

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

# COMPLIANCE TODAY

MAGAZINE

JULY 2025

**SHAWN MARCHESE, CHC**

SENIOR VICE PRESIDENT, COMPLIANCE  
OFFICER AT ACCESS TELECARE

## BUILDING CULTURES OF COMPLIANCE (P8)

Compliance risk  
assessment:

Mandatory or not? (P14)

False Claims Act: Preparing  
for and navigating internal  
complaints (P20)

Your role as an ACO  
compliance officer:  
Essential knowledge and  
strategies (P28)



**HCCA**



# HEALTHCARE COMPLIANCE ACADEMIES

## BRIDGE THE GAP BETWEEN PRINCIPLES AND PRACTICE

Learn key compliance fundamentals, build critical thinking skills through applied learning, and connect with your compliance peers in a highly interactive educational experience that will prepare you for real-world compliance management.



### HEALTHCARE BASIC COMPLIANCE ACADEMIES

Improve compliance program effectiveness with an understanding of the Seven Element approach.

July 21–24, 2025 • Nashville, TN    September 8–11, 2025 • Scottsdale, AZ    December 8–11, 2025 • Anaheim, CA  
August 11–14, 2025 • Jersey City, NJ    October 6–9, 2025 • San Antonio, TX

### HEALTHCARE PRIVACY COMPLIANCE ACADEMIES

Understand key regulations, privacy laws, and best practices for protecting sensitive data.

August 11–14, 2025 • Jersey City, NJ    December 8–11, 2025 • Anaheim, CA

### HEALTHCARE RESEARCH COMPLIANCE ACADEMIES

Maintain research integrity with a sound knowledge of research compliance regulations.

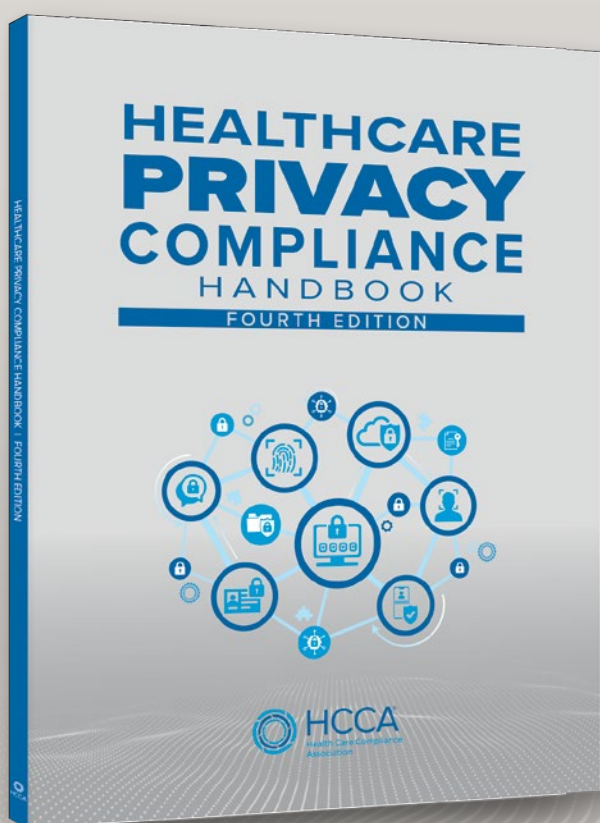
September 8–11, 2025 • Scottsdale, AZ

Learn more and register  
[hcca-info.org/academies](https://hcca-info.org/academies)



# Stay ahead of privacy regulations and emerging trends

The *Healthcare Privacy Compliance Handbook, 4th Edition* is designed to help you navigate the complex privacy landscape and keep patient information safe and private.



Written and updated by faculty of HCCA's Healthcare Privacy Compliance Academy, the fourth edition of our go-to handbook features updated content as well as brand new articles and resources including:

- Chapter 3: Information Sharing: Business Associates and Third Parties
- Chapter 5: Health Plan Privacy and Security
- Appendix 1A: HIPAA Privacy and Security Definitions
- Appendix 5A: ChatGPT Output
- Appendix 5B: Cybersecurity Trends
- Appendix 6A: FERPA Definitions
- Appendix 8A: Major Changes in the New Part 2 Rule/Definitions

Three purchasing options are available: softcover print book, online access, and a money-saving print + online bundle.

**Get your copy today**  
[hcca-info.org/hcpch](https://hcca-info.org/hcpch)





“ Be transparent;  
chances are, you’re  
not the only person  
who doesn’t know  
the answer. ”

See page 10



## Features

8 **Meet Shawn Marchese: Building cultures of compliance**  
an interview by [Shawn Marchese](#)

14 [\[CEU\]](#) **Compliance risk assessment: Mandatory or not?**  
by [Melinda Shapiro](#) and [Ximena Restrepo](#)  
Compliance professionals know that the compliance program is essential for identifying, reporting, and addressing suspected wrongdoing or noncompliance with company policies, or local, state, or federal laws. A compliance risk assessment (RA) is crucial to ensure a program’s effectiveness. Whether recommended or mandatory activity, learn how RAs are necessary to systematically uncover vulnerabilities and demonstrate due diligence.

20 **False Claims Act: Preparing for and navigating internal complaints**  
by [John Eason](#)  
The federal government’s False Claims Act (FCA) enforcement and qui tam lawsuits continue to target the healthcare industry — and there are no signs that FCA activity is slowing. In this environment, healthcare providers must consider when they might face an internal FCA-related complaint. Is your organization prepared to act promptly and reasonably *when* — not if — that moment arrives?

28 [\[CEU\]](#) **Your role as an ACO compliance officer: Essential knowledge and strategies**  
by [Divya M. Schavio](#) and [Joseph Grant](#)  
As private payers follow Centers for Medicare & Medicaid (CMS) Innovation’s and federal programs’ lead, CMS continues to drive a patient-centered approach in an industry-wide transformation. And with the continued expansion of Alternative Payment Models, the demand for Accountable Care Organization (ACO) compliance officers is increasing. Find out how an ACO compliance officer differs from other compliance roles and how to ensure success in this evolving field.

# COMPLIANCE TODAY

A PUBLICATION OF  
THE HEALTH CARE  
COMPLIANCE ASSOCIATION

July 2025

## Columns

- 13 **Exhale**  
by [Catherine Boerner](#)
- 27 **Managing compliance**  
by [Betsy Wade](#)
- 33 **V’s view on compliance transformed**  
by [J. Veronica Xu](#)
- 39 **Research reflections**  
by [Kelly M. Willenberg](#)
- 45 **All aboard on compliance**  
by [Frank Ruelas Sr.](#)

## Departments

- 5 **HCCA News**
- 7 **People on the move**
- 57 **Takeaways**
- 58 **Upcoming events**



## Articles

### 34 **Maintaining compliance in the face of disaster**

by **Jerry Kaner**

The fast digital transformation of the healthcare industry has transformed how organizations plan for and respond to natural disasters. Crises can expose healthcare IT vulnerabilities, threatening patient safety, data security, and HIPAA compliance. Disaster preparedness must be continuous. Discover how your healthcare organization can maintain compliance and protect patient privacy during disasters.

### 40 **When public voices vanish: Legal risks to health transparency**

by **Stacey Lee**

Public participation has long served as a cornerstone of health regulatory development. Yet, recent shifts in federal agency approaches to stakeholder engagement create urgent compliance risks for healthcare organizations. As federal agencies alter their procedures for public input, compliance officers face immediate challenges in tracking, interpreting, and implementing rapidly changing regulations. Learn how to navigate these updates without the benefit of transparent regulatory development processes.

### 46 **[CEU] Ransomware risk readiness**

by **Ali Pabrai**

Ransomware attacks pose a substantial cybersecurity threat to healthcare organizations. Although email remains a major method for ransomware malware and phishing attacks, today's hackers are advanced and persistent, integrating artificial intelligence tools to accelerate attacks. Discover ways to better prepare and move from ransomware risk to ransomware readiness.

### 50 **Is your cybersecurity program really valuable? Three questions to explore**

by **Eric Shoemaker**

The Change Healthcare breach sent a strong signal to those across the healthcare industry: We are at greater risk of having patient health information and other valuable data compromised. One study found that 37% of healthcare organizations are without an incident response plan. If you're one of them, there are three questions to ask of your organization that will help create a solid cybersecurity program.

## VOLUME 27, ISSUE 7

### EDITORIAL BOARD

Gabriel Imperato, Esq., CHC, CT Contributing Editor  
Managing Partner, Nelson Mullins

Donna Abbondandolo, CHC, CHPC, CPHQ, RHIA, CCS, CPC  
Chief Compliance Officer, Bon Secours Mercy Health

Charles E. Colitre, BBA, CHC, CHPC  
President, Healthcare Compliance Consultants

Cornelia Dorfschmid, PhD, MSIS, PMP, CHC  
Executive Vice President, Strategic Management Services, LLC

Adam H. Greene, JD, MPH, Partner, Davis Wright Tremaine LLP

Margaret Hambleton MBA, CHC, CHPC  
President, Hambleton Compliance LLC

Gary W. Herschman, Member of the Firm, Epstein Becker Green

David Hoffman, JD, FCPP  
President, David Hoffman & Associates, PC

Donnetta Horseman, CHC, CHPC, CHRC, CIPP/US  
Senior Vice President, Chief Ethics and Compliance Officer, City of Hope

Emmelyn Kim, MA, MPH, MJ, CHRC, VP  
Research Compliance & Privacy Officer, Office of Research  
Compliance, Northwell Health

Richard P. Kusserow, President & CEO, Strategic Management, LLC

Michael A. Morse, Esq., CHC  
Partner, Pietragallo Gordon Alfano Bosick & Raspanti, LLP

Erika Riethmiller, CHC, CHPC, CISM, CPHRM, CIPP/US  
Chief Privacy Officer, Sr. Director Privacy Strategy, UCHealth

Daniel F. Shay, Esq., Attorney, Alice G. Gosfield & Associates, PC

James G. Sheehan, JD, Chief of the Charities Bureau  
New York Attorney General's Office

Lori Strauss, CHC, CHPC, CCEP, CHRC  
Immediate past Chief Compliance Officer, Stony Brook Medicine

Debbie Troklus, CHC-F, CCEP-F, CHRC, CHPC, CCEP-I  
President, Troklus Compliance Consulting

Barbara Vimont JD, RHIA, CHC  
Corporate Compliance Director, Parkview Health System, Inc.

**PUBLISHER:** Craig Larson  
[craig.larson@corporatecompliance.org](mailto:craig.larson@corporatecompliance.org)

**MAGAZINE EDITOR:** Scott Moe, 952.567.6207  
[scott.moe@corporatecompliance.org](mailto:scott.moe@corporatecompliance.org)

**ADVERTISING:** [advertising@corporatecompliance.org](mailto:advertising@corporatecompliance.org)

**COPY EDITOR:** Julia Ramirez Burke  
[julia.ramirez.burke@corporatecompliance.org](mailto:julia.ramirez.burke@corporatecompliance.org)

**DESIGN & LAYOUT:** Pete Swanson  
[pete.swanson@corporatecompliance.org](mailto:pete.swanson@corporatecompliance.org)

**PROOFREADER:** Jack Hittinger  
[jack.hittinger@corporatecompliance.org](mailto:jack.hittinger@corporatecompliance.org)

**PHOTOS ON FRONT COVER, PAGE 2 & 8:** Tara Welch  
Photography

# 2025 COMPLIANCE INSTITUTE RE

**HCCA's 29<sup>th</sup> Annual Compliance Institute** is in the books, and it was a truly memorable event as always. Our attendees in Las Vegas enjoyed lively discussion, informative and thought-provoking educational sessions, networking receptions, presentations and engagement with solution providers, a new Passport to Prizes Exhibit Hall incentive, and a veteran-focused community service activity.

Our virtual attendees had the opportunity to engage with both on-site and virtual peers as well as learn from a variety of sessions live-streamed directly from the conference venue.

Huge thanks to all who helped make CI 2025 such a great experience. We couldn't do it without our dedicated sponsors and exhibitors, the behind-the-scenes track chairs, and fabulous session leaders. We're grateful to all who attended, whether in-person or virtually. Your commitment to and passion for compliance is what drives the CI and our association overall, and we are honored to support your goals.

We look forward to seeing you all in Orlando in 2026 as we celebrate the milestone 30<sup>th</sup> year of the Compliance Institute! [hcca-info.org/2026CI](https://hcca-info.org/2026CI)





# TROSPECTIVE

Attendees enjoyed a variety of networking activities, including SpeedNetworking and evening receptions.



A high volume of candidates took advantage of the opportunity to sit for the CHC®, CHRC®, and CHPC® exams on the last day of the event.



HCCA partnered with the United Way for an on-site volunteer activity, helping to prepare “thank you” kits for homeless and at-risk veterans. The kits contained items such as socks, tissues, combs, playing cards, hand sanitizer, and a personal note. Our participants packed an incredible 333 kits—thank you all!

# ATTENDEE VOICES



**Madhavi Perumpalath, CHC, CPC, C...** · 2nd · [Follow](#) · [...](#)  
Director of Compliance  
2w · Edited · [🔒](#)

Excited to share my recent experiences at the HCCA Compliance Institute 2025!

This event was an incredible opportunity for learning, sharing knowledge, and expanding my professional network. Engaging with industry leaders and fellow compliance professionals has enriched my understanding of the latest trends and best practices in our field.

I'm grateful for the insightful discussions and the chance to exchange ideas with so many passionate individuals. Together, we're shaping the future of compliance!

Looking forward to applying what I've learned and continuing these valuable connections. Let's keep the conversation going! 🙌🏻 [#HCCA2025](#) [#Compliance](#) [#Networking](#) [#ContinuousLearning](#)



**Alka K.** · 2nd  
Privacy and Compliance Professional  
2w · [🔒](#)

[+ Follow](#) · [...](#)

Had a great time attending the [Health Care Compliance Association \(HCCA\)](#) 29th Annual conference [#hccaci25](#) in Las Vegas!  
Had the opportunity to meet old compliance friends and make some new ones. The [#hccaci](#) was full of engaging and inspiring sessions.

A huge thanks to the [#hcca](#) team members for organizing and the sponsors for supporting such a fun and informative event!

Looking forward to attending the 30th CI in Orlando next year!



**Jennifer Marx M.S., CCC-SLP, CHC, RAC-CT, ...** · 3rd+ · [Follow](#) · [...](#)  
Healthcare Clinical and Compliance Officer, Training Expert, Leader, Visi...  
2w · Edited · [🔒](#)

I just wrapped up an inspiring few days at the 29th Annual [Health Care Compliance Association \(HCCA\)](#) Compliance Institute in Las Vegas.

It was an incredible opportunity to connect with peers, share ideas, and dive deep into the evolving challenges and innovations in healthcare compliance. I am reminded that earning a certification is just the beginning—the real impact comes from the continuous commitment to learning, growing, and staying ahead in a constantly changing environment. Whether it's navigating new regulations, embracing emerging technologies, or fostering a culture of integrity, staying engaged and informed is what empowers us to lead with purpose.



**Natak Gordon, CHPC, SHRM-CP** · 3rd+ · [Follow](#) · [...](#)  
Compliance @ Pomelo  
2w · [🔒](#)

Just got back from my first [Health Care Compliance Association \(HCCA\)](#) conference in Las Vegas last week, and it was an incredible experience!

It was an honor to be in the room with so many Compliance OGs! I left with a ton of golden nuggets that I'm excited to bring back to the team at Pomelo.

Some of my favorite sessions tackled key compliance topics such as conducting meaningful risk assessments, developing and maintaining a strong HIPAA privacy program, managing third-party risk, and sustaining an effective organization-wide compliance program.

One of the biggest highlights was attending alongside my manager, [Kimberly Silverio MLS, CHC, CHPC](#), who's been a constant source of support since day one. Huge shoutout to her—and to the team at [Pomelo Care](#)—for investing in my professional development and creating space for me to grow in my career.



**Anisa Scott** · 2nd  
HIPAA Privacy Analyst  
1w · [🔒](#)

[+ Follow](#) · [...](#)

Still beaming with joy and excitement about all of the insights, perspectives, and new ideas gained and learned at the [Health Care Compliance Association \(HCCA\)](#) Compliance Institute 2025. The conversations and shared knowledge were instrumental to help understand and navigate the complex challenges, trends, and best practices in our field. What I enjoyed most about the [#HCCAcI](#) is that there were opportunities for not only compliance/privacy program development, but also professional growth!

Some valuable take-aways:

🗨️: We are here to help people, not to catch people - we are 'compliance lifeguards'

🧠: Focus on the person, then on the problem

💡: View challenges and mistakes as a learning opportunity - what did I miss so I can learn?

🗨️: Teach for understanding and tailor your conversations - do they understand the external impact(s) of their actions?

**NOW  
AVAILABLE**

# New edition just released: update your library today!

Whether you have the 3<sup>rd</sup> edition of this essential text and want the latest insights or are looking for a new resource to help you maintain a compliant research environment, look no further! The 4<sup>th</sup> edition of our trusted handbook includes updates to every chapter as well as new content on artificial intelligence and its impact on compliance teams and research facilities.

## Key areas addressed include:

- **NEW!** Artificial intelligence
- Conflicts of interest
- Scientific integrity
- Biosecurity and biosafety
- Human subject protections
- Research using animals
- FDA regulation
- Privacy and security
- Records management
- Data and safety monitoring
- Clinical trial billing
- Grant management
- Auditing & monitoring
- Export controls

## AVAILABLE IN THREE OPTIONS



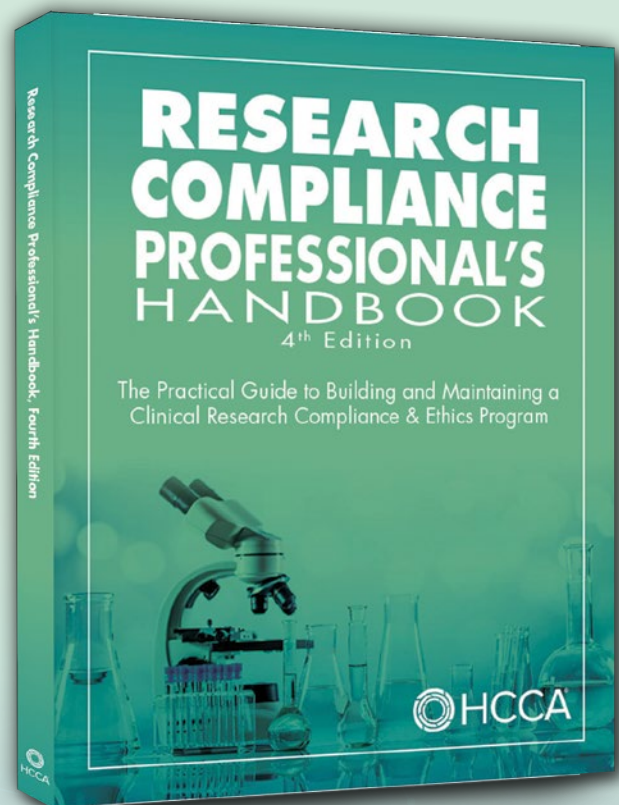
Online access



Softcover book



Print + Online bundle



**Buy now**  
[hcca-info.org/rcph](https://hcca-info.org/rcph)





# PEOPLE *on* *the* MOVE



## SHARE YOUR NEWS!

Celebrate career milestones with the compliance community and keep your colleagues up to date! Have you received a promotion, new credential, or industry recognition? Accepted a new position or added staff to your team?

