant practices. She can be reached at 810-853-6171, julie.hardy@rubinbrown.com, or on LinkedIn.

Jesse Parker, CPA, is a Partner in RubinBrown's Consulting Services Group. He has over 10 years of experience providing regulatory reimbursement and payment services in the healthcare industry. He has experience with financial and governmental reimbursement audits for healthcare organizations and government entities. He can be reached at 615-253-5200, jesse.parker@rubinbrown.com, or on LinkedIn.

Robert Rudloff, CISSP, CISA, QSA, is a Partner in RubinBrown's Consulting Services Group with more than 25 years of information security experience on security reviews, mitigation, strategy, and architecture development. He consults with clients on a variety of information security projects, including serving as a vCISO. He can be reached at 303-952-1220, rob.rudloff@rubinbrown.com or on LinkedIn.

The Seven Signs of Ethical Collapse – Part 2

Consider why no one sounded the alarm

By Marianne M. Jennings, JD

Twenty years ago, I published my book The Seven Signs of Ethical Collapse: How to Spot Moral Meltdowns in Companies...Before it's too Late. *While the companies whose names are splashed across the headlines for falling into ethical collapse have changed, the patterns that lead to collapse have not. Auditors should understand these patterns and evaluate if their organization is at risk.*

This is the second of a four-part series where I review the seven signs with examples of organizational collapses that occurred since my book's publication. This review serves as a refresher and an auditor's guide to avoiding or rerouting from the path to collapse.

The Seven Signs

In this four-part series, I review the seven signs of ethical collapse that auditors, leaders, governance, investors, and other stakeholders can observe and must confront:

1. Pressure to maintain the numbers (Part 1)
2. Fear and silence (Part 2)
3. Young 'uns and a bigger-than-life Chief Executive Officer (Part 2)
4. Weak board (Part 2)
5. Conflicts (upcoming)
6. Innovation like no other (upcoming)
7. Goodness in some areas atoning for evil in others (upcoming)

Sign #2: Fear and silence

In Part 1 of this series, I reviewed the first sign of ethical collapse: pressure to maintain the numbers. Unhealthy and unreasonable pressure to meet numbers (like earnings, performance scores, or customer volumes) can lead to manipulation, deception, and fraud. The second sign explains why the numbers pressures and resulting actions rarely percolate up to someone who can and will stop the irrational fixes and decisions.

Wells Fargo and its "Go for Greight!"

Wells Fargo had an incentive plan that gave employees bonuses for signing new customers and expanding existing customers' products with the bank. The bank's campaign was titled, "Go for Greight!" and resulted in unlawful practices that were referred to within Wells Fargo as "gaming." Ultimately, Wells Fargo agreed to pay $3 billion to resolve the criminal and civil investigations into their sales practices that involved opening millions of accounts without customer authorization (with a goal of eight bank products per customer).

Unhealthy and unreasonable pressure to meet numbers (like earnings) can lead to manipulation, deception, and fraud.

Then CEO, John Stumpf, boasted that Wells had only 1% of its workforce terminated for gaming the system to meet their numbers goals of "eight for great."[1] But that low percentage didn't reflect the terminations of those who initially reported the system gamers and the turnover rate of those who witnessed these terminations.

Employees described the high stress of the goals and their inability to find someone at a manager level or above who would address those concerns. When employees witness others being terminated for reporting issues to ethics and compliance or HR, the chance that they will raise issues becomes astronomically low. At Wells Fargo, the fear of termination meant that many concerned employees simply quit.

Atlanta Public Schools (APS) – Fear and humiliation

If a teacher or administrator filed a report raising the cheating issues described in Part One of this series, they were asked to alter the report and often had a reprimand placed in their employee file. One teacher who had witnessed tampering with test answer sheets was told to remain quiet or she would "be gone."[2]

Public humiliation was a tool used to instill fear and humiliation. At district meetings, principals who resisted the cheating scam were forced to sit in the bleachers along the side.[3] Teachers with low scores were forced to sit under tables in meetings. Those who questioned why they were changing students' answers were terminated, transferred, or investigated.