Submit your news via email to  
[scott.moe@corporatecompliance.org](mailto:scott.moe@corporatecompliance.org)

- ◆ **Annie Shieh** started as Medicare compliance officer at Centene Corporation, based in Saint Louis, MO.
- ◆ **Laura McNamara** joined the University of Vermont Health Network as vice president, chief compliance and privacy officer, in Burlington, VT.
- ◆ **Alice Elford** is now director of Compliance, Johns Hopkins Care at Home, at Johns Hopkins Medicine, in Baltimore, MD.

**COMPLIANCE TODAY**  
is available online on

**COSMOS**<sup>®</sup>  
Navigate the Compliance Universe

**[compliancecosmos.org](https://compliancecosmos.org)**

# BUILDING CULTURES OF COMPLIANCE

## Meet Shawn Marchese

CHC

Senior Vice President,  
Compliance Officer  
at Access TeleCare

an interview by  
Adam Turteltaub

**Shawn Marchese**, CHC ([smarchese@accesstelecare.com](mailto:smarchese@accesstelecare.com), [linkedin.com/in/shawn-e-marchese/](https://www.linkedin.com/in/shawn-e-marchese/)), is a Senior Vice President, Compliance Officer at Access TeleCare in Dallas, TX.

**Adam Turteltaub** ([adam.turteltaub@corporatecompliance.org](mailto:adam.turteltaub@corporatecompliance.org), [linkedin.com/in/adamturteltaub/](https://www.linkedin.com/in/adamturteltaub/)) is the Chief Engagement Officer at SCCE & HCCA in Eden Prairie, MN.





**AT:** You've worked in healthcare compliance for over 20 years now. What got you into the field?

**SM:** Early in my career, I was working at a regional health plan. It wasn't a compliance role, but my desk was right next to the compliance team office, and I used to help out when they needed extra hands. I quickly realized that this was work I would love to be doing and would be good at: developing training, reviewing beneficiary materials, regulatory filings. It may not sound like the most exciting work, but I saw a chance to flex my critical reading and writing skills, which I've always enjoyed. The fact that this work supported a good cause—keeping the company on the right side of the law—made it that much more appealing to me. So, one day a position opened, and I got the job. I guess the rest is history!

**AT:** How has compliance changed over the years?

**SM:** A true compliance program—even if it's just one person—has become more of a must-have for organizations of all sizes. Years ago, smaller organizations still often took a purely reactive approach to compliance: reacting to reports, audits, regulatory inquiries, etc., as they popped up in a perpetual game of “Compliance Whack-a-Mole” because there was no directive from the top to do otherwise. The chief compliance officer's role—if it existed—might be one of many hats worn by someone in a more general operational role.

Now, we're seeing boards and C-suites having a greater understanding of compliance concepts and demanding more proactive oversight: kicking the

proverbial tires, stress testing the business, and reporting on known risks and what's being done about them. This means a dedicated compliance leader is a must. And that senior-level buy-in and awareness means it's more important than ever that compliance leaders be able to manage all the elements of a compliance program effectively and report in a way that satisfies those executives.

**AT:** How do you think working in compliance has changed you?

**SM:** It's opened my eyes to thinking about risk in a nuanced way. Early on in my compliance career, I got to work closely with sales and marketing teams. Those partnerships were great for my professional development, and they're still some of my favorite teams to work with in every organization I've been at. I had to get really good at giving nuanced responses, being precise in terms of what's required versus nice to have, and finding ways to “get to yes.” That was invaluable to my career because I learned about risk tolerance and how to manage the most meaningful risks without standing in the way of strategic goals.

That's helped me in life outside of work as well. Just as every organization has risks—and it's not our job to shut down every idea or process that involves some risk—life is the same way. There are risks inherent in just going out there and living our lives, taking chances, trying to achieve personal goals. Working in compliance has helped me get comfortable with a little discomfort, focus on the risks I can control, and take chances. (Thanks for coming to my TED Talk!)

## Working in compliance has helped me get comfortable with a little discomfort, focus on the risks I can control, and take chances.

**AT:** You recently spent two-plus years working at a startup. How has that been different from working in a more established institution?

**SM:** My favorite thing about working at startups is that you get a chance to try on a lot of different hats. Established institutions—especially larger organizations—tend to create deep specialization in job roles that are very well defined. It's harder to step outside the lane of your narrowly defined role and get a chance to work on something new.

Startups are the exact opposite. Teams are small and doing more with less. Processes are fluid and, a lot of times, they aren't even fully defined yet. So, there are many opportunities to step up to new challenges, roll up your sleeves, and learn something new to solve a problem the business hasn't seen before. As a compliance officer at startups, I've gone beyond my compliance role to do business development, improve operational processes, manage

provider relationships, stand up procurement workstreams, and more that I'd never get to touch working at a bigger organization. This is a great way to improve your skill set laterally, which opens the door to roles outside compliance if you ever want to go that way. You never know what you might be good at until you try it!

**AT:** What advice would you give to others considering whether the startup life is right for them?

**SM:** To succeed in a startup, you'll have to (1) be curious and (2) be comfortable with a little bit of uncertainty. Curiosity is an essential trait for any compliance professional because it's your job to ask questions, challenge assumptions, and have a basic understanding of processes that nobody is going to explain to you: you have to ask. But it's especially crucial in a startup because often, the question on your mind has never been asked before and probably should be. This means you need to be comfortable, not just asking questions to test your business partners, but also be brave enough to ask questions when you don't understand something.

This gets to my second point about being comfortable with uncertainty. In startups, a lot of experiences are new, and the whole organization is learning together. You're building the plane while you're flying it. So don't be afraid to ask questions because you want to look smarter than everybody else. Be transparent; chances are, you're not the only person who doesn't know the answer. That transparency will build trust with your business partners.

If this all sounds exciting to you, startup life may be right for you.

**AT:** Let me follow up by asking, what advice would you give for most effectively establishing a compliance program at a startup?

**SM:** In addition to everything I previously said, establish yourself early as a collaborator and an information resource. Get to know leaders in all the functional areas of your organization: they're the people whose buy-in you're going to need to build your compliance program and whose support you're going to need to get team members at all levels on board. Find out what those leaders are concerned about and use your knowledge and influence to help them solve those problems in any way you can — even if they're not explicitly compliance risks. Show them that compliance is there to help them solve their problems and achieve their goals. This will build strong relationships and credibility that you'll need later when you need their support to push out training and policies, assess and monitor risks, and investigate potential noncompliance in their areas. And if you ever need to put the brakes on something for compliance reasons, it's a lot easier to do that with a partner that you've got a solid history with as opposed to someone you only reach out to when there's a problem.

**AT:** The great thing about a startup is that, from a culture perspective, it's fresh, untouched ground. What do you think are the keys to creating the right culture?

**SM:** That's absolutely right. Get into a startup early enough, and you can make a strong impression on the future culture of that organization. The best way to do that, I think, is to become an advocate and enabler for the

company's mission. Most startups are very mission-driven, and the people who work there strongly believe in what the company is trying to do: "empower our doctors," "achieve better outcomes for our patients," whatever it is. Figure out how compliance can support that mission, and make that case with leaders and employees — from the top down and the bottom up — that compliance and ethics are an integral part of that mission; that's where you come in. That way, if they believe in the mission, they will believe in what you're doing with the compliance culture.

**AT:** How can we best sustain one?

**SM:** Deliver on the promises you made. If you've convinced everyone in the organization that compliance is there to support them, then demonstrate that every day. Live the values. Support the mission. Be present and lean in. Be a collaborator — not the "Department of No." And perhaps most importantly, deliver on the promise to employees at all levels: protect those who speak up, make them feel heard, and ensure compliance is there for them the way you said it would be. Nothing kills culture faster than people thinking it's just a bunch of empty words.

**AT:** One key element is making sure that people know that compliance is there for them. What do you find is best for helping them see compliance that way?

**SM:** Be visible and vocal, preferably as the human being behind the role. This means different things at different levels: for leaders, it means connecting with them personally (in meetings



and one-on-one) to hear their concerns and work through issues together. For employees at a more tactical level, it means raising awareness of the compliance program through every channel at your disposal: staff meetings, newsletters, and training, of course.

I've gotten great results from introducing myself to every cohort of new employees as part of their onboarding, so they know my name and how to reach me. I've had so many people reach out to me or walk up to me at in-person meetings and say they remembered me from onboarding, and that made them feel comfortable coming to speak to me. That may not be possible at every organization, but if you can manage it, it's worth its weight in gold.

**AT:** What kinds of tools and resources should we provide?

**SM:** Anything that makes it easy to reach the compliance team is valuable. Compliance should absolutely have a page on the company intranet where people can find answers to frequently asked questions or raise concerns. A recurring feature in company newsletters is another great tool to remind people you're there and how to reach you. Include links to mailboxes where people can email you, as well as links to your compliance hotline or other reporting mechanisms. And quite possibly my favorite bit of new technology: QR codes! I've made QR codes that link to a compliance page or a reporting form and put them on posters in the office, presentation decks, and screen savers on company laptops. Make it easy for employees to find you; it'll increase your visibility and the frequency with which people reach out.

**AT:** How do we encourage workers to speak up? That's always a brave step.

**SM:** It absolutely is, and in some ways is the hardest hurdle to overcome. No matter how easy you make it to reach out to compliance, people won't do so if they don't feel safe. It's essential to reinforce your company's non-retaliation policy; remind team members that they can speak up without fear and say it in a way that doesn't feel mechanical. It's fine to have legal terms like "good faith reporting" in your code of conduct and policies, but when talking about these concepts informally, use simple words and warm, welcoming language. This sends the message that if they speak up, they'll find a human being on the other end.

But it's imperative that other leaders live and reinforce this message, too. That commitment to non-retaliation needs to be a reality for all leaders within the organization, and your compliance officer needs to be able to speak up to their peers, CEO, or board if that commitment isn't being met.

**AT:** Speaking of speaking up, you don't only speak up about compliance. You speak up a lot about the work of J.R.R. Tolkien. You're a part of a podcast about him, give talks, and even published a book about his work. Tell us about what made you so passionate about his writing.

**SM:** I wasn't expecting to get to talk about this in an interview about compliance! Thank you, I love this. I first read Tolkien's work in the 1990s, years before the movies came out. I read *The Hobbit* and *The Lord of the Rings*,

got hooked, and kept reading: really deep cuts, collections of unfinished drafts, stuff you have to be a real geek to get into. I'd read fantasy novels before, but reading Tolkien for the first time was like nothing else I'd ever experienced. Talk about building cultures! Tolkien built a whole fantasy world with thousands of years of history, invented languages, gods, monsters, and heroes. There's an entire mythology there, like ancient Greek or Norse, but it was all created by one person.

**It's essential to reinforce your company's non-retaliation policy; remind team members that they can speak up without fear and say it in a way that doesn't feel mechanical.**

And yet — at its heart — these are simple stories about ordinary people. Hobbits are the smallest people imaginable, literally, but they step outside of their comfortable little Shire and do something significant — not because they're the strongest or the bravest, but because it's the right thing to do. So, Tolkien's stories really speak to me, not just for the depth of the world he invented but for the ethical core of the story, too. I read a lot, but no author comes close to Tolkien for me.

**AT:** Has it helped you in your work as a compliance officer? Or has it just been a fun hobby?

**SM:** Podcasting and speaking publicly about Tolkien has been a fun hobby, for sure, but it's helped me in my career, too. I tend to be a bit, well, verbose on topics that are valuable to me. But the practice of preparing for a podcast or a speaking engagement—where I have a limited amount of time—has helped me learn the subtle art of editing: communicating the key stuff quickly in a way that gets my main point across and leaves space for my audience to ask me questions. It's also helped me learn how to answer tough questions on my feet in a live

setting. These are great skills to have for any speaking opportunity, from a 50-minute seminar talk to a five-minute slot in a board meeting.

**AT:** That's terrific. So, let me go back to the start of the interview. I asked you how the profession has changed in the last 20 years. What's your sense of how it will evolve over the next few years?

**SM:** As I mentioned earlier, I've seen a shift in the industry from reactive to more proactive compliance. I think that's going to lead to a trend of greater accountability: really walking the walk on compliance instead of just checking boxes. Employees

today expect more accountability from their organizations than they did years ago, and that includes ethical conduct. They want to feel safe and empowered to speak up and know that their concerns are listened to, and I think that mindset will continue to spread and drive compliance accountability. So, even if government agencies slow down on enforcement or regulation lags behind industry developments, we'll see more organizations lean into ethical and compliant culture because their employees demand it of them. I think that's a really exciting trend to look forward to in the compliance profession.

**AT:** Thank you, Shawn! CT

## Your guide to defining, assessing, and addressing risk

This book walks you through the compliance risk assessment process step by step. Learn how to build a robust process, avoid common pitfalls, and work towards continuous improvement.



Learn more  
[corporatecompliance.org/risk-intro](https://corporatecompliance.org/risk-intro)





# Artificial intelligence governance in healthcare

by Catherine Boerner

**J**ust when compliance professionals thought they were keeping up with compliance and privacy risks to the organization, artificial intelligence (AI) comes along with very new and unique challenges.

It will become important for compliance officers to be members of an AI governance committee in your organization. The committee members must educate themselves on AI opportunities in healthcare and which departments AI use requests are already coming from. Unfortunately, the requests to “use” AI may become more of a discussion about where employees are already using AI without an AI governance committee review and approval.

AI opportunities in healthcare will be present in many areas. It can be used for clinical outcomes, event predictions around readmissions, emergency room visits, sepsis, and length of hospital stay, and in areas for imaging for tumor diagnosis and progression.

AI can be applicable in operations and total cost of care to analyze cost and utilization, referrals, billing and collections, accounts receivable work queue optimization, staff volume, and fraud, waste, and abuse.


AI can be utilized in provider engagement for computer-assisted coding, scheduling, staff volume, voice-to-text, and clinical document summarization.

AI can be used for patient engagement chatbots, scheduling, digital assistants, patient engagement and satisfaction, and call volume forecasting.

## AI in Healthcare Statistics: Comprehensive List for 2025<sup>1</sup>

### Key takeaways

- ◆ “The global AI in healthcare market grew from **\$1.1 billion in 2016** to **\$22.4 billion in 2023**, marking a staggering **1,779% increase**.”
- ◆ “By **2030**, the global AI healthcare market is projected to soar to **\$188 billion**, driven by a **37% CAGR [compound annual growth rate]** from **2022 to 2030**.”
- ◆ “In the USA, the AI healthcare market is projected to grow from **\$11.8 billion in 2023** to **\$102.2 billion by 2030**, reflecting a **36.1% growth rate**.”
- ◆ “**AI-assisted surgeries** could shorten **hospital stays by over 20%**, with potential savings of **\$40 billion annually**.”
- ◆ “AI is expected to reduce healthcare costs by **\$13 billion by 2025**.”
- ◆ “The **AI-integrated medical imaging** market is anticipated to expand at a **26.5% CAGR** from **2021 to 2028**.”
- ◆ “**AI can rule out heart attacks** twice as fast as humans with **99.6% accuracy**.”
- ◆ “**94% of healthcare executives** reported expanding AI adoption during the **COVID-19 pandemic**.”
- ◆ “The **AI nursing assistant market** is forecast to reduce **20% of nurses’ maintenance tasks**, saving **\$20 billion annually**.”
- ◆ “By **2025, 90% of hospitals** are expected to utilize AI-powered technology for **early diagnosis and remote patient monitoring**.”

AI is integrating into society much more rapidly than computers, and AI affects more sectors simultaneously. So much to learn with so little time! 



**Catherine Boerner**  
JD, CHC

([cboerner@boernerconsultingllc.com](mailto:cboerner@boernerconsultingllc.com),  
[linkedin.com/in/catherineboerner](https://www.linkedin.com/in/catherineboerner))

*is the President of  
Boerner Consulting LLC  
in New Berlin, WI.*

### Endnotes

1. Sean Roy, “AI in Healthcare Statistics: Comprehensive List for 2025,” Dialog Health, accessed May 1, 2025, <https://www.dialoghealth.com/post/ai-healthcare-statistics>.

# COMPLIANCE RISK ASSESSMENT: MANDATORY OR NOT?

by Melinda Shapiro  
and Ximena Restrepo



**Melinda Shapiro**

*(mshapiro@nu.edu) is a Senior  
Director of Compliance at National  
University in San Diego, CA.*



**Ximena Restrepo**

*(xrestrepo@logan.org) is a Compliance  
and Privacy Partner at Logan Health  
in Kalispell, MT.*

**T**he compliance program plays an integral role in preventing, detecting, and responding to identified misconduct and noncompliant activities that may violate internal policies, procedures, and/or federal and state laws and regulations. One compliance program element foundational to the program's effectiveness is the compliance risk assessment (RA) function. An RA—whether conducted annually, every other year, or as often as necessary based on the size of the organization—must be conducted to identify and prioritize new risk areas, detect new trends, and develop corrective actions to meet regulatory compliance obligations. Regardless of being a recommended or mandatory activity, RAs are necessary to systematically uncover any vulnerabilities and simply demonstrate due diligence. Due diligence also includes conducting RAs annually as a best practice to ensure ongoing risk awareness and mitigation tracking.

## Evolution of the regulatory landscape

To better understand the importance of RAs, it is helpful to explore the historical context of their integration into U.S. government practices.