Audit tools for Sign #2

The hallmarks of this sign are turnover and terminations and even increases in the amount of PTO. HR can usually identify areas of focus and zero in on some root causes.

If demographics are not collected in employee engagement and ethics surveys, the surveys can reveal areas where fear and silence may be concentrated. Concerns are often more easily identified in open-ended comments than in quantifiable data. Slow-walked investigations reveal potentially complicit management or investigation teams. Exit interviews often find employees unloading the burden of fear and silence. Social media sites where former employees offer insights into companies are a wealth of information.

Fear and silence in healthcare

Even when a healthcare system doesn't collapse financially, fear and silence can lead to more dire consequences. Employees and patients are encouraged to speak up for safety because medical errors are the third leading cause of death in the U.S., and more than 400,000 Americans die from a preventable medical mistake each year.

Fear and silence were contributing factors when patients of one oncologist endured years of chemotherapy for cancer they never had. Other clinicians were skeptical of the oncologist's diagnosis and treatment but kept quiet about their misgivings for years. The oncologist was a powerful figure within the hospital and town. He was earning $2 million a year and had threatened to sue the hospital several times, court records show. While his nurses adored him, others inside the hospital feared him. Many on staff credited him with forcing out two hospital CEOs who had challenged his pay, court records show.

Sign #3: Young 'uns and a bigger-than-life CEO

In my book, I told the stories of bigger-than-life CEOs from the past like Richard Scrushy, Jack Welch, and Jeff Skilling, and the inexperienced supporters who often became their unwitting accomplices.

[1]Emily Glazer, "Battered Bank Seeks New CEO," *Wall Street Journal*, March 30-31, 2019, p. B12. Rachel Louise Ensign, "Embattled Wells Fargo CEO Exits," *Wall Street Journal*, March 29, 2019, p. A1. Emily Glazer, "Wells Fargo Regulators Weigh Shake-Up," *Wall Street Journal*, March 12, 2019, p. B10. Ryan Tracy and Emily Glazer, "Fed Orders Wells Fargo to Change Board," *Wall Street Journal*, February 3-4, 2018, p. A1, Emily Flitter, Binyamin Appelbaum, and Stacy Cowley, "Rebuking Wells Fargo for Abuses, Fed Demands Shake-Up of Board," New York Times, February 3, 2018, p. A1.

[2]CRCT Report, Vol. 3, p. 362.

[3]Michael Winerip, "A New Leader Helps Heal Atlanta Schools, Scarred by Scandal," *New York Times*, February 21, 2012, p. A12.

The charismatic, colorful CEO is still alive and well and somehow immune to media scrutiny.

- Elizabeth Holmes of Theranos was a media charmer who, with her Steve-Jobs-like wardrobe, was lionized for dropping out of Stanford to change the medical world with a blood testing product that was revealed as a fake.
- Beverly Hall, the superintendent of APS, was given national and international awards for her achievements in APS test scores.
- John Stumpf of Wells Fargo was profiled by all the business publications for his "cross-selling" strategy of growing revenues by expanding customers' accounts.
- The FAA was deferential to Boeing executives—despite fatalities caused by Boeing's concealing known flaws in its aircraft—because of Boeing's reputation and considerable contracts with the government.
- Nikola's CEO, Trevor Milton, was 32 when he founded the company and experienced media adulation for his parallels to Elon Musk before the company's electric trucks were revealed as fake.

FTX – A Gen Y CEO and friends

Samuel Bankman-Fried, the founder of FTX (a crypto-currency company), offers a slight nuance in Sign #3. With Bankman-Fried, we have the first of the Gen Y (aka Millennial) CEOs. They may or may not be charismatic, but their charm comes from winning over the hearts and minds of their own generation and putting fawning Millennials into direct-report positions.

There are still the same problems the charismatic CEO presents, but these Gen Y CEOs buy their charisma with perks and compensation. Their direct reports are still trapped by the trappings. Their direct reports' lack of business experience gives the young CEO control.

Bankman-Fried's surrounding "young 'uns" were tech whizzes but not especially knowledgeable about financial reporting and audit practices. They loved the pay as well as the elegant beaches of Nassau where they were headquartered and were easily persuaded when they raised concerns.

For example, one of Bankman-Fried's direct reports questioned the legality and/or propriety of using customer cryptocurrency funds to finance FTX's hedge funds (a valid question since it was illegal) and asked. "Will the auditors raise concerns about the use of customer funds?" Bankman-Fried had a glib and outrageous reply, "[A]uditors do not typically focus on such issues." The potential revolt was quelled quite easily.

Bankman-Fried had both media attention as well as the support of star power that a charismatic CEO could buy through endorsements and political donations. Representative Maxine Waters, Stephen Curry, Tom Brady, Giselle Bünchen, Shaquille O'Neal, and *Shark Tank* financier Kevin O'Leary were all part of the stable of FTX stars. Bankman-Fried was neither charming nor charismatic on his own, but he could draw in hangers-on through political donations and endorsement contracts. He also managed to use his political connections to staunch regulatory inquiries.

The bias of hero worship and the power of star-studded immunity curb the critical eye and dismiss skepticism—both necessary for analyzing what is really happening at the company.

Audit tools for Sign #3

The lack of experience of direct reports is a topic for auditors to discuss with the board's audit and risk committee; likewise for the CEO's actions. CEOs are a risk factor. Monitoring the decisions made at this level is crucial because halting illegal actions can be easier than trying to clean up a debacle created by an amateur CEO and direct reports.

Expense audits are a risk management tool for these executives because their travel and reimbursements reflect problematic conduct and, too often, poor judgment. Just the knowledge that leaders have their expenses tracked in the same way as employees is a powerful curb on C-suite behaviors.

Sign #4: Weak board

What makes a board weak varies, but in ethical collapses, a weak board is always present. A board can be weak

At Wells Fargo, the fear of termination meant that many concerned employees simply quit.

Exit interviews often find employees unloading the burden of fear and silence.

because it does not ask enough questions. Clearly, the Theranos board members were not asking the right questions. Asking Ms. Holmes to come to the next meeting prepared to demonstrate the company's product might have been helpful.

Often, boards are weak because they are simply not paying attention to the numbers or the right numbers. For example, Wells Fargo had a culture of pressure, fear, and silence, and the result was that it made sense to employees to create 3.5 million fake accounts or services existing customers did not know about. The response to this revelation was, "Who knew?"

Everyone should have known, given the numbers that leaders were focused on. Wells' products per customer ratio was nearly three times the rate of the banking industry. The banking industry average was 2.7 products per customer. Wells achieved 6.3 products (fake and otherwise) per customer before the systemic fraud was uncovered.[4]

When employees are making up accounts and customers, that ratio does climb. When board members see company numbers that are stunningly higher than the industry, the questions to ask are, "Are we that much better than the other banks?" "What are we doing that is different and makes these numbers possible?"

Some boards are weak because they are not using the audit function effectively. In the case of Wells, the directors should have simply asked questions about the growth in accounts and whether there were internal controls to prevent or detect fraud.

For example, one control that should exist is a system of follow-up with customers with new accounts or additional services to verify their approval. Had the auditors at Wells just examined the forms on the accounts and services, they would have seen that bank employees were listing their emails as "noname@wellsfargo.com," a bright red flag.

A board's expertise may be most helpful when a company faces a crisis and when a change in leadership is needed. For example, with Wells Fargo's deep-seated culture driven by pressure and numbers, a change in CEOs was necessary. Yet the board elected another member of outgoing CEO John Stumpf's executive team, Timothy Sloan. Sloan had already been slated as the officer in line to take over for Stumpf upon his retirement.

An executive who was part of the culture that had been in place for 10 years cannot function as an effective agent of change. The board's decision did not last because necessary changes in culture and processes were, not surprisingly, forthcoming. Sloan left in 2019 and Charlie Scharf, a veteran of Bank of New York Mellon, Visa, JPMorgan Chase, and Bank One took over and has remained in place. Under his watch, Wells was able to resolve its legal issues in 2025.