Corporate compliance began to evolve in the U.S. in the 1960s, following the bid-rigging and price-fixing conspiracies involving General Electric and Westinghouse.<sup>1</sup> This incident prompted the establishment of the first in-house corporate compliance programs. In 1977, during President Richard Nixon's administration, the Watergate investigation and the issues surrounding the Foreign Corrupt Practices Act (FCPA) highlighted the need for greater transparency and compliance. President Nixon's resignation marked a significant shift, leading to the passage of the Inspector General Act in 1978. In the 1980s, the Reagan administration initiated a major compliance effort aimed to address fraud, waste, and abuse within the procurement process to "provide for continuing improvement in the Department of Defense's peacetime and combative effectiveness."<sup>2</sup> This initiative was intended to improve the Department of Defense's effectiveness in both peacetime and combative situations, particularly in response to cases of fraud and resource misuse within the defense industry. In 1986, the Blue Ribbon Commission—commonly known as the Packard Commission—was established under President Ronald Reagan's Executive



Order 12,526. This commission issued a report that made several compliance recommendations to prevent and deter fraudulent practices.<sup>3</sup> Subsequently, in 1989, the Federal Trade Commission Office of the Inspector General (OIG) was created to specifically address government abuse and fraud. In response to these developments, the Defense Industry Initiative on Business Ethics and Conduct (DII) was formed, which resulted in the establishment of the five core code of conduct; these principles laid the groundwork for the evolution of compliance programs in the U.S. today:<sup>4</sup>

1. Act honestly to protect and provide (dealings, products, services)
2. Promote ethical values and nurture ethical culture (comms, training, etc.)
3. Establish and sustain effective business ethics and compliance programs (hotline, disclosures)
4. Share best practices (participate in DII Best Practices Forum)
5. Accountable to the public (sharing/reporting)

In 1991, the U.S. Sentencing Commission established and released the *Federal Sentencing Guidelines Manual*, which was developed based on the DII core principles.<sup>5</sup> These guidelines serve as a reference for prosecutors and clearly outline how the absence of corporate compliance can be considered a crime. Over the years, various updates have provided additional guidance to corporations on maintaining an effective compliance program.

### The value of RAs

RAs play a crucial role in an organization's efforts to identify, monitor, and implement policy

changes that demonstrate adherence to all seven elements of an "Effective Compliance and Ethics Program" (§ 8B2.1.(b)).<sup>6</sup>

When conducted on an ongoing basis, RAs become increasingly valuable as they demonstrate how the organization is taking a proactive and consistent approach to identify potential vulnerabilities or areas of noncompliance, in addition to new opportunities. It allows organizations and compliance officers to provide valuable insights to their board members and senior leadership when prioritizing risks based on potential *impact* and *likelihood* of recurrence.

To have an effective compliance program, one should conduct an annual compliance RA to update and ensure an effective annual auditing and monitoring (A&M) plan. As you create specific action plans, whether it is a targeted audit, updating policies, enhancing training, bringing external resources, or implementing other internal controls, it reduces the impact of compliance issues; it keeps leadership informed of new regulatory expectations.

Are you taking for granted the value of your RA? Table 1 (see page 16) contains a helpful list of questions and tips to help evaluate your current RA.<sup>7</sup>

### Additional recommendations from government agencies

#### 2004 USSG Chapter 8 2B.2 added the term "ethics" and RA requirement

The U.S. Sentencing Commission was established to develop the federal sentencing policy, known today as the U.S. Sentencing Guidelines (USSG). The USSG was to help the government and judges impose fair and consistent sentences/fines under the Sentencing Reform Act of 1984.

In 2004, the commission issued a news release regarding amendments made to USSG Chapter 8, Section 2B.1—Effective Compliance and Ethics Program.<sup>8</sup> The release detailed the amendment's goal which was to require organizations to identify areas of risks and give the compliance officer sufficient authority and resources to carry out the responsibilities to better promote organizational and ethical culture.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.<sup>9</sup>

### ECCP and FCPA evolution on assessing corporate compliance programs

The U.S. Department of Justice (DOJ) first released its *Evaluation of Corporate Compliance Programs* (ECCP) guidance in 2017 to provide prosecutors with a roadmap on how to evaluate the effectiveness of corporate compliance, including specific criteria and government expectations. The document was later updated in 2019 under the DOJ Criminal Division to harmonize other DOJ guidance and standards, including the three fundamental questions prosecutors should ask in evaluating compliance programs:<sup>10</sup>

1. Is the program well-designed?
2. Is the program effectively implemented?
3. Does the compliance program actually work in practice?

Table 1: Tips to help evaluate your RA

Self-assessment	Tip
Policies and procedures Do your policies and procedures align with current regulations? Are you assessing the risk or gap between the regulations and your policies and procedures?	It is imperative to have coverage of a specific risk area that impacts your organization. Create a matrix of laws that apply to your organization and align the current policies and procedures to those regulations. Conduct a gap analysis to identify missing policies/procedures. Conduct a risk analysis to prioritize the largest regulatory risks and track corresponding policies and procedures.
Compliance oversight Are you engaging your board and key leaders in risk management? Do they participate in your annual compliance RA or similar efforts?	Engaging is key, but leadership participation is critical to increase understanding of risks, feedback, and visibility to the rest of the organization, demonstrating importance and value. This has a cascading effect on the rest of the organization in fostering a compliance culture.
Education and training Do you develop issue-specific or targeted training based on the results of your RA or enterprise risk management (ERM) findings?	Evaluate internal/external control weaknesses. Assessments are a great way to check if training is effective or identify whether it is needed. Review your current training plan (including compliance training) to ensure existing training addresses or should be updated to address the risks identified that could expose your organization to vulnerabilities.
Communication, reporting, and disclosures Do you provide progress reports on identified risks and activities taking place that address the issues?	Providing a progress report or brief update keeps leaders informed of current or emerging issues but also promotes a culture of transparency by ensuring visibility into ongoing work. These updates help maintain engagement with leadership, allowing for input and approval. Create a record of decisions made or discussed.
Standards enforcement Do you leverage your RA to enforce regulatory standards and best practices?	RAs and risk registries (or inventories) are powerful tools. Leverage the data and the risk scores for buy-in as a strategy to request additional resources or key operational changes, ensuring enforcement of regulatory standards.
Monitor and audit Do you proactively update your A&M plan based on the results of your RA and ERM risks identified?	The compliance RA is foundational for the annual A&M plan. Review the A&M plan regularly to reprioritize or make any adjustments throughout the year.
Detection, response, and corrective actions Do you review previous RA findings to ensure consistency, mitigations, and positive improvements over time?	Whether tracking for trends, mitigations, or performance improvement, it is vital to review previous findings and consistently follow up with efforts being taken towards the highest risks to the organization. This proactive technique ensures consistency, guides institutional investments, and enhances corrective action planning.

The June 2020 revisions were not extensive, but they emphasized mergers and acquisitions and due diligence during the integration. Most recently, the March 2023<sup>11</sup> and September 2024<sup>12</sup> updates refine the three fundamental questions to:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

3. Does the corporation's compliance program work in practice?

In addition, the *ECCP* incorporated and emphasized an increased responsibility of the compliance officer to participate



in policymaking and use metrics to measure the effectiveness of their programs, along with guidance on the ethical use of artificial intelligence (AI). In addition, the importance of access to data and tools to proactively, rather than reactively, detect and mitigate risks associated with new emerging technologies, such as AI, is also highlighted.

DOJ expectations are clear regarding risk management and provide prosecutors with tips to consider when assessing the effectiveness of the organization's RA process, giving credit to organizations that take a risk-based approach and periodically update, prioritize the risks identified, and value the overall organizational or enterprise risk management (ERM) framework for better risk accountability.

Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies?

Similarly, in 2024, DOJ also revised and released FCPA 9-47.120 - Criminal Division Corporate Enforcement Policy<sup>13</sup> to align with *ECCP* and other guidelines. DOJ not only encourages but also incentivizes organizations that voluntarily self-disclose or report misconduct and demonstrate having an effective compliance program that has been tailored to the annual RA.

#### 2024 HHS OIG CPG and RAs

The U.S. Department of Health and Human Services (HHS)

OIG developed the *General Compliance Program Guidance (GCPG)* for the healthcare sector since 1998 for use as an ongoing resource to help identify risk areas in particular industry segments such as hospitals, clinical laboratories, pharmaceutical manufacturers, etc.<sup>14</sup> The most recent 2023 GCPG for hospitals, followed by the 2024 GCPG for nursing facilities, make emphasis on the role of a formal and centralized compliance RA to improve healthcare outcomes and better detect fraud, waste and abuse practices, including the RA function as part of one of the compliance program elements – A&M. HHS also shared that they will be releasing newer CPGs and making them available on the HHS website and will no longer publish them on the *Federal Register*.<sup>15</sup>

#### Impact of Loper and current administration

Last year, the U.S. Supreme Court's decision during the 2024 *Loper Bright Enterprises v. Raimondo* case<sup>16</sup> overruled the Chevron deference,<sup>17</sup> which shifted power away from administrative agencies to federal courts to interpret the law in question. In other words, courts are no longer required to defer to agencies' interpretations of statutes or laws they administer when the law is too broad or seems ambiguous. Nonetheless, this may have a minimal impact in industries such as finance or healthcare, where laws are more prescriptive and defined, leaving less room for interpretation.

This unprecedented court decision is an alert

for organizations to take a more proactive approach and update their regulatory strategy. Recently, the Trump administration has taken various actions that have destabilized the structure of many government enforcement agencies, including the U.S. Department of Education and HHS. A likely forecast is that the actions of limiting or restricting federal activity may shift states into a leadership role. As such, regulatory fluctuations will be an increasing occurrence, making a proactive approach, such as conducting RAs, more imperative.

#### Industries with regulatory RA requirements

To emphasize the importance of assessments, numerous industries are subject to regulatory requirements mandating RAs, such as the following:

- ◆ Credit card industry - PCI-DSS,
- ◆ Agriculture, U.S. Environmental Protection Agency, and U.S. Department of Agriculture
- ◆ Accounting, PCAOB AS 2110
- ◆ Energy/utilities - NERC-CIP and Federal Energy Regulatory Commission (FERC)
- ◆ Info/cybersecurity - NIST 800-30 and new AI pubs NIST AI 600-1, AI 100-4, and AI RMF; ISO:23894 and 42001
- ◆ Higher Education - Title IX, Clery Act, and most Accrediting Agencies
- ◆ Banking/finance - Gramm-Leach-Bliley Act's Safeguards Rule 16 C.F.R. § 314.4b

Table 2. Polling Question #1: Are compliance RAs mandatory?

Poll option	Count	Results
Yes	88	68%
No	38	29%
I don't know	4	3%

Table 3. Polling Question #2: How often do you conduct your organizational compliance RA?

Poll option	Count	Results
Annually	103	68%
Biannually	8	5%
Other cadence	26	17%
We don't currently conduct one	15	10%

Table 4. Polling Question #3: Collaborative risk management: Do other business units include/share results with compliance?

Poll option	Count	Results
No	12	8%
Yes	60	42%
Occasionally	43	30%
Only when we ask for/aware of it	27	19%


**Bottom line: Assessments are necessary**

The RA function is imperative to ensure the effectiveness of a compliance program. In our most recent HCCA risk management

webinar — conducted in November 2024 — we asked over 200 participants three polling questions (see Tables 2-4). Here are some key insights from their responses.<sup>18</sup>

While a majority of the participants indicated RAs are mandatory, 3% either believed they were not required or were unsure. This variation could be reflective of differences in regulatory requirements across industries or indicate inconsistencies in organizational practices and potential gaps in awareness or understanding of compliance obligations.

The majority of participants in this polling question believe it is mandatory and conduct their RAs annually. However, it is alarming that one out of five participants in this poll have irregular assessment cadences, and about 10% of participants reported they do not currently conduct one. The results indicate that more than 10% of participants may have an ineffective compliance program in place and are missing the opportunity to implement key internal controls to better prevent, detect, and correct misconduct or violations.

Although most participants answered favorably about sharing information with the compliance unit, over 19% do not have a regular cadence or effective sharing of information. Assessments are a great way to break down silos and collaborate with other business units within the same organization. If you are conducting your compliance RA for the first time, do not get frustrated if you do not receive great participation or results. Consistency and education are key. Ask your compliance committee(s) and board members for feedback and connect with other peers in the network for insights. 





### Endnotes

1. D. Armentano, "The Great Electrical Equipment Conspiracy," March 1972, Reason, March 1972, <https://reason.com/1972/03/01/the-great-electrical-equipment>.
2. "Remarks Announcing the Establishment of the Blue Ribbon Commission on Defense Management," Ronald Reagan Presidential Library & Museum, June 17, 1985, <https://www.reaganlibrary.gov/archives/speech/remarks-announcing-establishment-blue-ribbon-commission-defense-management>.
3. "Executive Order 12526 – President's Blue Ribbon Commission on Defense Management," Ronald Reagan Presidential Library & Museum, July 15, 1985, <https://www.reaganlibrary.gov/archives/speech/executive-order-12526-presidents-blue-ribbon-commission-defense-management>.
4. Defense Industry Initiative, "The DII Principles," updated March 2010, [https://higherlogicdownload.s3.amazonaws.com/DII/b52278df-d15b-4fa7-a326-9894c0ff0ea7/UploadedFiles/FBYARzFSBCjIhRAjweeY\\_DII%20principles.pdf](https://higherlogicdownload.s3.amazonaws.com/DII/b52278df-d15b-4fa7-a326-9894c0ff0ea7/UploadedFiles/FBYARzFSBCjIhRAjweeY_DII%20principles.pdf).
5. U.S. Sentencing Commission, "1991 Federal Sentencing Guidelines Manual," November 1, 1991, <https://www.ussc.gov/guidelines/archive/1991-federal-sentencing-guidelines-manual>.
6. U.S. Sentencing Commission, "Chapter 8 – Sentencing of Organizations: § 8B2.1. Effective Compliance and Ethics Program," accessed May 8, 2025, [https://guidelines.ussc.gov/apex/r/ussc\\_apex/guidelinesapp/guidelines?app\\_gl\\_id=%C2%A78B2.1](https://guidelines.ussc.gov/apex/r/ussc_apex/guidelinesapp/guidelines?app_gl_id=%C2%A78B2.1).
7. Many of these assessment questions came from the HCCA–OIG Compliance Effectiveness Roundtable, *Measuring Compliance Program Effectiveness: A Resource Guide*, March 27, 2017, <https://assets.hcca-info.org/Portals/0/PDFs/Resources/ResourceOverview/oig-hcca-roundtable.pdf?ver=2017-03-28-062709-153> <https://assets.hcca-info.org/Portals/0/PDFs/Resources/ResourceOverview/oig-hcca-roundtable.pdf?ver=2017-03-28-062709-153>.
8. U.S. Sentencing Commission, "Commission Tightens Requirements for Corporate Compliance and Ethics Programs," news release, May 3, 2004, <https://www.ussc.gov/about/news/press-releases/may-3-2004>.
9. U.S. Sentencing Commission, "Chapter 8 – Sentencing of Organizations: § 8B2.1. Effective Compliance and Ethics Program."
10. U.S. Department of Justice, Criminal Division, "Criminal Division Announces Publication of Guidance on Evaluating Corporate Compliance Programs," news release, April 30, 2019, <https://www.justice.gov/archives/opa/pr/criminal-division-announces-publication-guidance-evaluating-corporate-compliance-programs>.
11. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, <https://www.justice.gov/archives/opa/speech/file/1571911/dl>.
12. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated September 2024, <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=>.
13. U.S. Department of Justice, Criminal Division, "FCPA Resource Guide," updated December 16, 2024, <https://www.justice.gov/criminal/criminal-fraud/fcpa-resource-guide>.
14. U.S. Department of Health and Human Services, Office of the Inspector General, General Compliance Guidance, November 2023, <https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf>. <https://oig.hhs.gov/compliance/compliance-guidance/>
15. Modernization of Compliance Program Guidance Documents, 88 Fed. Reg. 25,000 (April 25, 2023), <https://www.federalregister.gov/documents/2023/04/25/2023-08326/modernization-of-compliance-program-guidance-documents> <https://www.federalregister.gov/documents/2023/04/25/2023-08326/modernization-of-compliance-program-guidance-documents>.
16. Loper Bright Enterprises v. Raimondo, No. 22–451, 603 U.S. 369 (2024), [https://www.supremecourt.gov/opinions/23pdf/22-451\\_7m58.pdf](https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf).
17. Cornell Law School, Legal Information Institute, "Chevron deference," updated July 2024, [https://www.law.cornell.edu/wex/chevron\\_deference](https://www.law.cornell.edu/wex/chevron_deference).
18. Ximena Restrepo and Melinda Shapiro, "Mandatory or Not, Compliance Risk Assessments Are Necessary!" HCCA webinar, November 13, 2024, <https://learn.corporatecompliance.org/courses/74953>.

### Takeaways

- ◆ Often, an effective compliance program is recommended as a condition of probation.
- ◆ An organization that does not regularly conduct a compliance risk assessment (RA) is missing the opportunity to optimize and empower its decision-making, resource allocation, and overall risk management strategy.
- ◆ Compliance RAs are integral tools for checking your organization's risk temperature. A high temperature score may indicate a lack of internal controls.
- ◆ Take a proactive approach to risk mitigation rather than a reactive approach.
- ◆ Prevent internal control failures, unexpected fines, and reputational damage by conducting your compliance RAs on a regular basis.

# FALSE CLAIMS ACT: PREPARING FOR AND NAVIGATING INTERNAL COMPLAINTS

by John Eason

Complaint



**John Eason**

*([jeason@bassberry.com](mailto:jeason@bassberry.com)) is a Member of Bass Berry & Sims in Nashville, TN.*

An employee at a medical facility emails a supervisor with concerns that the facility is improperly billing the government for certain services. The supervisor, uncertain of what to do in response, assumes that the employee is mistaken about the situation or that the concerns have little merit. Ultimately, the supervisor decides to ignore the email, and unfortunately, such decisions can become extraordinarily costly for healthcare providers.