At Boeing, the Board's advice was needed in addressing the 737 MAX issues. The statements from CEO Dennis Mullenberg immediately following the crashes were inaccurate and perceived as callous. He went to congressional hearings without first communicating with the families of the crash victims. The victims' families came with protest signs, and Mullenberg made no contact with them at the hearing.

Board deference to leaders who have presided over a crisis is misguided. Resolution of a crisis does not come from those who were in charge when the crisis occurred. Yet it was 2019 before the board terminated Mullenberg. Mullenberg was replaced by Dave Calhoun, but the board endured continuing quality control issues before Calhoun was replaced by Kelly Ortberg in 2024. Ortberg resolved Boeing's civil, legal, regulatory, and liability issues by 2025.

Audit tools for Sign #4

Auditors often think that they are powerless to address the reality of weak boards. But auditors can turn weak boards into strong ones and perhaps exert the greatest influence under this sign by using the numbers at their fingertips.

An examination of Wells Fargo's turnover rate would have been revealing. Long before the 3.5 million fake accounts

[4] Aaron Back, "Wells Fargo Isn't Sorry Enough," *Wall Street Journal*, September 14, 2016, p. C12.

employees created because of pressure to cross-sell, and as early as 2005 (the fake accounts story did not become public until 2016), there were hundreds of reports to HR and compliance about employees gaming the system.[5] Discussions with HR and compliance about the types of cases they were handling would also have provided insights.

CEO Stumpf kept touting the low termination rate for employees as an indicator that there was no problem with pressure or fake accounts. However, Wells had a turnover rate that was a head-turner.

Employees who were not gaming were leaving the bank because of the pressure, fear, and silence, and because of the lack of enforcement for employees who were gaming the system and management ignoring reports of gaming.[6] Auditors need to be sure boards have the right numbers to understand how the organization is doing.

Auditors paying attention to media coverage is also helpful. If negative comments about the company are true, there is a problem. If what the media are reporting is false, there is a bigger problem of understanding why and how the news coverage resulted, especially if employees and former employees provided such information.

Sound the alarm

This subset of the Seven Signs underscores why auditors must stay alert for those in their organization who can't, won't, or don't speak up when ethical challenges arise. An internal auditor can mitigate the impact of these signs before it becomes a catastrophe. **NP**

Profiled organizations

In this four-part series, we'll consider the ethical and financial collapse of:

- Atlanta Public School system (APS)
- Boeing
- BP p.l.c. (formerly British Petroleum)
- Columbia University Medical School and New York Presbyterian Hospital
- FTX
- Madoff Investment Securities, LLC
- Nikola
- Theranos
- Wells Fargo
- WeWork

Marianne M. Jennings, JD, is a Professor Emeritus of Legal and Ethical Studies in Business at the W.P. Carey School of Business, Arizona State University, where she taught for 35 years. Her book The Seven Signs of Ethical Collapse *(St. Martin's Press, 2006) has received several book awards, including recognition of the* Library Journal. *Her next book,* Hornswoggled: How Management Books, Gurus, Theories, and Fads Harm Organizations, *is forthcoming in 2026. You can reach Marianne at Marianne.Jennings@asu.edu.*

[5] Stacy Cowley, "Fake Accounts at Wells Fargo Raised Alarms Starting in 2005," *New York Times*, October 12, 2016, p. B1.

[6] "Independent Directors of the Board of Wells Fargo & Company, Sales Practices Investigation Report," April 10, 2017, p. 32.

AZBEE AWARD ARTICLE ENCORE

Behavioral Health Billing Compliance

Close the gap between documentation and revenue integrity

By Sonda J. Kunzi, CPC, COC, CPB, CRC, CPCO, CPMA, CPPM, CPC-I

Behavioral health billing has unique challenges. Services are complex, documentation standards vary by payer, and organizations often struggle to connect clinical work to the codes they submit. These issues create significant risks for noncompliance, overpayment, and revenue loss.

This article outlines frequent problem areas found in behavioral health audits and offers practical steps to strengthen oversight, improve documentation, and reduce risk.