The False Claims Act (FCA) is a federal statute that allows individuals to file suit on behalf of the government against a person or entity that has allegedly submitted false claims to government programs, such as Medicare, Medicaid, and Tricare. These private persons—known as qui tam whistleblowers or relators—can obtain a percentage of any government recovery resulting from a lawsuit they file. Defendants in these lawsuits can

be liable for three times the damages incurred by the government and penalties ranging from about \$14,000 to \$28,000 for *each* false claim, in addition to costs for the whistleblower's attorneys.<sup>1</sup>

The healthcare industry remains the primary focus of the federal government's FCA enforcement efforts and qui tam lawsuits. On average, over the last five years, the U.S. Department of Justice (DOJ) has recovered nearly \$2.5 billion annually in FCA settlements and judgments from healthcare providers and entities.<sup>2</sup> The driving force behind those billions of dollars is qui tam lawsuits, which usually account for 80% of total recoveries. Looking ahead, there are no signs that FCA activity is slowing. Last year, whistleblowers filed 979 new qui tam lawsuits (the highest number ever recorded), and DOJ filed 423 new FCA actions on its own (the second highest number ever).<sup>3</sup>



In this environment, healthcare providers must consider *when* — not *if* — they will confront an internal complaint relating to the FCA. Inadequate responses or delays in addressing these complaints can cause significant issues. Such failures can create potential FCA liability — especially if a provider fails to investigate potential overpayments from Medicare. Under Medicare rules, a provider “has identified an overpayment” when it “knowingly receives or retains an overpayment,” at which point it “must report and return the overpayment” within a specified time period.<sup>4</sup> The term “knowingly” is significant regarding the FCA: “in cases where a provider or supplier acts in deliberate ignorance or reckless disregard of the existence of the overpayment,” it has just 60 days to report and return the overpayment (or risk FCA exposure), starting “on the date that the provider or supplier acted in deliberate ignorance or reckless disregard of the truth or falsity of information regarding the overpayment.”<sup>5</sup> By contrast, when a provider is conducting a “timely, good faith investigation,” the 60-day window to return overpayments may be suspended for up to 180 days after the date the initial overpayment was “identified.”<sup>6</sup>

A lack of internal investigation can frustrate employees and encourage them to report outside the organization (whether to the government or the media) or file a qui tam lawsuit — all of which can bring additional costs, reputational harm, and liability risk. Furthermore, should a related government investigation ensue, such inaction would come under additional scrutiny and could undercut a provider’s defenses. A provider that delays its response can also miss opportunities with the government

to voluntarily self-disclose improper conduct or receive cooperation credit for actions taken in advance of a government investigation.<sup>7</sup>

As such, providers should take steps now to prepare for an internal FCA-related complaint and understand how to navigate the response. Doing so enables an organization to act promptly and reasonably when — not if — that moment arrives.

### Proactive compliance: Planning ahead

Internal complaints alleging FCA violations can arise unexpectedly and carry significant legal, financial, and reputational risks. Proactive preparation is essential to ensure a prompt, effective, and compliant response.

The following are some key measures healthcare providers can take to prepare for such situations.

### Develop a culture of compliance that encourages internal reporting

No provider can address an employee’s FCA concern if they never raise it internally. Healthcare providers, therefore, must promote internal reporting — rather than external escalation — to identify and remedy problems early. Building this culture requires an organization to view compliance complaints as an opportunity — not something to suppress — thus, creating a feedback loop that encourages honest communications from employees. To help achieve this environment, a healthcare organization can take several measures, many of which have the added benefit of preparing the organization to effectively address internal FCA-related concerns:

- ◆ **Confidential reporting channels.** Create and publicize multiple avenues for employees to report concerns, including anonymous hotlines, online portals, and direct access to compliance personnel.
- ◆ **Timely follow-up.** Follow up and report back to anyone raising compliance concerns in a timely fashion.
- ◆ **Non-retaliation policy.** Implement and adhere to a policy of no retaliation for reporting suspected compliance concerns, and discipline anyone engaging in retaliatory conduct.

## Offer monetary and nonmonetary benefits to employees for reporting good faith compliance concerns and to management who demonstrate significant leadership in compliance efforts.

- ◆ **Evaluate employee compliance.** Include compliance and self-reporting as part of the employee evaluation process.
- ◆ **Incentivize compliance efforts.** Offer monetary and nonmonetary benefits to employees for reporting good faith compliance concerns and to management who demonstrate significant leadership in compliance efforts.
- ◆ **Benchmark compliance protocols.** Compare internal



compliance processes against industry standards to assess whether they effectively encourage internal reporting and mitigate risks.

- ◆ **Clear and consistent disciplinary standards.** Ensure disciplinary standards are well-defined and fairly enforced so that employees are confident the company will address concerns objectively and impartially.
- ◆ **Exit interviews.** Conduct exit interviews with departing employees, as they might reveal unknown concerns.

DOJ recently emphasized the importance of having a compliance program that incentivizes and protects whistleblowers through its policies, training, and actions—as the above measures do—when it revised (in September 2024) its *Evaluation of Corporate Compliance Programs* guidance,<sup>8</sup> detailing how prosecutors evaluate corporate compliance programs during government investigations.

#### **Routinely train management and employees about the FCA**

A healthcare organization should provide regular training to all staff—including leadership—on the requirements of the FCA, whistleblower protections, and

compliance policies. Compliance officers, HR personnel, and other employees should know how to identify red flags within a complaint that may implicate the FCA. In addition to references to “false claims,” “illegal billing,” or “fraud” involving federal healthcare programs like Medicare and Medicaid, such complaints would include ones that allege or suggest:

- ◆ **Billing for services not rendered.** Submitting claims for services, tests, or procedures that were not actually provided to the patient.
- ◆ **Upcoding, unbundling, or double billing.** Billing for a more expensive service than was provided, billing separately for services that should have been bundled, or billing twice for the same services.
- ◆ **Kickbacks.** Offering or receiving something of value to influence the referral of medical services violates the Anti-Kickback Statute.
- ◆ **Self-referrals.** Referring patients or clients to entities in which the referring provider has a financial interest is in violation of the Stark Law.
- ◆ **Falsification of records.** Altering or fabricating medical records or documentation to support the services billed.

- ◆ **Lack of medical necessity.** Billing for services that are not medically necessary.
- ◆ **Unqualified or unsupervised providers.** Submitting claims for services provided by individuals who were unlicensed, unqualified, or not properly supervised.
- ◆ **Cost report fraud.** Misrepresenting costs or expenses in reports submitted to federal healthcare programs.

#### **Establish investigation protocols and staffing**

Any healthcare organization should have written procedures that clearly outline how the organization will receive, investigate, and respond to internal complaints that may involve FCA violations. In providing training on these procedures, staff should be instructed on key elements related to their participation in any investigation, including providing access to relevant information, not destroying relevant records, participating in interviews, maintaining confidentiality, and prohibiting retaliation against individuals who raise concerns. A healthcare provider should have clear documentation preservation policies in place and know when and how to preserve relevant information in response to a complaint.

It is important to determine in advance who will be responsible for overseeing an investigation of an internal FCA-related complaint (e.g., board committee, in-house counsel, or compliance officer) and, generally, how to staff any investigation. By maintaining a well-defined and smaller control group for any inquiry and establishing clear channels of communication, a company can better preserve the confidentiality of its investigative efforts. Staffing considerations should also include

identifying internal resources that could be leveraged (and/or need improvements) for an internal investigation, including IT, internal audit, HR, and accounting. To avoid improper influences on the process, a healthcare organization should have a policy in place to address potential conflicts of interest (e.g., the individuals managing an investigation should not be implicated in the alleged misconduct at issue).

In general, appropriately staffing an investigation is critical to ensure the effort is completed in a timely and effective manner. If necessary, it can also serve as evidence to a government enforcement agency that the company took the matter seriously. To that point, when DOJ assesses a company's compliance program during an investigation, it considers "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts," and whether compliance program's internal audit functions are "conducted at a level sufficient to ensure their independence and accuracy."<sup>9</sup>

### Prepare for legal engagement

Healthcare providers should identify in advance legal counsel with expertise in handling internal investigations, government enforcement actions, and FCA matters, so that they can be engaged immediately upon receipt of an FCA-related complaint. Often, outside counsel can more readily identify any potential liability or legal theories at issue from an internal complaint to enable an organization to better navigate the investigative process. Outside counsel can also protect the confidentiality of materials created and communications made

during the investigation through the attorney-client privilege and work product doctrines. In addition, outside counsel can assist healthcare providers in thinking through the need for self-disclosure following an investigation and the various channels for doing so, as well as preparing a provider for a potential government investigation or litigation should that appear likely following an internal complaint.

### Effectively responding to internal complaints

The timeline and steps taken for an internal investigation into FCA allegations can vary widely based on the complexity of the issues, the scope of the alleged misconduct, and the organization's size. However, a typical investigation may unfold over several months, with the following general phases:

- ◆ **Initial response and assessment.** Acknowledge and triage the complaint, identify and secure relevant documents, assemble the investigation team, and determine if any immediate action is necessary (e.g., halting certain billing practices or suspending an employee). Evaluate whether there are immediate reporting obligations to government agencies, auditors, insurers, or other stakeholders.
- ◆ **Plan and scope the investigation.** Clarify the allegations at issue, develop an investigation plan, identify legal issues implicated, and collect key documents and data.
- ◆ **Conduct a formal investigation.** Conduct document review, witness interviews, and data analysis to determine the validity and scope of the allegations. If necessary, engage outside

consultants for complex billing or regulatory issues to conduct medical record reviews, billing data analysis, or similar assessments.

- ◆ **Legal analysis and findings.** Assess whether the facts support any finding of FCA violations or other legal noncompliance. Determine whether there are any overpayments to federal healthcare programs and, if so, estimate financial exposure.

## Outside counsel can also protect the confidentiality of materials created and communications made during the investigation through the attorney-client privilege and work product doctrines.

- ◆ **Internal reporting.** Prepare a report of the findings (e.g., written or oral presentation) that details the investigative process, any individuals responsible for misconduct related to an FCA violation, an estimation of any potential overpayments, and recommendations for corrective action.
- ◆ **Corrective action and remediation.** If violations are found, take corrective action, which may include self-disclosure to government agencies, repayment of overpayments, revisions



to internal policies, additional training, and disciplinary measures.

- ◆ **Ongoing monitoring.** Implement enhanced compliance measures as necessary and monitor for recurrence of similar issues.

### **Promptly define scope of the investigation**

Defining the scope of an internal investigation at the outset enables a healthcare provider to focus its investigative efforts to avoid unnecessary costs, disruptions, and delays chasing down tangential or irrelevant issues—while at the same time ensuring that the investigation identifies any broader, systemic issues and underlying root causes.

While the scope of any investigation is fact-dependent, at a minimum, setting the scope requires identification of the main allegations, relevant time period, the specific parties and potential witnesses involved, internal and external stakeholders, the legal issues and federal healthcare programs at play, and the potential sources of information regarding the allegations. Drafting an investigative plan can further clarify an investigation's scope and avoid mission creep. An effective plan outlines main objectives, relevant witnesses to interview, potential targets or bad actors, key sources of information, investigative methods, and anticipated timelines.

As an investigation progresses, its scope may need to be updated based on new information gathered from interviews and document review. For example, initial allegations may only reference one physician, time period, or type of procedure, and subsequent information gathered in the investigation reveals that

similar practices occur in a broader period, with several physicians, or with other similar procedures. By contrast, investigations into complaints that are quite broad can be narrowed to certain discrete areas if a preliminary assessment recommends it.

### **Communicating with complainants during investigation**

Any internal complaint should be promptly acknowledged, and the complainant should be assured that the matter will be taken seriously. A healthcare provider should never assume that an internal complaint is baseless, but instead, enter with an open mind as to what may have happened, and who might be credible. For lengthy investigations, companies should consider providing updates to the reporting employee so that they do not feel ignored. Such transparency and feedback to a reporting employee can demonstrate a provider's good faith efforts to resolve any compliance concerns.

At the same time, it is necessary to consider what aspects of the investigation must remain confidential and whether the employee's background suggests that the individual is building a qui tam and/or retaliation lawsuit. Companies need to be aware of the possibility that otherwise privileged communications with a potential whistleblower may not remain protected if that employee later brings a whistleblower retaliation claim. It is critical that legal counsel, compliance, and HR work together throughout this process and are aligned to ensure there are no delays or mixed messages in these communications and mitigate any potential concerns of privilege waiver.

### **Resolving the investigation and next steps**

When an internal investigation uncovers potential FCA violations, taking prompt and effective corrective action is not only prudent but essential. Corrective action could include implementing procedures to cease and correct illegal conduct, taking appropriate disciplinary actions against individuals responsible for the conduct, and revising compliance protocols and training.

Specific to the FCA, other remedial measures a provider should consider are whether to disclose any identified misconduct to the government and make repayments to government healthcare programs. Healthcare providers are advised to work with experienced counsel to carefully assess these options and obligations and how they apply to any specific set of facts. For example, Medicare overpayment regulations require a provider to return an overpayment within 60 days of identifying it, and failure to return an identified overpayment may subject a provider to FCA liability. But, this 60-day deadline is suspended for 180 days if the provider is conducting a timely, good-faith investigation to determine if related overpayments exist.<sup>10</sup> Regarding self-disclosure, a provider may consider repaying any affected funds to the relevant government agency, which is a straightforward and more subtle approach but does not protect a provider from FCA liability or administrative liability under the Civil Monetary Penalties Law. Other routes include voluntarily disclosing conduct directly to DOJ or through specific self-disclosure protocols with the U.S. Department of Health and Human Services Office of

Inspector General and the Centers for Medicare & Medicaid Services.<sup>11</sup>

Prior to closing any investigation, a provider should make certain it has maintained proper documentation of its response to any complaint and investigative process. Having a defensible audit trail of your organization's efforts will be crucial should the organization subsequently face a whistleblower lawsuit or government investigation. For example, did you provide additional training in response to the complaint? Did you terminate responsible employees? Conduct an audit of alleged billing issues and make a difficult decision on its scope? Maintain any documentation regarding such efforts, as they will be helpful should the provider need to defend its response to the government in the future.

Following any investigation, a provider should monitor its employees to confirm no retaliation has occurred against the complainant. Consider whether to conduct intermittent check-ins with the complainant and the complainant's supervisors after

resolving the complaint to ensure no retaliatory efforts are detected. A provider should also assess what lessons were learned after the investigation (e.g., internal process improvements, resource additions, revised training, system changes). DOJ has recently highlighted the need for compliance programs and training to adapt based on lessons

learned from both the company's own prior issues and those at other companies in similar industries and geographies.<sup>12</sup> Incorporating lessons learned from an internal investigation should also build trust among employees about the effectiveness of a company's compliance program and its reporting protocols. **CT**

#### Endnotes

1. 31 U.S.C. § 3729(a)(1); Civil Monetary Penalties Inflation Adjustments of 2024, 89 Fed. Reg. 9,764 (Feb. 12, 2024), <https://www.govinfo.gov/content/pkg/FR-2024-02-12/pdf/2024-02829.pdf>.
2. U.S. Department of Justice, Civil Division, "Fraud Statistics – Overview: October 1, 1986 – September 30, 2024," accessed May 13, 2025, <https://www.justice.gov/archives/opa/media/1384546/dl>.
3. U.S. Department of Justice, Office of Public Affairs, "False Claims Act Settlements and Judgments Exceed \$2.9B in Fiscal Year 2024," news release, updated February 6, 2025, <https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024>.
4. 42 C.F.R. § 401.305(a)(2).
5. Medicare and Medicaid Programs; CY 2025 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment and Coverage Policies; Medicare Shared Savings Program Requirements; Medicare Prescription Drug Inflation Rebate Program; and Medicare Overpayments, 89 Fed. Reg. 97,710, 98,336 (Dec. 9, 2024), <https://www.govinfo.gov/content/pkg/FR-2024-12-09/pdf/2024-25382.pdf>.
6. 42 C.F.R. § 401.305(b)(3); *see also* Medicare and Medicaid Programs; CY 2025 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment and Coverage Policies; Medicare Shared Savings Program Requirements; Medicare Prescription Drug Inflation Rebate Program; and Medicare Overpayments, 89 Fed. Reg. 97,710, 98,336-98,337 (Dec. 9, 2024), <https://www.govinfo.gov/content/pkg/FR-2024-12-09/pdf/2024-25382.pdf>.
7. U.S. Department of Justice, "4-4.000 – Commercial Litigation: 4-4.112 – Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters," *Justice Manual*, May 2019, <https://www.justice.gov/jm/jm-4-4000-commercial-litigation#4-4.112>.
8. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated September 2024, <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=>.
9. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*.
10. 42 C.F.R. § 401.305(b)(3)(ii).
11. U.S. Department of Health and Human Services, Office of Inspector General, "OIG's Health Care Fraud Self-Disclosure Protocol," amended November 8, 2021, <https://oig.hhs.gov/documents/self-disclosure-info/1006/Self-Disclosure-Protocol-2021.pdf>; Centers for Medicare & Medicaid Services, "Self-Referral Disclosure Protocol," last modified September 10, 2024, <https://www.cms.gov/medicare/regulations-guidance/physician-self-referral/self-referral-disclosure-protocol>.
12. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*.

## Takeaways

- ◆ The U.S. Department of Justice enforcement actions and qui tam whistleblower lawsuits under the False Claims Act (FCA) are at an all-time high, remain largely targeted at the healthcare industry, and can leave defendants with significant costs.
- ◆ For most healthcare providers, it is a matter of when — not if — an FCA-related complaint will arise. Take proactive steps now to establish investigation protocols to ensure a quick and thorough response when such a complaint does arrive.
- ◆ Dismissing internal compliance complaints or creating a culture where internal complaints are discouraged can lead to increased liability, scrutiny from government agencies, and reputational harm — particularly as it relates to the FCA. Every internal allegation of FCA violations should be treated with the utmost seriousness and initially viewed with an open mind.
- ◆ Healthcare providers must act quickly to assess and scope any internal allegations implicating the FCA and determine how to staff an investigation, including the involvement of outside counsel.
- ◆ Use any investigation as an opportunity to strengthen compliance practices, educate staff, and reduce future risk.

# Gain specialized compliance knowledge to fit your needs



## One-day virtual learning events

offer comprehensive updates and information on a wide variety of compliance topics without the time and cost commitment of travel.

**Check out these upcoming opportunities and register today!**

## Compliance in Smaller Organizations

Explore topics such as working with leadership, doing more with less, and leveraging resources from other departments.

**July 31, 2025**

## Compliance, Ethics, and Organizational Culture

Learn how to build and maintain a culture of ethics and compliance within your organization.

**August 5, 2025**

**Compliance Auditing & Monitoring Conference**  
September 25, 2025

**Behavioral Health Compliance Conference**  
October 21, 2025

**Physician Practice Compliance Conference**  
October 28, 2025

**Healthcare Privacy Compliance Conference**  
November 5, 2025

**Intersection of Compliance & Quality**  
November 18, 2025

**AI & Compliance**  
November 20, 2025

**Compliance & Post-Acute Care**  
December 2, 2025

**Learn more**  
[hcca-info.org/virtual](https://hcca-info.org/virtual)





# I-9 compliance is a federal audit focus and should be monitored

by Betsy Wade

**B**usinesses and healthcare organizations nationwide have reported in recent months receiving subpoenas from the U.S. Department of Homeland Security (DHS) requesting copies of all I-9s for current and former employees within the last 12 months.

The reason: U.S. Department of Justice Attorney General Pamela Bondi announced in February an increased focus on immigration enforcement and the agency's intent to pursue criminal prosecution of immigration-related violations, including prosecution for unlawful employment of unauthorized workers, harboring undocumented individuals, and immigration document fraud.