Why behavioral health billing is risky

Behavioral healthcare is, at least since COVID-19, one of the most audited and error-prone areas of healthcare billing. The reasons are clear:

Multiple payer rules – Medicare, Medicaid, managed care organizations, and commercial insurers each have different documentation and billing standards.

Supervision requirements – Services are often delivered by dependently licensed (see sidebar) or unlicensed certified providers with Medicaid-based services under a supervising provider. If supervision rules are misunderstood or poorly documented, billing is noncompliant.

Disconnect between treatment plans and billing – Often, organizations fail audits because the progress notes do not support the billed code or align with the initial assessment or treatment plan. This is inherently different from other types of services such as evaluation and management (E/M) codes that only consider services delivered during the encounter or on the encounter date. Behavioral health reviews require consideration of more than just the progress notes.

Complex service types – Psychotherapy, crisis care, and now more community-based support such as detoxification (detox), residential case management, and peer support require documentation that reflects interventions, progress, and clinical necessity.

A dependently licensed* behavioral health professional is an individual who is authorized to practice but must do so under the supervision of a more senior, independently licensed clinician. The specific requirements are determined by each state's licensing board, so titles and requirements vary by state, but common examples include:

- Licensed Professional Counselor (LPC): In some states, an LPC is a dependent license that requires supervision.
- Licensed Master Social Worker (LMSW): In some states, an LMSW must work under the supervision of a higher-level license, such as a Licensed Clinical Social Worker (LCSW).
- Post-Doctoral Fellow or Resident: In many fields, individuals must complete supervised practice after finishing their degree before they are eligible for full licensure.

**This link is specific to Ohio, but the explanation it offers is reasonably universal.*

Substance use disorder (SUD) programs introduce additional layers of complexity. Payers often require documentation consistent with the American Society of Addiction Medicine (ASAM) criteria for level-of-care decisions, yet organizations fail to consistently capture this information. Detox, intensive outpatient (IOP), and residential treatment each require different documentation standards, and inadequate evidence supporting medical necessity for the chosen level of care

Substance use disorder programs introduce additional layers of complexity.

is frequently brought forth as an adverse audit finding. For you, this means understanding the ASAM framework and reviewing whether records clearly justify the intensity and setting of services provided. Your review of one encounter might require reviewing the episodic care of different disciplines' contributions to the documentation overall.

Different types of substance use disorder providers add layers to the complexity of documentation, coding, and billing. Some facilities are providing medication-assisted treatment only, acting as an Opioid Treatment Program. They also have many different ways to bill their services based on Medicare vs Medicaid vs commercial payers. In this article, we only scratch the surface of the unique requirements facing these providers.

Auditor takeaway

A service may be clinically appropriate but fail an audit if payer rules for documentation, supervision, or medical necessity are not met. Learn all elements that may be considered in the payer's determination of medical necessity. Make sure your organization's different disciplines are working together, not independently.

Common documentation gaps

Behavioral health audits frequently uncover the following documentation issues:

- *Vague or repetitive progress notes* – Notes are sometimes nearly identical across sessions, with little detail about patient progress or the interventions provided.
- *Outdated or generic treatment plans* – Plans lack individualized goals or are not updated when the patient's condition changes.
- *Incorrect use of add-on codes* – Add-on codes such as 90833 (psychotherapy with E/M) or 90785 (interactive complexity) are often billed without meeting documentation requirements.
- *Improper use of crisis codes* – Codes 90839 and 90840 are billed when the notes do not clearly support the time spent or the severity that justifies the crisis designation.

In SUD programs, additional documentation gaps include the lack of ASAM criteria to justify the level of care, incomplete discharge or transition planning, and progress notes that fail to support continued stay at higher levels of care, such as residential treatment, when outpatient criteria are met. These gaps are significant because payers increasingly require robust justification for both admission and continued stay in SUD programs.

Auditor takeaway

You should compare progress notes to treatment plans (and the most recent assessment) and verify that the documented interventions align with problems identified in the assessment and active goals developed in the treatment plan. Understanding ASAM criteria and ensuring the clinical team integrates that information into documentation will be important to the entire organization.

Behavioral health operational red flags

Operational and system-level practices often contribute to compliance risks, so audits should extend beyond reviewing individual progress notes to look for:

- *Template overuse* – Electronic health records (EHRs) sometimes include auto-populated content that appears identical across multiple patients. This may indicate "note cloning," which can undermine the accuracy of the record.
- *Weak audit trails* – Missing or incomplete audit trails make it difficult to verify when entries were made, edited, or co-signed.
- *Lack of coding oversight* – A high volume of the same Current Procedural Terminology (CPT) code (for example, consistent billing of 90837 for 60-minute psychotherapy) may suggest upcoding or a failure to document varying session lengths.

For SUD services, per diem bundled billing creates additional risks. Facilities may inappropriately bill separately for psychiatric or primary care services that are already included in the bundled per-diem rate. You should review payer contracts, policies, and claims to ensure that only services legitimately excluded from the per diem are billed separately.

Auditor takeaway

Audit for variability. If every note looks the same, every psychotherapy session is billed at the highest duration, or supervision is never explicitly documented, those are signs that controls are weak or nonexistent. Actual payer contracts play a role in understanding when unbundling occurs in the SUD sector. This is when collaboration with clinical and operational team members is essential for billing compliance.

Key behavioral health risks

Behavioral health billing risks typically fall into three categories:

- *Documentation risk* – Notes do not reflect medical necessity, services rendered, or the time spent.
- *Compliance risk* – Supervision requirements are not followed or documented, particularly when dependently licensed or unlicensed providers render services.
- *Revenue cycle risk* – Claims are denied or underpaid due to mismatched coding, poor treatment plan integration, or missing prior authorizations.

Each of these risks can result in repayment obligations, penalties, or lost revenue.

Auditor takeaway

Internal or external audit teams can reduce risk and strengthen behavioral health compliance by:

- *Developing behavioral health-specific audit tools* – Include checklist items for treatment plan linkage, time documentation, supervision verification, and CPT code accuracy.
- *Performing targeted reviews* – Select high-risk services such as crisis intervention, psychotherapy add-ons, and community-based services for deeper review.
- *Engaging clinical leadership* – Partner with clinical teams early to interpret ambiguous notes and ensure findings lead to meaningful corrective action. A collaborative approach is key!
- *Monitoring denial trends* – Review denial trends for patterns that may indicate upstream process issues, while recognizing that these denials typically occur before documentation or medical necessity is ever evaluated. These trends often reveal systemic issues.
- *Providing education* – Use audit findings to drive targeted training for clinicians, supervisors, and billing staff. Remember to show the good with the bad. Support the right way to document, do not just include education based on the wrong way to document. Providers are used to hearing what they should not do and are usually more interested in what they should do.

For substance use disorder programs, you should specifically evaluate whether documentation includes ASAM criteria for level-of-care determinations, validate that services billed outside of bundled per-diem rates are appropriate, and confirm that provider types delivering SUD services are eligible under state Medicaid and payer-specific requirements.

Sample Audit Questions for Behavioral Health Encounters

Audit Focus	Sample Questions
Treatment plan	• Is there a current, individualized plan with measurable goals?
Progress notes	• Do notes clearly support the billed service type and duration?
Supervision/provider type eligibility	• If unlicensed staff provided the service, is supervision documented appropriately? Are providers delivering SUD services eligible and credentialed under payer and state Medicaid Rules?
Time-based services	• Is time documented, and does it match the code billed?
Code accuracy	• Do codes align with documented interventions and payer rules? • Is there accuracy with coding per diem and professional services?

(See Exhibit 1 for a full checklist)

Exhibit 1 – Comprehensive Behavioral Health Audit Checklist

You can use this checklist to evaluate the compliance of behavioral health services. It covers treatment planning, documentation, coding, supervision, and operational controls to ensure claims are supported and compliant with payer and regulatory requirements. This is a general list and is not intended to replace specific payer requirements. Please make sure to understand payer requirements for behavioral health services.