Employers are required to verify the identity and employment eligibility of all individuals hired in the United States.<sup>1</sup> U.S. Citizenship and Immigration Services (USCIS) requires employers to use the Employment Eligibility Verification Form I-9.<sup>2</sup>

## I-9 verification

*I-9 verification is imperative because it:*

- ◆ Verifies employment eligibility by ensuring employees are either U.S. citizens, U.S. nationals, or authorized noncitizens with the proper work documentation.
- ◆ Prevents illegal employment by confirming a worker's legal status. I-9 verification helps prevent hiring unauthorized immigrants who are not eligible to work.
- ◆ Maintains legal compliance. Employers are legally required to complete and retain I-9 forms for all employees **within three days of hiring**.

## Completing the I-9

*Employers should:*

- ◆ Have all new hires complete Section 1 of the I-9 form within the first three business days of employment.
- ◆ Accept original, unexpired documents from List A (identity and employment authorization) or a combination of List A and List B (identity) and List C (employment authorization) documents. Federal regulations do not require employers to keep copies of the documents.
- ◆ Carefully review all documents presented by employees, ensuring they are genuine and meet the requirements outlined by DHS.
- ◆ Reverify employees whose employment authorization expires within the required time frame, following the guidelines provided by USCIS.

## Penalties for noncompliance

*On January 2, 2025, DHS announced new civil penalties for I-9 violations, with increased fines on employers for failure to comply:*

- ◆ I-9 paperwork violations increased from \$288 to \$2,861 per Form I-9 violation;
- ◆ Knowingly employing unauthorized employees (first offense) increased from \$716 to \$5,724 per violation;
- ◆ Knowingly employing unauthorized employees (second offense) increased from \$5,724 to \$14,308 per violation; and
- ◆ Knowingly employing unauthorized employees (third or more offenses) increases from \$8,586 to \$28,619 per violation.

## What can compliance do?

- ◆ Add I-9 compliance monitoring to their annual work plans.
- ◆ Conduct education within their organizations about the importance of completing and retaining the I-9. CT



**Betsy Wade**

MPH, CHC, CHPC, CNA

*([bwade@signaturehealthcarellc.com](mailto:bwade@signaturehealthcarellc.com), [bit.ly/Linkedin-BetsyWade](https://bit.ly/Linkedin-BetsyWade)) is the Chief Compliance and Ethics Officer at Signature HealthCARE in Louisville, KY.*

### Endnotes

1. 8 U.S.C. § 1324a.
2. 8 C.F.R. § 274a.2.

# YOUR ROLE AS AN ACO COMPLIANCE OFFICER: ESSENTIAL KNOWLEDGE AND STRATEGIES

by Divya M. Schavio  
and Joseph Grant



**Divya M. Schavio**

MHA, CHC

[divya.schavio@religroupinc.com](mailto:divya.schavio@religroupinc.com)

is a Model Lead at RELI Group  
in Windsor Mill, MD.



**Joseph Grant**

MBA, LSSYB

[joseph.grant@religroupinc.com](mailto:joseph.grant@religroupinc.com) is a  
Compliance Specialist III at RELI Group  
in Windsor Mill, MD.

Value-based care (VBC) is reshaping the healthcare landscape, offering a patient-centered approach that prioritizes quality and outcomes over volume. As private payers follow the lead of Centers for Medicare & Medicaid (CMS) Innovation and federal programs, CMS continues to drive this industry-wide transformation. And, with the continued expansion of Alternative Payment Models (APMs) by payers like Humana, Aetna, and Blue Cross Blue Shield, the demand for Accountable Care Organization (ACO) compliance officers is on the rise. As such, the need for dedicated compliance professionals to manage ACOs and APMs will continue to grow. Compliance professionals are essential to ensure that providers adhere to federal and private payer regulations, accurately report quality metrics, prevent fraud, and navigate evolving policies set by CMS and private payers. As more payers and providers engage in VBC, the demand for experts to manage compliance risks and optimize program participation will continue to rise.

Given the increasing specialization of this role, it is crucial to understand what distinguishes an ACO compliance officer from

other compliance roles. This article highlights the top five areas of expertise necessary for success in this evolving field.

*Authors' note: While "APM" is often used interchangeably with "ACO" in the industry, this article uses "ACO compliance officer" for familiarity and "APM" to reference VBC arrangements, including ACOs.*

## Read and know the APM agreement

Understanding the APM participation, which is a binding contract between the payer offering the APM and the ACO, provider, or entity delivering on the APM, is crucial for compliance and effective participation.

Understanding key provisions in the participation agreement ensures that ACO and APM participants operate effectively within the program's framework. To best understand the participation agreement, take the time to attend webinars and read educational information, such as listservs and newsletters—put out by the payer—as they provide valuable summaries of key information. If attending an event in real time is not possible, accessing the slides afterward can still be beneficial. Staying informed also ensures that provider organizations

Table 1

Common areas in participation agreements	What’s typically included
Provider/entity obligations	Provider/entity obligations ensure care is delivered according to the quality and cost-reduction standards outlined in the participation agreement. To receive financial benefits, such as shared savings, ACOs may be responsible for reporting patient data, tracking performance metrics, and adhering to care coordination and population health initiatives. Compensation and incentives are also detailed, including capitation payments (if applicable), bonus structures for quality and cost efficiency, and preventive care and care coordination incentives. Financial aspects of the participation agreement, such as benchmarking and reconciliation criteria that inform shared savings and losses, dictate how performance-based distributions are made among APM participants.
Data-sharing obligations	Data-sharing obligations serve as a critical part of participation agreements, ensuring collaboration among APM participants to improve care quality. Compliance with HIPAA and the Health Information Technology for Economic and Clinical Health Act is essential for the secure exchange of patient information. Participation agreements also outline permitted uses of Medicare claims data for analytics and risk adjustment, helping providers manage populations more effectively. Additionally, the participation agreement clearly defines termination and exit provisions, ensuring all participants understand their obligations and potential consequences.
Patient attribution and beneficiary engagement guidelines	Patient attribution and beneficiary engagement guidelines dictate how patients are attributed to the APM. The participation agreements will also typically establish rules for patient outreach, education, and patient alignment to the APM while ensuring compliance with payer marketing and engagement regulations — especially for government payers — where the marketing and engagement standards may be more stringent.

are well-prepared for reporting and auditing requirements.

Table 1 shows common areas of these types of participation agreements with which ACO compliance officers should inform themselves.

Ultimately, participation agreements are the primary tool that the payer offering the APM will use to audit, monitor, and ensure compliance on behalf of the provider organization participating in the APM. Common audits and reviews focus on areas such as financial arrangements between participating providers in the continuum of care, the governance board of the APM, patient alignment, quality measures,

provider network incentives, provider website monitoring, and more. When auditing time arrives, you must provide evidence for key provisions and activities. One way to be prepared is to have canned reports of up-to-date member and provider lists, as these may be commonly requested during auditing and monitoring activities; this proactive approach helps maintain accuracy and readiness for audits. Some payers may also develop audit and monitoring templates for you to populate with the requested information as well as track necessary documentation and procedures. Staying on top of these aspects ensures smooth operations

and compliance with program expectations.

**Understand your APM’s governing body**

A thorough understanding of your APM’s governing body and/or board of directors is vital for ensuring compliance oversight, reporting, and effective decision-making. This includes familiarity with their meeting processes, membership, roles, and responsibilities. The participation agreement typically outlines requirements for the APM’s or ACO’s governing body, which is often separate and distinct from the provider organization’s governing body and typically operates under



specific compliance requirements, including voting rights for appointed officials.

Much like standard governing bodies, the governing body of an APM must usually maintain full control over its structure, with control percentages equaling 100%. Additionally, it holds sole and exclusive authority to appoint or remove executives, officers, managers, general partners, and other similar leadership roles. A conflict-of-interest policy should also apply to all governing body members, addressing relevant financial interests or any known or potential conflicts of interest that could impact decision-making.

Providing evidence of governance structure and compliance is also typically a key requirement. This includes documentation outlining how the APM is structured, board representation, voting rights, and participant roles, such as beneficiary representatives, health equity perspectives, and/or consumer advocacy roles. Additionally, clear dispute resolution mechanisms should be established to effectively manage conflicts among participants.

Oversight responsibilities for ACO compliance officers and legal teams must also be well-defined. These roles ensure that governance adheres to regulatory standards and that all participants operate within the framework set by the governing body.

### **Serving as the liaison among internal and external stakeholders**

Understanding and adhering to the various notification requirements across multiple parties is complex but important for ACO compliance officers. Key stakeholders in the arrangements, such as beneficiaries,

other providers, and the general public, must be informed in a timely and appropriate manner; this includes using the website and press releases, especially for APMs through CMS. This is particularly applicable to providers who receive benefit enhancements, waivers, administrative simplification, and other incentives that enable nontraditional approaches or coverage for care because of their participation in the APM; the notification requirements for these benefits and incentives to be communicated to patients can be complex and time-sensitive.

Again, attending webinars and reviewing materials developed by the payer can help clarify these requirements. These materials provide valuable summaries of key information, and if attending in real-time is not possible, reviewing the slides afterward ensures that critical details are not missed.

When notifying beneficiaries, APMs may require the use of regular postal mail, email, or outbound patient portal communications—or a combination of these methods. If a notification is posted on a patient portal, outbound communication must typically accompany it to meet compliance requirements. Beneficiary notification forms must be free from influence or coercion and comply with documentation maintenance standards while upholding beneficiary protections and established processes.

Certain marketing or descriptive materials that an APM plans to distribute to beneficiaries or providers may need to be reviewed and approved by the payer before dissemination—especially if that payer is CMS. Maintaining an active, publicly accessible website or webpage is usually another crucial requirement, as it serves

as a transparent resource for beneficiaries and other stakeholders.

### **Work with other departments to enable payment obligations**

Because cost savings and payments are one central component of participating in APMs, collaborating with your finance, billing, and/or quality departments is essential to ensure all stakeholders fully understand what is needed in their respective roles.

Your finance department may need clarification on how certain financial and operational aspects are managed. This may include requirements regarding how providers will be compensated in the APM, detailing capitation, reduced, or supplemental payments if applicable. Additionally, financial provisions, such as shared savings and losses or payments for meeting quality and cost-efficiency targets, determine how performance-based payments are allocated among APM participants and can help your finance department with financial forecasting and budgeting.

Billing guidance is another fundamental area where support may be necessary. Some APMs require that providers meet certain benchmarks to maximize reimbursements; these determinations are often claims- or coding-based. Payments may also be adjusted based on patient risk scores using Hierarchical Condition Category coding, which accounts for the complexity of patient populations.

You may also be involved in quality-related discussions. As many APM payments are tied to quality metrics, serving as the liaison that helps clinical teams understand performance and reporting expectations allows them to focus on providing quality care that can

also enable maximum payments and reimbursements. Audits of APMs' quality performance typically involve validation of data accuracy against medical records, risk scores, or claims data, and beneficiary sample review to confirm that reported services were properly documented and delivered. When electronic clinical quality measures are submitted, payers may also validate that the most recent specification versions and certified health IT were used. Since this information is directly tied to financial performance in the APM, understanding and communicating requirements to these teams in these key areas is essential.

While payment obligations may not be an ACO compliance officer's primary responsibility, it is beneficial to read the participation agreement for these finance, coding, billing, and quality-related details. Having a basic understanding of these obligations will allow you to provide better support, communicate effectively with stakeholders, and ensure compliance with payers' requirements to achieve the benefits of participating in the APM.


### Ask the payers

#### questions — support is available

Don't hesitate to ask questions of the APM payer you are working with. Most payers with APMs have dedicated support staff versed in the requirements and are there to help; payers prefer that you maintain up-to-date information and respond to audit requests correctly the first time rather than struggle with uncertainties. As the ACO compliance officer, should you need clarification on compliance, financial obligations, or reporting requirements, reaching out early to the payer team can prevent mistakes and streamline processes.

You can submit questions through the payer's help desk or a designed platform specifically for its APM participants. When doing so, it may be helpful to include your APM identifiers to ensure your request is properly tracked and directed to the right team and check that the primary contact information for your organization is up to date so messages don't get missed. Being specific in your request will help the support staff provide clear and accurate

answers, reducing back-and-forth communication. Proactively seeking guidance ensures compliance and helps keep your APM operations running smoothly.

As the healthcare landscape continues to evolve, the role of the ACO compliance officer is becoming more critical than ever. These professionals are at the forefront of ensuring that VBC arrangements operate smoothly, ethically, and in alignment with payer expectations. From mastering APM participation agreements and understanding governance structures to navigating complex notification requirements and collaborating across departments, ACO compliance officers must be both strategic thinkers and detail-oriented practitioners. By cultivating deep expertise in these areas, ACO compliance officers not only safeguard their organizations but also contribute meaningfully to the broader goals of improved healthcare quality, population health, and cost efficiency. The future of VBC depends on capable leaders who are ready to meet these challenges head-on. 

### Takeaways

- ◆ **Master the Alternative Payment Models (APM) agreement:** Ensure full compliance with payer requirements by understanding financial models, maintaining audit readiness, and establishing clear documentation and reporting practices.
- ◆ **Understand governance structures:** Know your APM's governance framework, including oversight responsibilities, voting rights, conflict-of-interest policies, and board accountability.
- ◆ **Navigate notification requirements:** Effectively manage complex notification rules to ensure timely and compliant communications with beneficiaries, providers, and the public through approved channels.
- ◆ **Foster cross-departmental collaboration:** Work in conjunction with finance, billing, and quality teams to align payment structures, coding practices, reporting standards, and reimbursement goals.
- ◆ **Leverage payer support:** Engage payers early by asking precise questions through official channels to prevent compliance missteps and streamline operations.

# Stay in the know with peer-driven compliance insights



Did you know you can learn from your peers on SCCE & HCCA's regularly published podcast? Check out this episode and learn more about value-based care – an alternative model to fee-for-services healthcare that emphasizes collaboration and transparency across all channels.



Read educational insights and compliance news from industry professionals and leaders in the Compliance & Ethics Blog. Explore regulatory updates, compliance best practices, and strategies for mitigating risk.

Write for our blog and share your knowledge with your peers! Submit an article today at [complianceandethics.org/contact-us](https://complianceandethics.org/contact-us)

**Join our online community:**



**Stay connected**  
[complianceandethics.org](https://complianceandethics.org)



**SCCE**  
Society of Corporate  
Compliance and Ethics



**HCCA**  
Health Care Compliance  
Association



# Invigorated and re-energized through the compliance community

by J. Veronica Xu

**W**hat is a community? Merriam-Webster defines it as “people with a common characteristic or interest living together within a larger society,” among other things. To me, a community is not merely a geographic location where random people stay in proximity to each other. Rather, it is a place where people help and support each other regardless of age, gender, religious belief, or political affiliation. It is a welcoming environment where everyone is engaged and has a sense of belonging. The compliance community and compliance professionals thrive and prosper when we care about and contribute to the success and future of our profession.


## Engage in the compliance community

Recently, I had the opportunity to attend the SCCE's 13th Annual European Compliance & Ethics Institute in Portugal, where compliance professionals from a wide variety of private sectors attended, including manufacturing, banking, healthcare, and technology. It was a unique and positive experience because it was inspiring to hear what risks and challenges others face and how they tackle problems and overcome barriers, regardless of industry, region, or culture. Moreover, it is refreshing to gain an understanding of timely and

relevant topics, participate in those insightful and thought-provoking discussions, and exchange ideas with fellow compliance colleagues. The knowledge, ideas, support, and validation received from each other have not only increased our professional knowledge but have also invigorated and energized all of us. The warmth everyone brought, the shared passion for compliance, rapport built, and comradery felt at the conference made it such a heart-warming and memorable event.

## Expand your horizons

As we always say, compliance work never stays static; the same applies to our learning and professional growth. It is important for us to step out of our comfort zones and not limit ourselves to the sole industry that we work in. Proactively seeking opportunities to learn beyond our daily interactions and department functions, such as attending regional, national, and international conferences, will definitely expand our horizons and, in turn, enhance our job performance. Being the compliance person in a company can be lonely and challenging in and of itself. One healthy way to counter it and stay relevant is to connect with fellow compliance professionals across all industries. The new ideas and fresh perspectives brought by them are helpful and invaluable.

With that being said, I hope to connect with you soon. 



**J. Veronica Xu**

Esq., CHC, CHPC, CCEP

*([veronica.xu@saberhealth.com](mailto:veronica.xu@saberhealth.com)) is the Chief Compliance Officer at Saber Healthcare Group headquartered in Cleveland, OH.*

# MAINTAINING COMPLIANCE IN THE FACE OF DISASTER

by Jerry Kaner



**Jerry Kaner**

*(jkaner@ciphertex.com) is the Founder and CEO of Ciphertex Data Security in Chatsworth, CA.*

**W**hile some threats can be prevented, natural disasters are not among them. These crises put patients — and their data — at risk. Beyond structural damage and dangerous conditions, they expose IT vulnerabilities and create lucrative opportunities for threat actors to kick a facility when it's down. Unfortunately, natural disasters are not a valid excuse for HIPAA violations. Noncompliance still risks costly fines, operational disruptions, and reputational turmoil.

According to the World Meteorological Organization, the number of these events has increased fivefold in the last 50 years.<sup>1</sup> That said, it is only a matter of time before disaster strikes your organization. Are you prepared enough to remain compliant and protect your patients' privacy when it does?

## **The shift to EMRs: Progress and persistent vulnerabilities**

The rapid digital transformation of the healthcare industry has fundamentally changed how organizations prepare for and are affected by natural disasters. In the past, a lack of centralized, portable, and easily recoverable patient data significantly hindered both immediate disaster response and long-term recovery. In 2005, for example, many healthcare facilities had yet to implement electronic medical records (EMRs), relying entirely on paper-based systems. When Hurricane Katrina struck, this dependence on physical records led to catastrophic losses.

Floodwaters and structural damage rendered thousands of patients' charts unreadable at best, wiping out vital details about treatment histories, medication regimens, and allergies. This strained hospitals receiving displaced patients, as they were forced

to conduct redundant tests or make clinical decisions with limited access to important information. In contrast, early EMR adopters were able to weather the storm more easily. The Veterans Administration already had a robust system in place when Katrina hit, and its providers were able to access the records of displaced patients from outside the disaster zone.<sup>2</sup>

The value of EMRs was demonstrated again in 2011 when an EF5 tornado devastated the community of Joplin, MO., and left St. John's Regional Medical Center severely damaged. A mere three weeks prior, the facility had completed its transition to electronic recordkeeping. Although some paper records and X-rays were lost, the switch meant that most patient information remained intact and accessible. Less than a week after the tornado, the hospital's staff was operating again in a temporary medical unit with full access to digital records.<sup>3</sup>

Broad adoption of EMR systems and cloud technology has helped mitigate some of the challenges posed by natural disasters, allowing healthcare providers to access patient information from off-site locations even when local systems are compromised. However, the effectiveness of these tools depends on factors like connectivity, power, and the stability of third-party providers. When supporting infrastructure fails, digital records are far less useful.

### **Infrastructure failures reveal gaps**

During Hurricane Sandy in 2012, hospitals in New York and New Jersey faced severe flooding that knocked out power and local servers, leaving some facilities unable to access EMRs.<sup>4</sup> In 2017, Hurricane Maria further demonstrated the

fragility of healthcare IT systems in prolonged disaster scenarios. The storm left much of Puerto Rico without power for months, rendering digital records inaccessible at many healthcare facilities.<sup>5</sup> More recently, the Los Angeles wildfires caused widespread power outages and infrastructure damage, leading clinics to close and prompting the evacuation of patients at long-term care facilities.<sup>6</sup> Clearly, while EMRs have improved healthcare resilience, they are *not* a fail-safe solution in disaster scenarios. Cloud storage alone is insufficient if network connectivity is disrupted, and even the most advanced digital infrastructure can be debilitated by power failures, damaged servers, or cyberthreats. Furthermore, without seamless data exchange, providers may still face delays or discrepancies in patient records, complicating disaster response and potentially putting patients at risk.

### **Steps for maintaining security and compliance during a disaster**

#### **Planning ahead (again and again)**

Although healthcare systems cannot prevent natural disasters, they can prepare for them. Not doing so puts organizations at risk of noncompliance. Under HIPAA, covered entities must maintain retrievable copies of electronic protected health information (ePHI) and have a tested disaster recovery protocol in place.

The first step is to ensure you have a comprehensive plan outlining specific procedures for protecting data in an emergency, including considerations for alternative work arrangements in case a facility is rendered inaccessible. Ensure that the necessary steps for securing sensitive information and maintaining compliance both on-site and remotely are clear and easily

accessible to those who may need to execute them.

Team members must understand their roles, as even the most well-designed plan will be ineffective if staff members are unclear on what actions to take. Conducting training sessions, tabletop simulations, and live drills can help clarify individual responsibilities and reveal organizational weaknesses. Likewise, proactively testing backup and recovery processes under controlled conditions ensures that key system functionalities are working properly before they are needed.

Beyond general preparedness exercises, regular compliance audits and after-action reviews should be conducted to evaluate how well teams follow protocols during simulations. These audits should also assess data integrity, ensuring patient records remain complete, accurate, and retrievable across all backup systems. Even minor data corruption or system failures can compromise compliance, leading to missing or altered records that hinder patient care and trigger regulatory scrutiny.

Coordinating with third-party vendors is also critical, and not just because of the impact a local natural disaster can have on a healthcare organization. Vendors themselves are not immune to these events and if one providing cloud storage, data processing, or other essential services is impacted, access to patient information could still be compromised. Compliance officers should review business associate agreements to confirm that vendors have adequate security and redundancy measures in place.

It is vital to understand that preparation — and all it involves — is not a one-and-done activity. Too often, organizations rely on



outdated strategies that fail to address evolving risks. Annual risk assessments, ongoing staff education, and regular audits of third-party vendors must be part of a hospital's long-term compliance strategy. A reactive approach to disaster preparedness leaves patient data vulnerable. A proactive, continuously refined strategy ensures facilities maintain compliance, protect patient privacy, and sustain operations even in challenging circumstances.

### **Diversifying data storage**

As demonstrated by the examples mentioned earlier, no single storage solution can guarantee uninterrupted access to patient data during a disaster. The need for data redundancy and secure backup systems cannot be overstated. Cloud solutions have been widely adopted by the industry due to their cost-savings, scalability, and geographic redundancy. Unfortunately, power, internet, and service provider outages can interfere with access.

Only storing data on-site creates its own risks, as servers cannot easily be moved but can be destroyed by a fire or flood. Although hard drives could be removed and taken elsewhere without robust encryption mechanisms, there is a risk that they could fall into the wrong hands and expose vast amounts of patient data.

In any case, when providers lose access to ePHI, they face regulatory scrutiny, fines, and legal action. For example, a healthcare provider that cannot retrieve patient records due to power outages or network disruptions may be found to be noncompliant. A hybrid approach that leverages both on-premises and cloud storage

reduces compliance risks by ensuring multiple access points to patient data—even when primary systems fail.

Incorporating portable solutions, such as secure network-attached storage, into backup strategies can bolster resilience. They allow hospitals and clinics to maintain critical data backups that can be accessed quickly in the event of network failures. The devices also offer the ability to quickly move data to a safer location without compromising integrity; this feature is especially valuable for those operating in disaster-prone regions where evacuations are a factor.

### **Leveraging encryption**

Regardless of whether data is stored on-site, in the cloud, or on a portable server, encryption (both at rest and in transit) is imperative for safeguarding patient records. Without it, backup files, removable drives, and even transmitted data could be intercepted or compromised, increasing the risk of HIPAA violations.

Not all encryption is created equal. Hardware encryption is built directly into physical storage devices, such as encrypted external drives or self-encrypting solid state drives, offering faster performance and better resistance to brute-force attacks. These operate independently of the host system, reducing exposure to malware and keylogging attacks. Additionally, some storage solutions offer an extra level of physical security with custom-designed hardware encryption keys.

On the other hand, software encryption relies on applications to encrypt data, providing more flexibility but potentially being more vulnerable to cyberthreats if the

encryption keys are not properly secured. A strong data protection strategy should leverage both.

### **Recognizing that an organization's crisis is a cybercriminal's dream**

Although natural disasters pose immediate risks to patient safety and operations, for threat actors, they present a lucrative opportunity. IT security often becomes a secondary concern when an organization scrambles to restore services and maintain continuity of care. Cybercriminals recognize this and launch attacks, knowing that overstretched teams are likelier to overlook security warnings or make mistakes under pressure.

One of the most significant threats post-disaster is ransomware. With systems down and urgent medical needs at stake, some organizations have been forced to pay a hefty price just to regain control of their records; however, data may still be leaked. Phishing is a leading vector for these attacks, with criminals posing as IT team members or executive leadership to trick employees into providing their login credentials. In such high-stress environments, even seasoned professionals can fall victim to increasingly sophisticated scams.

Another major concern comes in the form of malicious insiders. During disasters, organizations frequently bring in temporary personnel or relocate patients, creating a need for flexible yet secure data access. Without strict controls in place, this can lead to breaches as unauthorized individuals gain entry to sensitive systems.

### **Building cyber resilience**

Continuously monitoring cybersecurity risks and

revisiting protocols helps reveal vulnerabilities such as outdated software or inadequate access controls before they become a target for threat actors. Organizations also benefit from proactively educating their staff on emerging threats, common attack vectors, digital hygiene, and the need to report suspicious activity.

Network segmentation helps prevent the spread of ransomware and malware by isolating backup systems and sensitive databases from the broader hospital network. Another critical safeguard is multi-factor authentication (MFA). Countless data breaches have proven that passwords alone are insufficient. Implementing MFA lowers the odds of unauthorized access even if credentials are compromised.

Additionally, establishing read-only emergency access to electronic health records for essential staff can prevent workflow bottlenecks without compromising compliance.

In parallel, manual documentation protocols should be outlined in case systems go offline, allowing for continued patient care without unnecessary compliance risks.

### Can your organization weather the storm?

The question isn't *if* another disaster will strike; it is *when*. The real concern is whether the healthcare sector has the infrastructure, policies, and risk management strategies to minimize the impact when it does.

Past incidents have made one thing clear: Organizations that invest in strong infrastructure, diversified storage, and cybersecurity recover faster with less data loss. Those that don't face prolonged downtime, compliance violations, reputational damage, and, in some cases, permanent loss of critical patient records. Waiting until something goes wrong isn't an option; protecting ePHI isn't just a compliance issue; it is a matter of patient safety, regulatory responsibility, and the long-term stability of healthcare institutions. CT

#### Endnotes

1. World Meteorological Organization, "Weather-related disasters increase over past 50 years, causing more damage, fewer deaths," news release, August 31, 2021, <https://wmo.int/media/news/weather-related-disasters-increase-over-past-50-years-causing-more-damage-fewer-deaths>.
2. Steven H. Brown et al., "Use of Electronic Health Records in Disaster Response: The Experience of Department of Veterans Affairs After Hurricane Katrina," *American Journal of Public Health* 97, Supplement\_1, (April 2007): S136–S141, <https://doi.org/10.2105/AJPH.2006.104943>.
3. Nicole Lurie and Farzad Mostashari, "Electronic Health Records Prove to be Invaluable After Crisis," *Health IT Buzz*, June 22, 2011, <https://www.healthit.gov/buzz-blog/ehr-case-studies/electronic-health-records-prove-invaluable-crisis>.
4. Sheilla L. Rodriguez-Madera et al., "The impact of Hurricane Maria on Puerto Rico's health system: post-disaster perceptions and experiences of health care providers and administrators," *Global Health Research and Policy* 6, (November 2021): 44, <https://doi.org/10.1186/s41256-021-00228-w>.
5. Stephanie Baum, "Hurricane Sandy proves the value of health IT infrastructure, state info exchanges," *MedCity News*, October 30, 2012, <https://medcitynews.com/2012/10/hurricane-sandy-underscores-new-yorks-health-information-exchange-and-data-storage-logistics>.
6. Emily Alpert Reyes, Bernard J. Wolfson, and Molly Castle Work, "Doctors, nurses press ahead as wildfires strain L.A.'s healthcare," *Los Angeles Times*, January 10, 2025, <https://www.latimes.com/california/story/2025-01-10/la-wildfires-strain-la-healthcare>.

### Takeaways

- ◆ Natural disasters expose healthcare IT vulnerabilities, threatening both patient safety and data security; however, HIPAA compliance is still mandatory even during crises.
- ◆ While digital records help mitigate disruption, their effectiveness depends on stable power, connectivity, and infrastructure.
- ◆ Disaster preparedness must be continuous; regular simulations, audits, and updated protocols are essential for maintaining compliance and readiness.
- ◆ Relying solely on cloud or on-premises systems is risky; a hybrid model ensures better accessibility during outages.
- ◆ Cyberattacks spike during disasters as threat actors exploit weakened defenses; having strong access controls, employee awareness, multi-factor authentication, and segmented networks helps reduce the risk of breaches.

# HCCA webinars

## Want to stay up to date on the latest in healthcare compliance?

Explore topics like regulatory updates, data privacy, managed care, telehealth, and much more from the comfort of your home or office with HCCA® webinars!

HCCA offers a robust schedule of interactive healthcare compliance webinars each year.

Attend a live webinar and earn continuing education units (CEUs). You can also instantly access previously recorded webinars in our On-Demand Learning Center.



HCCA members get their choice of any four webinars free each year, and save on additional registrations!

**See what's coming up**  
[hcca-info.org/webinars](https://hcca-info.org/webinars)





# Do I still belong?


by Kelly M. Willenberg

**I**n the evolving landscape of research compliance, professionals often find themselves grappling with a question that is as personal as it is professional: Do I still belong? Belonging is fueled by connection, meaning, and purpose. When we belong, we feel valued, aligned, and confident. We perform better when we are resilient and encouraged. For research compliance officers, a dilemma can emerge from shifts in regulatory frameworks, organizational priorities, or increasing reliance on technology. Understanding and addressing these feelings of displacement is vital for personal well-being and maintaining the integrity and efficacy of research compliance programs.

Research compliance officers are essential in ensuring that research activities adhere to ethical and regulatory standards. They are the gatekeepers of integrity, balancing the dual responsibilities of supporting research innovation and safeguarding against risks. However, this role is not without its challenges. Regulatory landscapes are constantly shifting, with new guidelines and requirements adding layers of complexity. At the same time, the rise of automation and data analytics in compliance tasks may leave some officers questioning their relevance. The past six months have seen significant changes and unknowns in compliance and governance. There were new executive orders, sudden grant cuts, stop work orders, and many layoffs. Navigating these challenging times requires

focusing on the human side of what we do. As we move toward more technology and artificial intelligence, we cannot replicate the nuances of ethical discernment and relationships where the ability to delve into context and conflict becomes indispensable.

So, what can you do? Advocate for your contributions by celebrating others' achievements. Engage with the community by building relationships and networks. Utilize the HCCA community by joining discussion groups, attending webinars, and attending live events while exchanging ideas. Communicate your value to advocate for your team's contributions to the broader institution or company. You will also build trust, providing a sense of belonging to the profession. Always encourage and embrace lifelong learning. The field of research compliance is dynamic. Staying updated on new regulations, trends, and tools can help you remain relevant and confident in your role and help others feel a sense of purpose.

Ultimately, the question of belonging is one of identity. Your role may evolve as a research compliance officer, but your commitment to fostering ethical research practices remains a cornerstone of your professional identity. In adapting to change, you reaffirm your place in the field and the enduring significance of your work. Help your team feel that sense of belonging to their roles, positions, customers, and themselves. "Community offsets loneliness. It gives people a vitally necessary sense of belonging."<sup>1</sup> 



**Kelly M. Willenberg**

DBA, RN, CHRC, CHC

([kelly@kellywillenberg.com](mailto:kelly@kellywillenberg.com),

[bit.ly/in-Kelly-Willenberg](https://bit.ly/in-Kelly-Willenberg))

is the President and CEO of  
Kelly Willenberg LLC in Greenville, SC.

## Endnotes

1. Alvin Toffler, *The Third Wave* (New York: William Morrow, 1980).



# WHEN PUBLIC VOICES VANISH: LEGAL RISKS TO HEALTH TRANSPARENCY

by Stacey Lee



**Stacey Lee**

JD

*(staceyb.lee@jhu.edu) is a Professor at Johns Hopkins Carey Business School with a joint appointment at the Bloomberg School of Public Health in Baltimore, MD.*

**P**ublic participation has long served as a cornerstone of health regulatory development. Yet, recent shifts in federal agency approaches to stakeholder engagement create urgent compliance risks for healthcare organizations. As federal agencies alter their procedures for public input, compliance officers face immediate challenges in tracking, interpreting, and implementing rapidly changing regulations without the benefit of transparent regulatory development processes.

## **The legal foundation of public input**

The Administrative Procedure Act (APA) establishes strict procedural requirements that federal agencies must follow when developing regulations.<sup>1</sup> These requirements aren't merely bureaucratic formalities; they create legally enforceable guardrails that protect both public and regulated entities.

## **Core legal requirements**

Under the APA, agencies must generally provide:

- ◆ Notice of proposed rulemaking
- ◆ Opportunity for public comment
- ◆ Consideration of significant comments before finalizing rules
- ◆ Adequate justification for rule decisions

When these procedures are bypassed or abbreviated, regulated entities face both operational uncertainty and potential legal vulnerability. This procedural foundation directly impacts compliance teams' ability to maintain organizational compliance.

## **Recent agency shifts: Compliance implications**

Several federal health agencies have recently revised their approaches to public engagement, resulting in a cascade of compliance challenges.

In February 2025, the U.S. Department of Health and Human Services (HHS) rescinded a longstanding policy requiring notice and comment for certain benefit program rules. This change was formalized in the department's "Policy on Adhering to the Text of the Administrative Procedure Act" published in the *Federal Register*.<sup>2</sup> While the APA exempts benefit program rules from formal comment processes, HHS's longstanding internal policy had gone beyond the APA's requirements. The 2025 rescission now aligns departmental procedures with the statute, significantly altering expectations for public engagement in policymaking.

**Compliance impact:** Without consistent notice-and-comment periods, compliance teams may face dramatically shorter time frames to evaluate and implement new requirements. Organizations that historically relied on the regulatory development process to prepare for implementation may find themselves scrambling to adapt.

The U.S. Food and Drug Administration (FDA) has recently revised several advisory committee meeting procedures. These include shortened public notice periods in some cases, limiting speaker time in open hearings, and increasingly shifting to virtual meetings. The agency has also released briefing documents just 48 hours before meetings in some instances, compressing preparation timelines for stakeholders.<sup>3</sup>

**Compliance impact:** For pharmaceutical and device companies, these procedural changes significantly compress the timeline for analyzing FDA briefing materials and preparing responses to potential approval concerns. Compliance officers now

have just two business days to review scientific materials, assess regulatory implications, and develop compliant response strategies. Companies must restructure their FDA meeting preparation protocols to accommodate these accelerated timelines or risk being unprepared for critical regulatory discussions.

In December 2024, the National Institutes of Health (NIH) issued a revised Public Access Policy, effective for manuscripts accepted after July 1, 2025.<sup>4</sup> This policy eliminates the prior 12-month embargo and requires that NIH-funded publications be made publicly available within 30 days of publication. The revised policy also mandates immediate sharing of supporting datasets, removing the previous six-month grace period. Unlike earlier iterations, the new policy does not include phased implementation — requirements are applied uniformly (Note: As of May 2025, this is the primary source for the December 2024 update, effective July 1, 2025, which requires NIH-funded publications to be made publicly available within 30 days of publication and mandates immediate sharing of supporting datasets. If/when NIH posts a specific policy notice or FAQ for the July 2025 changes, that link should be substituted.)

**Compliance impact:** Research institutions now face dramatically accelerated compliance deadlines with no transition period. Organizations must simultaneously revise their publication submission workflows, data management protocols, and researcher training programs to ensure consistency and effectiveness. Eliminating the embargo period creates particular challenges for clinical research compliance, as institutions must develop new processes to ensure

patient privacy protections while meeting the accelerated data-sharing requirements. Many academic medical centers report that their compliance systems cannot be updated within the compressed time frame, creating immediate risks of noncompliance with grant obligations.<sup>5</sup>

### Legal vulnerabilities created by process changes

From a compliance perspective, these procedural adjustments create several distinct legal risks that require immediate attention. Each agency modification potentially conflicts with specific APA requirements, creating actionable legal vulnerabilities.

### Administrative law challenges

The APA explicitly requires agencies to provide (1) adequate notice of proposed rulemaking, (2) meaningful opportunity for public participation, and (3) a reasoned explanation of the final rule that responds to significant comments. The recent agency modifications appear to conflict with these core requirements in specific ways:

- ◆ HHS's proposed elimination of public comment periods directly contradicts APA § 553(c), which requires agencies to "give interested persons an opportunity to participate in the rule making."
- ◆ FDA's shortened timeline for materials review may violate the "meaningful opportunity" standard established in *MCI Telecommunications Corp. v. FCC*,<sup>6</sup> which held that comment periods must provide sufficient time for affected parties to analyze and respond to agency proposals.
- ◆ NIH's elimination of the implementation review period



conflicts with APA requirements for a “concise general statement of their basis and purpose” that addresses stakeholder concerns.