Audit Focus	Questions for Evaluation of Data and Documentation
System and process	• Are EHR templates used appropriately without overuse or note cloning? • Is there a clear audit trail for documentation edits, co-signatures, and supervisory notes? • Are denial trends reviewed to identify front-end process issues? • Is there a process for regularly auditing behavioral health documentation and providing feedback to clinical staff? • Are prior authorizations and eligibility checks documented and aligned with billing practices?
Assessment/treatment plan	• When was the last assessment to evaluate the client? Within 12 months? • Is there a current, individualized treatment plan with measurable goals?
Progress notes	• Do progress notes clearly support the billed service type and duration? • Are interventions documented with enough detail to reflect active treatment? • Is time documented for all time-based codes, and does it match the CPT code billed?
Provider credentials and supervision	• Is the rendering provider credentialed and authorized to deliver the billed service? • If unlicensed staff provided the service, is the appropriate level of supervision documented? • Are incident-to or general supervision requirements met and documented?
Coding and billing	• Do billed CPT and ICD-10 codes match the conditions and services documented in the record? • Is there evidence pointing to potential upcoding or overuse of high-level codes (e.g., 90837 for every psychotherapy session)? • Are modifiers used appropriately and supported by documentation? • Do billing patterns align with payer-specific rules (e.g., Medicaid vs. Medicare)? • As applicable: Are crisis intervention codes (90839, 90840) supported by documentation of severity and time? • As applicable: Are add-on codes (e.g., 90833, 90785) supported by documentation that meets all criteria?

	Additional Substance Use Disorder Considerations
ASAM criteria	• Does documentation include ASAM criteria supporting the level of care for admission and continued stay?
Level-of-care justification	• Do progress notes justify the current level of care (e.g., residential, IOP) based on clinical need?
Bundled billing	• Are services billed outside per-diem bundles appropriate and justified?
Discharge/transition planning	• Is there documentation of discharge planning and transitions to lower levels of care when appropriate?
Provider type eligibility	• Are providers delivering SUD services eligible and credentialed under payer and state Medicaid rules?

Practical steps for strengthening compliance

Improving compliance in behavioral health requires cross-functional action:

- *Establish clear supervision protocols* – Ensure that supervisory requirements are well-documented and integrated into workflows.
- *Leverage EHR capabilities wisely* – Use templates carefully to maintain efficiency without compromising note quality.
- *Implement routine internal audits* – Perform regular reviews to catch issues before they become external audit findings.
- *Integrate billing and clinical teams* – Encourage collaboration so documentation reflects both clinical care and payer requirements.

Conclusion

Behavioral health compliance is complex, but you can make a meaningful impact by focusing on the right risks, developing tailored audit tools, and working closely with clinical and revenue cycle teams. By identifying and correcting weaknesses in documentation, supervision, and coding, organizations can reduce compliance exposure and protect revenue. **NP**

Sonda J. Kunzi, CPC, COC, CPB, CRC, CPCO, CPMA, CPPM, CPC-I, is the founder and CEO of Coding Advantage, LLC, a healthcare consulting firm specializing in behavioral health compliance and revenue cycle optimization. Her 35 years of experience in healthcare include comprehensive knowledge of coding concepts, documentation and training, compliance, and healthcare reimbursement methodology. She can be reached at skunzi@codingadvantage.com and 866-530-5705.

Providers are used to hearing what they should not do and are usually more interested in what they should do.

CHIAP
Certified Healthcare Internal Audit Professional®

The CHIAP Certification is the only professional certification unique to healthcare internal auditors. Take the next step in your career by adding this valuable certification to your resume!

Start Your Exam Preparation Today...

Review the complete Body of Knowledge (BOK) outline in the CHIAP Candidate Handbook.

- Test your knowledge with over 50 Sample Exam Questions.
- Watch the 8-part BOK Webinar Series.
- Search for additional resources in the AHIA Virtual Learning Audit Resource Center.
- Visit the AHIA website for more information on Exam Preparation Resources.
- FAQs