**Case example:** In *American Hospital Association v. Azar*,<sup>7</sup> a federal district court invalidated the Centers for Medicare & Medicaid Services’ Transparency in Coverage rule implementation timeline because the agency failed to provide sufficient time for organizational compliance preparations despite stakeholder feedback identifying operational barriers. Healthcare organizations that had already invested in compliance systems faced significant costs in adjusting to the court-modified timeline.

### Weakened legal defensibility

Regulations lacking a robust administrative record are harder to defend against legal challenges, creating downstream uncertainty for compliant organizations.

**Compliance tip:** Document your organization’s good-faith efforts to implement regulations developed through abbreviated processes. Documentation may prove valuable if the regulation faces subsequent legal challenges.

### Increased interpretation burden

When rules are issued without stakeholder feedback, they often lack operational clarity. This shifts the interpretive burden to compliance officers, who must make judgment calls with limited regulatory guidance.

**Compliance tool:** Create a standardized “regulatory interpretation memo” template to document how your organization interprets ambiguous regulatory requirements, including the rationale for your approach and any external guidance consulted.

### Operational impacts on compliance functions

The reduced transparency in regulatory development directly affects day-to-day compliance operations in healthcare settings.

#### Compressed implementation timelines

- ◆ Organizations must now implement changes in 30–60 days versus previous 90–180 days timelines
- ◆ Staff training must be accelerated while maintaining quality
- ◆ Technology system updates face compressed testing periods
- ◆ Documentation updates require rapid approval cycles

**Action step:** Develop a rapid response protocol for addressing shortened implementation timelines. Identify key stakeholders who can be quickly mobilized when new requirements emerge with minimal notice.

#### Documentation challenges

- ◆ More extensive documentation of internal decision-making becomes necessary
- ◆ Interpretation rationales must be thoroughly recorded
- ◆ Implementation decisions require stronger justification
- ◆ Contemporaneous documentation becomes essential for potential legal challenges

#### Resource allocation pressures

- ◆ Compliance teams face competing emergent priorities.
- ◆ Legal review resources become strained.
- ◆ Training teams must develop materials with less preparation time.

- ◆ IT resources may need emergency reassignment.

### Key developments to monitor

Compliance officers should closely track the following indicators and upcoming developments to anticipate further changes in agency procedure:

#### Near-term monitoring priorities

- ◆ Impact of HHS’s March 2025 rescission of the Richardson Waiver limiting public comment opportunities;<sup>8</sup> ongoing monitoring of stakeholder responses and follow-up actions
- ◆ FDA Advisory Committee procedural manual update (scheduled for July 2025)
- ◆ NIH implementation guidance for revised public access policy (pending)
- ◆ Industry association legal challenges to procedural changes
- ◆ Congressional oversight hearings on agency procedural changes

### Warning signs of increased compliance risk

- ◆ Agency use of “interim final rules” with delayed or no comment periods
- ◆ Shortened time between proposed and final rules (less than 60 days)
- ◆ Reduced availability of agency guidance documents
- ◆ Elimination of technical assistance webinars for new requirements
- ◆ Withdrawal of previously published guidance without replacement

### Proactive strategies for compliance teams

While these challenges are significant, they also present

an opportunity for compliance officers to demonstrate their strategic value.

The following are specific actions to consider:

### Enhance regulatory monitoring systems

Establish a more robust system for tracking regulatory developments across healthcare agencies. Don't rely solely on formal notice-and-comment alerts.

**Implementation tip:** Create agency-specific monitoring protocols that include:

- ◆ Daily checks of agency websites and social media
- ◆ Automated alerts from the *Federal Register*
- ◆ Regular review of agency meeting minutes and transcripts
- ◆ Monitoring of trade association updates

### Document interpretive decisions

When regulations lack clarity, thoroughly document your

organization's interpretation process. Documentation template elements should include:

- ◆ Regulatory requirement text
- ◆ Identified ambiguities
- ◆ Interpretive options considered
- ◆ Selected approach with rationale
- ◆ Legal authorities consulted
- ◆ Implementation timeline
- ◆ Review schedule

### Engage in pre-rulemaking activities

Identify and participate in agency listening sessions, public meetings, and informal feedback opportunities that occur before formal rulemaking begins.

#### Practical approach:

Designate a team member to monitor agency calendars for upcoming listening sessions and create a streamlined process for developing organizational input — especially on short notice.

### Strengthen legal partnerships

Develop closer working relationships with internal

and external legal counsel specializing in administrative law.

#### Collaboration model:

Consider implementing quarterly “regulatory landscape” meetings that bring compliance and legal teams together to anticipate and prepare for upcoming regulatory changes.

### Leverage trade associations

Industry associations often have enhanced access to agency officials and advance notice of regulatory shifts.

#### Engagement strategy:

Actively participate in association compliance committees and regulatory working groups to gain early insights into agency thinking and contribute to collective advocacy efforts.

### Conclusion

The erosion of transparent regulatory development processes creates significant challenges for healthcare compliance functions. By strengthening monitoring,

Table 1: Comparing traditional vs. emerging regulatory process response strategies

Process element	Traditional approach	New recommended approach
Monitoring	Rely on <i>Federal Register</i> notices	Implement multichannel agency monitoring
Comment preparation	Standard 60-day timeline	Rapid response capability (10–15 days)
Implementation	Sequential planning approach	Parallel implementation workstreams
Documentation	Focus on final rule requirements	Document interpretation rationale extensively
Training	Comprehensive pre-implementation training	Modular, just-in-time learning approach

documentation, and engagement strategies, compliance officers can help their organizations navigate this shifting landscape while maintaining both operational effectiveness and legal defensibility.

For compliance professionals, the goal isn't merely to adapt to reduced transparency; it's to develop resilient systems that maintain compliance integrity even when regulatory development processes become less predictable and participatory. <sup>CT</sup>

#### Endnotes

1. Administrative Procedure Act, 5 U.S.C. § 553(c).
2. Policy on Adhering to the Text of the Administrative Procedure Act, 90 Fed. Reg. 11,029 (March 3, 2025), <https://www.federalregister.gov/documents/2025/03/03/2025-03300/policy-on-adhering-to-the-text-of-the-administrative-procedure-act>.
3. U.S. Government Accountability Office, "Government Auditing Standards 2024 Revision," GAO-24-106786, February 1, 2024. <https://www.gao.gov/products/gao-24-106786>.
4. National Institutes of Health, "NIH Public Access Policy Overview: Public Access Policy Details," accessed May 26, 2025, <https://sharing.nih.gov/public-access-policy/public-access-policy-overview#public-access-policy-details>.
5. National Academies of Sciences, Engineering, and Medicine, *Optimizing the Nation's Investment in Academic Research: A New Regulatory Framework for the 21st Century* (Washington, DC: The National Academies Press, 2016), <https://doi.org/10.17226/21824>.
6. MCI Telecommunications Corp. v. FCC, 57 F.3d 1136 (D.C. Cir. 1995).
7. American Hospital Association v. Azar, 385 F. Supp. 3d 1 (D.D.C. 2019).
8. Policy on Adhering to the Text of the Administrative Procedure Act, 90 Fed. Reg. 11,029.

#### Takeaways

- ◆ Public input in regulatory development provides legal safeguards that directly impact the effectiveness of compliance programs.
- ◆ Recent actions by federal health agencies have reduced transparency and stakeholder engagement in regulatory development.
- ◆ Organizations face increased compliance risk when regulations are developed without adequate public input.
- ◆ Compliance officers should enhance monitoring, documentation, and legal coordination to mitigate regulatory uncertainty.
- ◆ Proactive engagement in pre-rulemaking activities can help identify compliance risks before regulations are finalized.

#### SCCE & HCCA 2024–2025 BOARD OF DIRECTORS

##### EXECUTIVE COMMITTEE

###### Louis Perold, CCEP, CCEP-I

SCCE & HCCA President

Principal, Citadel Compliance, Pretoria, South Africa

###### Greg Triguba, JD, CCEP, CCEP-I

SCCE & HCCA Vice President

Principal, Compliance Integrity Solutions, Bothell, WA, USA

###### Kelly Willenberg, DBA, RN, CHRC, CHC

SCCE & HCCA Second Vice President

Owner, Kelly Willenberg & Associates, Greenville, SC, USA

###### Betsy Wade, MPH, CHC, CHPC, CNA

SCCE & HCCA Treasurer

Chief Compliance and Ethics Officer, Signature HealthCARE, Louisville, KY, USA

###### Jiajia Veronica Xu, CCEP, CHC, CHPC

SCCE & HCCA Secretary

Chief Compliance Officer, Saber Healthcare Group, Cleveland, OH, USA

###### Niurka Adorno-Davies, JD, CHC

SCCE & HCCA Non-Officer of the Executive Committee

AVP Compliance, Molina Healthcare, Charleston, SC, USA

###### R. Brett Short, CHC, CHPC, CHRC

SCCE & HCCA Immediate Past President

UK HealthCare, University of Kentucky, KY, USA

###### Walter E. Johnson, CCEP, CCEP-I, CHC, CHPC

SCCE & HCCA Past President

Assistant Privacy Officer, Inova Health System, Falls Church, VA, USA

##### EX-OFFICIO EXECUTIVE COMMITTEE

###### Stephen Warch, JD

SCCE & HCCA General Counsel, Nilan Johnson Lewis, PA,

Minneapolis, MN, USA

##### BOARD MEMBERS

###### Adam Balfour, CCEP

Vice President and General Counsel for Corporate Compliance and Data Privacy, Bridgestone Americas Inc., Nashville, TN, USA

###### Hassan Chaudry, MBA, CCEP, CAMS

POSCO JV Chief Compliance Officer, General Motors, Montreal, Quebec, Canada

###### Odell Guyton, CCEP, CCEP-I

SCCE Co-Founder, Compliance & Ethics Professional, Quilcene, WA, USA

###### Shin Jae Kim, CCEP, CCEP-I

Partner, TozziniFreire Advogados, São Paulo, Brazil

###### Lisa Kuca, CCEP

Enterprise Risk Management Executive – Regulatory Compliance & Ethics, Mid-Atlantic Region, USA

###### David Lane, PhD

Vice President & Chief Compliance Officer, Providence St. Joseph Health, Renton, WA, USA

###### Judith W. Spain, JD, CCEP

Compliance Collaborative Program Consultant, Georgia Independent Colleges Association, Atlanta, GA, USA

###### Debbie Troklus, CHRC, CHC-F, CCEP-F, CHPC, CCEP-I

President, Troklus Compliance Consulting LLC, Louisville, KY, USA

###### Sheryl Vacca, RN, MS, CCEP-I, CCEP-F, CHC-F, CHPC, CHRC

President, Vacca Consulting LLC, Scottsdale, AZ, USA

###### Art Weiss, JD, CCEP-F, CCEP-I

Principal, Strategic Compliance and Ethics Advisors, Henderson, NV, USA



# Multi-factor authentication's role in cybersecurity

by Frank Ruelas Sr.

**A**s healthcare increasingly relies on interconnected digital systems for everything from patient records to critical care delivery, cybersecurity has transitioned from a technical concern to a core operational priority and a constant point of focus for leadership. A prime objective of effective cybersecurity practices is to minimize the likelihood that an unauthorized person will access an information system using an authorized user's access. To decrease the likelihood of this happening, multi-factor authentication (MFA) is a widely used tool.

The following is information about MFA so you can understand it and respond to pushbacks against its use.


At its core, MFA is a process used to authenticate that an authorized person trying to access an information system is who they claim to be. This is done by using a combination of the following three factors that make up MFA.

Factor 1 is a knowledge factor often referred to as something a person knows. Examples include a password, personal identification number, passphrase, or the answer to a security question. Factor 2 is a possession factor that describes something a person has in their possession at the time the authentication process is occurring. An example that people may be familiar with is that of a smartphone. Factor 3 is an inference factor often described as something you are. Examples include detecting biometrics using such devices as a fingerprint sensor or facial recognition application.

In practice, MFA uses at least two different factors to authenticate a user. For example, logging into a bank account using an internet-connected device. To access their bank account information, individuals are asked to

enter their username and password (Factor 1) and then enter a security code sent by text, email, or voice call (Factor 2). In this scenario, if someone were to guess a person's username and password, that person would still be unable to access the bank account information unless they were also somehow able to meet the Factor 2 requirement. This might include receiving a series of text or numbers that must be inputted during the login process.

When implementing MFA, you may encounter pushbacks or resistance from users. These pushbacks may include the idea that MFA is inconvenient and takes too much time. Another pushback is that people feel it is unnecessary because no one would be interested in trying to use their credentials to access an information system. The good news is that there are good responses that one can offer when encountering these pushbacks.

MFA has become increasingly user-friendly. The interfaces used are very straightforward and use actions or behaviors that many users are comfortable and familiar with, such as smartphones or email. Accessing an information system using MFA typically adds only a few seconds to the entire authentication process. As for the idea that people may think their account is not a target, one can share that unauthorized individuals look for any weakness they can to try to access an information system. This includes trying to access authorized users' accounts, which could then result in unauthorized users accessing information that could lead to a breach, the theft of valuable data, or uploading software that could disrupt the information system. 



**Frank Ruelas Sr.**

*([frank@complianceacademy.com](mailto:frank@complianceacademy.com))*

*is a Compliance Professional  
in Casa Grande, AZ.*

# RANSOMWARE RISK READINESS

by Ali Pabrai



## Ali Pabrai

MSEE, DoD CMMC  
(Lead CCA, CCP, RPA, RP),  
HITRUST CCSFP

*(ali.pabrai@ecfirst.com, linkedin.com/in/pabrai/) is the Chief Executive Officer at ecfirst in Irvine, CA.*

A real-world situation in a small rural hospital in America: John Pascal, a nurse, receives a fraudulent email from a person assuming the title of an IT support person from within the healthcare organization where he is employed. John is forwarded an email and is asked to click on a link to update the password for the electronic health record (EHR), as it has expired. The link directs an unsuspecting John to a fake login page, which then collects the credentials and sends this information to attackers. Attackers can now access the hospital's EHR application and the associated databases, which contain terabytes of protected health information (PHI) and other confidential data.

*A ransomware cyberattack has just taken place.*

The hackers have now encrypted patient data. Subsequently, access to systems and applications has been restricted. A pop-up appears when

clinical or other staff attempt to log in and access healthcare applications. **ACCESS DENIED!**

Clinical staff, such as nurses and physicians, are unable to access applications and do not have visibility into patient data. This scenario can cause a plethora of disastrous circumstances regarding patient safety risks (delayed/missed treatments, medical errors, inability to monitor high-risk patients) as well as operational delays. This is the *ransomware risk* that organizations face.

We must remember that *cyber safety IS patient safety*.

## Beyond ransomware, risk of exfiltration

So, what exactly is ransomware? Ransomware is a distinct type of malware (malicious software) designed to deny users access to their data by encrypting it with a key known only

to the attacker. Once encryption is complete, the ransomware demands payment—typically in cryptocurrency, such as Bitcoin—in exchange for the decryption key.

However, hackers may deploy ransomware that also destroys or *exfiltrates*. Exfiltration is the unauthorized transfer of information from an information system.

### **Not if, but when**

Ransomware attacks should not be considered an *if*, but a *when*! Organizations must be prepared as ransomware attacks are highly disruptive to healthcare operations, including patient care.

The combination of a large volume of digitized patient data, interconnected medical devices, and limited cybersecurity operations staff, make healthcare organizations prime targets for ransomware attacks.

Attack surfaces have increased, providing greater opportunities for threat actors to compromise healthcare systems and applications. Further, Ransomware-as-a-Service (RaaS) has lowered entry barriers for attackers lacking technical expertise.

### **HIPAA compliance and ransomware**

On average, there have been 4,000 daily ransomware attacks since early 2016.<sup>1</sup> Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure to deny the organization access to its own data by encrypting it.

Exfiltration of confidential information such as PHI is a serious business risk for healthcare organizations.

The attacks are costly, with healthcare organizations losing up to \$900,000 per day on downtime

alone.<sup>2</sup> Healthcare organizations that admitted to paying the ransom, the median payment was \$1.5 million, and the average payment was \$4.4 million.

Clinically integrated care networks of connected devices and medical technologies have broadened the digital attack surface—something threat actors are increasingly exploiting.

Healthcare organizations are online and digitized more than ever. Connecting critical medical devices such as CT scanners, patient monitoring systems, and infusion pumps to networks reflects the reality of patient data flowing across a complex computing ecosystem—an ecosystem that spans mobile devices and a multi-cloud environment.

“On average, 70% of a hospital's endpoints are not computers but rather devices.” Further, healthcare organizations also transmit vast amounts of data. More than 88% of hospitals report electronically sending and obtaining patient health information, and more than 60% report integrating that information into their EHRs.

Many healthcare organizations' business continuity plans are outdated or inadequate in addressing cyberthreats like ransomware.

*The bottom line is that ransomware attacks disrupt business processes and operations.*

### **Tracing a ransomware attack**

So, what are the techniques used by hackers? There are typically three ways a ransomware event is successful.

◆ **First**, attackers used compromised credentials to access the network via a vulnerable remote access gateway without multi-factor

authentication (MFA). They encrypted critical infrastructure and exfiltrated sensitive data in a double extortion scheme, threatening to release it unless a ransom was paid.

◆ **Second**, attackers exploited vulnerabilities in the organization's unpatched legacy software, moving laterally to compromise patient scheduling and medical records. Using a double extortion tactic, they exfiltrated sensitive data and threatened to release it unless a ransom was paid.

**Clinically integrated care networks of connected devices and medical technologies have broadened the digital attack surface—something threat actors are increasingly exploiting.**

◆ **Third**, attackers used phishing emails to access the organizational network and exploited unpatched vulnerabilities to deploy ransomware, encrypting EHR and patient care systems. In a double extortion tactic, they exfiltrated sensitive patient and financial data, threatening to leak it if the ransom was not paid.

After gaining initial access, attackers often conduct network



reconnaissance, which can be identified by indicators such as unusual scanning activity.

Once ransomware is deployed, attackers typically move quickly to encrypt critical systems and data, often within a matter of hours. They target essential infrastructure, such as patient records, diagnostic systems, and even billing operations, to maximize the impact and pressure on healthcare organizations to pay the ransom.

### Ransomware readiness is about establishing resilience

Ransomware resilience in healthcare cybersecurity involves ensuring that the computing ecosystem—including a multi-cloud environment—can withstand and recover from attacks. A comprehensive approach to resilience is vital, focusing not only on safeguarding patient data but also on reinforcing the entire infrastructure that supports healthcare operations. This includes the entire computing ecosystem: network, supply chain, medical devices, and more.

Areas that organizations should prioritize in their journey to mitigate ransomware risk and establish ransomware readiness programs include:

- ◆ Creating a ransomware readiness plan. Align this plan with the National Institute of Standards and Technology (NIST) IR8374 guidance document on ransomware (discussed in the next section).
- ◆ Developing a ransomware readiness policy.
- ◆ Performing a business impact analysis to clearly identify critical assets, systems, and applications and establish recovery priorities.

- ◆ Enhancing the business continuity plan (BCP) and the disaster recovery plan (DRP) to document step-by-step procedures is imperative for recovery in a predictable, defined time frame.
- ◆ Crafting ransomware readiness procedures (step-by-step guidance for recovery) and aligning with the BCP and DRP documents.
- ◆ Performing regular social engineering phishing exercises to ensure workforce members are trained on ransomware and better skilled to detect such attacks.
- ◆ Aligning the ransomware readiness program with the organization's incident response plan.
- ◆ Implementing near real-time threat detection controls and associated capabilities.

These are core components of a ransomware readiness program and should be managed and monitored continually.

### NISTIR 8374, a valued ransomware resource

*NISTIR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile*, is a valuable resource for establishing the foundation for an organization's ransomware readiness program.<sup>3</sup> The NISTIR 8374 publication is aligned with the NIST Cybersecurity Framework and is an excellent reference to leverage for identifying possible gaps in the ransomware readiness program.

NISTIR 8374 maps security objectives to the NIST Cybersecurity Framework functions:

- ◆ **Identify:** Organizations should inventory assets,

assess vulnerabilities, map data flows, and classify critical systems to understand ransomware exposure. A clear understanding of risks allows organizations to allocate resources effectively.

- ◆ **Protect:** Implementing MFA, access controls, software patching, endpoint protection, network segmentation, and zero-trust principles minimize attack surfaces and limits the spread of ransomware if an infection occurs.
- ◆ **Detect:** Continuous monitoring, anomaly detection, and real-time threat intelligence help identify ransomware activity before it spreads. Organizations should deploy intrusion detection systems, endpoint detection and response tools, and behavioral analytics to spot early indicators of compromise.
- ◆ **Respond:** A structured incident response plan with predefined containment actions, forensic analysis, and internal/external communication protocols ensures a rapid and coordinated response. Organizations should conduct regular ransomware tabletop exercises to test and refine their response strategies.
- ◆ **Recover:** Regular, tested backups, disaster recovery plans, and business continuity measures are essential for restoring operations after an attack. Data restoration processes must be frequently tested to ensure functionality in real-world attack scenarios.

Organizations should train employees, conduct ransomware simulations, and establish response playbooks to ensure readiness when an attack occurs. Additionally,

NISTIR 8374 also aligns with ISO/IEC 27001 and NIST SP 800-53 Rev. 5,<sup>4</sup> which reinforce best practices across industries, and NIST SP 800-61 r3 (another valuable resource) focuses on incident response.<sup>5</sup>

### Risk to readiness

Healthcare organizations face a range of cybersecurity threats, with ransomware attacks emerging as one of the most significant. Email remains one of the largest vectors for delivering malware and phishing attacks for ransomware attacks. Remember, the threat is global, and the impact is local. Today's attackers are advanced and persistent, integrating artificial intelligence tools to accelerate attacks. These attacks are much more difficult to detect than ever before. Organizations must be better prepared and move from ransomware risk to ransomware readiness.

As we have discussed, a ransomware attack process typically follows a consistent approach: gaining initial

access to the network — often through phishing or exploiting vulnerabilities — followed by the deployment of ransomware to encrypt critical systems and data. Once initial access is gained — typically through phishing or malware delivered via email — threat actors move to the next phase: the deployment of ransomware. The proliferation of RaaS has made attacks more accessible and frequent.

An organization's ransomware readiness program should align with both the NISTIR 8374 and NIST SP 800-61r3. By leveraging NISTIR 8374, organizations can reduce attack impact, recover

faster, and ensure business continuity.

Ransomware attacks are disruptive. Consider the impact of a ransomware attack on a 44-bed hospital in Spring Valley, IL.<sup>6</sup> The hospital never recovered. It shut down in 2023 partly due to a 2021 ransomware attack that worsened financial woes and other problems already dealt with before the incident.

Establishing a credible ransomware readiness program ensures that healthcare organizations are resilient to such attacks. It is not all about risk mitigation; it is about ransomware risk resilience. CT

### Endnotes

1. U.S. Department of Health and Human Services, Office for Civil Rights, "Fact Sheet Ransomware and HIPAA," content last reviewed September 20, 2021, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>.
2. Microsoft, "US Healthcare at risk: Strengthening resiliency against ransomware attacks," accessed May 5, 2025, <https://www.microsoft.com/en-us/security/insider/emerging-threats/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks>.
3. William C. Barker et al., *Ransomware Risk Management: A Cybersecurity Framework Profile*, NISTIR 8374, February 2022, <https://doi.org/10.6028/NIST.IR.8374>.
4. William C. Barker et al., *Ransomware Risk Management: A Cybersecurity Framework Profile*, NISTIR 8374, National Institute of Standards and Technology, U.S. Department of Commerce, February 2022, <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf>.
5. National Institute of Standards and Technology, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," April 2025, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.ipd.pdf>.
6. Kevin Collier, "An Illinois hospital is the first health care facility to link its closing to a ransomware attack," NBC News, June 12, 2023, <https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983>.

### Takeaways

- ◆ Examine key phases of a ransomware attack so the organization can be better prepared to identify such events with automated, near real-time capabilities.
- ◆ Review the disruptive impact of a ransomware attack on business operations and priorities, including data. Such awareness will provide opportunities to enhance enterprise recovery processes.
- ◆ Gain insight into the value of a ransomware readiness plan, one that aligns with industry standards, such as the National Institute of Standards and Technology IR 8374, which provides a framework to address compliance mandates.
- ◆ Establish key components of a ransomware readiness program, including controls and capabilities.
- ◆ Implement steps for ransomware attack resilience to ensure confidence in managing such events.

# IS YOUR CYBERSECURITY PROGRAM REALLY VALUABLE? THREE QUESTIONS TO EXPLORE

by Eric Shoemaker



**Eric Shoemaker**

*(EricS@geniusgrc.com) is an Advisory  
Chief Information Security Officer  
at Genius GRC in Alpharetta, GA.*

Cybersecurity risk, especially brought on by third parties, shows no signs of slowing. A recent study from Imprivata released earlier this year found that **47% of organizations have experienced a data breach or cybersecurity incident in the last year that involved a third party accessing their network.**<sup>1</sup> Another interesting stat that the survey revealed? **Fifty-eight percent of respondents didn't feel that their current security plans to address third-party risk are existent or consistent.** This means there is a major opportunity for organizations in healthcare and beyond to bolster their defenses.

Just over one year ago, in February 2024, the Change Healthcare breach brought hospital and health system executives across the country to their knees.<sup>2</sup> The breach affected approximately 190 million individuals and caused widespread disruption,

such as suspended payments, inability to submit claims or receive electronic remittance, and lost revenue—which doesn't even scratch the surface of the ripple effects felt by patients and those whose access to care was severely impacted.

The Change Healthcare disaster sends a strong signal to those of us across the healthcare industry that we are at greater risk of having patient health information and other valuable data compromised. In 2023, **healthcare topped the list of industries most targeted by cybercriminals**, with the average cost per breach totaling roughly \$10.93 million.<sup>3</sup> As of midyear 2024, cybersecurity attacks had risen by 30% year-over-year.<sup>4</sup>

If you are in the 37% of healthcare organizations without an incident response plan or feel that your cybersecurity program is lacking in true value for the health of your



organization, it is not too late to make a change.<sup>5</sup>

Read on to learn three questions every team needs to be asking.

### **Question 1: What does “value” mean to your organization?**

The first piece of advice I give to anyone looking to strengthen their cybersecurity program is to define what “value” means for the organization and determine how you’re going to measure it. Understandably, the goals of the cybersecurity program need to align with the goals of the business. All too often, I see teams view regulatory requirements as the sole driver of their cybersecurity compliance program and, in turn, they miss other key areas.

Don’t get me wrong! Regulatory requirements are important, and healthcare organizations (especially) can pay the price if they don’t meet the guidelines. Take HIPAA, for example. **In 2023, the U.S. Department of Health and Human Services Office for Civil Rights reported a record number of 725 data breaches involving 500 or more records, meaning a grand total of 133 million records were exposed or impermissibly exposed.**<sup>6</sup> While the breakdown in HIPAA compliance and increase in violations is a grim reality that needs to be addressed, meeting the HIPAA Security Rule shouldn’t be your team’s only goal. Otherwise, it can become very easy for leadership and other stakeholders in the organization to resent compliance requirements. Resentment leads to reducing the budget at the first available opportunity.

Instead, value should include myriad considerations that all paint a better and brighter future for the organization’s well-being. Sit down with various

departments—including leaders from finance, development and operations, IT, sales, marketing, and others—to level-set expectations and ensure that everyone agrees on their respective expectations of your information security (InfoSec) program. See if you can define each department’s take on “How does the InfoSec program help me?”

A common area that most departments can always agree on—regardless of the size or scope of the organization—is commitment to pursuing new business. It’s possible that without a solid InfoSec program or rock-solid cybersecurity strategy in place, your organization is missing out on bringing in a valuable prospect or patient population. I recently worked with a healthcare software as a service company that frequently engages with large hospitals and revenue cycle firms and is subject to stringent cybersecurity and compliance requirements. It became readily apparent that the lack of a System and Organization Controls (SOC) 2 attestation made it more difficult to go through customer-vendor procurement processes and gave their upper management and sales team alike unnecessary friction.

Over time, we were able to help this company achieve SOC 2 attestation while also handling other pertinent tasks, such as answering security questionnaires and working with prospect risk teams to go through the process of vendor due diligence. Thanks to an interdepartmental collaboration between sales and management individuals, this company was able to bolster its cybersecurity posture and positively impact its sales funnel. Win-win!

### **Question 2: How do you measure the program’s value?**

Once your organization comes together and identifies what value means and looks like, it’s essential to ensure that the program is structured in such a way that value is measurable. There are a couple of ways to do this, starting with codifying the program in a cybersecurity program charter. This charter should be owned by the highest level of management with appropriate **input** from qualified individuals (i.e., the stakeholders from various departments, as previously defined in the article). That input could simply be the output of the discussions mentioned earlier. This charter will coerce and establish objectives and codify everyone’s roles and responsibilities.

**It’s possible that without a solid InfoSec program or rock-solid cybersecurity strategy in place, your organization is missing out on bringing in a valuable prospect or patient population.**

It’s crucial to ensure that the program is driven by one key, qualified individual. This individual will help define the program’s pillars and ensure everyone is on task. Lastly, it’s vital to consider areas such as:

◆ Vendor management



- ◆ Risk management
- ◆ Data management
- ◆ Vulnerability management
- ◆ Business continuity
- ◆ Incident response

Failure to recognize any of these areas can result in devastating consequences for the longevity of a successful cybersecurity program. Organizations that take the time upfront to structure the program appropriately and assign the right individual(s) to lead and address the various areas will have a serious advantage over those who don't.

In January of 2023, the Federal Trade Commission (FTC) enacted a revised version of the Safeguards Rule as part of the Gramm-Leach-Bliley Act. Under this rule, many nonbanks, such as insurance companies, dealerships, and revenue cycle agencies, were classified as financial institutions. The rule requires many security controls to be implemented and maintained. A healthcare revenue

cycle management company I worked with for years came to me around this time with a desire to expand its already robust approach to cybersecurity with a new emphasis on achieving the guidelines laid out in the Safeguards Rule.

This example serves as a great testament to being proactive on the front end. Thankfully, this company had already been working to manage their SOC 2 and HIPAA compliance well ahead of the new regulation that winter, so all my team had to do was a quick gap analysis. This analysis would determine two things: one, which requirements were already being met with existing controls, and two, what additional controls would need to be implemented. The gaps that did exist were few and very easy to remediate. Furthermore, the chief information officer and chief financial officer were grateful to have the added peace of mind that they were

meeting industry and government regulations.

### **Question 3: What do you do to enforce accountability and transparency?**

No cybersecurity program is complete without ensuring there are checks and balances in place to keep folks within the organization accountable. An organization's security posture is only as strong or secure as its weakest person, combined with appropriate technology safeguards. If you set people up for success, you can build off that success and have a plan with little room for error. If you set people up for failure, you know what you're going to get!

Software has come a long way over the years in helping organizations enforce transparency and longevity. It's well proven that leveraging appropriate tools ensures greater consistency and efficiency when used correctly. Much like finance departments use

Quickbooks for their accounting needs, cybersecurity teams can use governance, risk, and compliance (GRC) software to manage all aspects of the cybersecurity program. If you're not using a GRC tool to better equip yourself and your team for optimal efficiencies and success in managing your cybersecurity program, this is your sign to start.

Remember, too, that organizations that are more secure from a cybersecurity standpoint also open themselves up to more financial profitability. The revenue cycle management company I mentioned earlier, which was trying to adhere to updated FTC guidelines, had previously gone through SOC 2 attestation in 2020. In the years following that process, they have doubled in size and unlocked new revenue growth. Needless to say, there is a direct correlation between companies with robust cybersecurity measures and financial performance.

Cyberattacks have almost doubled since before the COVID-19 pandemic.<sup>7</sup> While small losses typically start at around \$500,000, extreme losses can be

upwards of \$2.5 billion. For small and large healthcare organizations alike, this kind of hit could be the difference between keeping the lights on and shutting down operations.

Having a strong security posture will also lead to your prospects and customers trusting you with their most valuable data instead of your competitors.

### In closing

As a believer in “never taking a day off from security,” here are some key questions for leadership to ask concerning your cybersecurity and compliance program:

- ◆ How does our current program meet defined objectives?

- ◆ What contractual obligations exist, and what controls have been implemented to meet these obligations?
- ◆ What cybersecurity controls have failed in the last 90 days?
- ◆ How many close calls have we had (i.e., events that could have led to a breach or other incident had one or two variables been slightly different)?

Whether you build the program with internally qualified staff or with a qualified partner, please ensure that you define a strategic, objective-oriented program that demonstrates real value to all parts of your organization on an ongoing basis. CT

### Endnotes

1. Imprivata, “Imprivata Study Finds Nearly Half of Organizations Suffered a Third-Party Security Incident in Past Year,” news release, February 13, 2025, <https://www.imprivata.com/company/press/imprivata-study-finds-nearly-half-organizations-suffered-third-party-security>.
2. Hyperproof Team, “Understanding the Change Healthcare Breach and Its Impact on Security Compliance,” updated November 6, 2024, <https://hyperproof.io/resource/understanding-the-change-healthcare-breach/>.
3. rAVE Team, “Top 10 Industries Targeted The Most By Cybercriminals,” BlogSquad, June 25, 2024, rAVE Pubs, <https://www.ravepubs.com/top-10-industries-targeted-the-most-by-cybercriminals/>.
4. Check Point Research, “Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years,” Dark Reading, news release, July 22, 2024, <https://www.darkreading.com/cyberattacks-data-breaches/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years>.
5. Steve Alder, “37% of Healthcare Organizations Do Not Have a Security Incident Response Plan,” *The HIPAA Journal*, May 29, 2024, <https://www.hipaajournal.com/37-pc-healthcare-organizations-no-security-incident-response-plan/>.
6. Steve Alder, “Healthcare Data Breach Statistics,” *The HIPAA Journal*, updated May 5, 2025, <https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=Trends%20In%20Healthcare%20Data%20Breach,were%20exposed%20or%20impermissibly%20disclosed>.
7. Fabio Natalucci, Mahvash S. Qureshi, and Felix Suntheim, “Rising Cyber Threats Pose Serious Concerns for Financial Stability,” April 9, 2024, <https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability>.

### Takeaways

- ◆ Understand the current cybersecurity landscape as well as certain complexities that make cybersecurity strategy a must-have at any healthcare organization, regardless of size.
- ◆ Discover what value means for your organization from a healthcare cybersecurity perspective and how to put an achievable plan in place.
- ◆ Remember that cybersecurity is not limited to one individual or department but instead requires a multipronged approach from the entire organization.
- ◆ Learn how to measure the value of your organization's cybersecurity strategy, such as increased vendor, risk, and data and vulnerability management, to name a few examples.
- ◆ Seek out tools that can ensure your teams stay accountable to cybersecurity goals while also providing an edge over competitors in the market.



# Stand out from the crowd

Take your career to the next level: Become certified!



## Enhance your credibility

Certification authenticates your knowledge of current compliance industry standards.



## Increase your competitive edge

Certification sets you apart in the eyes of current and future employers, calling attention to your higher-level expertise. Many employers now require certification for their roles!



## Show your commitment to the profession

Certification affirms your dedication to compliance and helps you stand out as a passionate and diligent professional.

Learn more and get started  
[hcca-info.org/certification](https://hcca-info.org/certification)





# REGIONAL HEALTHCARE COMPLIANCE CONFERENCES

Explore a diverse spectrum of topical compliance issues through in-person educational sessions led by experienced healthcare compliance professionals. As an attendee, you will have the chance to earn continuing education units and make valuable connections with compliance peers from your area.

**Get the latest best practices, strategies, and updates in:**



Regulatory  
requirements



Risk  
management



Compliance  
enforcement



Maintaining an effective  
compliance program

---

## UPCOMING DATES FOR 2025

---

September 11 • Minneapolis, MN

September 12 • Boston, MA

September 19 • Indianapolis, IN

October 10 • Louisville, KY

October 10 • Pittsburgh, PA

October 17 • Denver, CO

October 23–24 • Honolulu, HI

November 7 • Philadelphia, PA

November 7 • Scottsdale, AZ

November 14 • Nashville, TN

December 5 • Houston, TX

December 5 • San Francisco, CA

**Register online**  
[hcca-info.org/regionals](https://hcca-info.org/regionals)





# Upcoming workshops

## Take a deep dive into core compliance elements

SCCE & HCCA workshops are designed to help you strengthen your understanding of the essential elements of an effective compliance program. Led by experienced compliance professionals, each workshop focuses on a single topic to expand the depth of your knowledge.

**Learn more**  
[hcca-info.org/workshops](https://hcca-info.org/workshops)

### **Fundamentals of Compliance Investigations Workshop**

Skilled investigators teach the core principles of investigations, from planning and gathering evidence to conducting interviews and reporting results.

July 15–16, 2025 • Virtual (CT)

December 3–4, 2025 • Virtual (CT)

### **Compliance Risk Assessment and Management Workshop**

Get guidance and insights on how to conduct effective risk assessments and manage organizational risk.

September 18–19, 2025 • Nashville, TN

### **Experienced Investigator Workshop**

This workshop is for experienced investigators who already know the basic skills and for leaders who supervise the organization's investigations program.

September 18–19, 2025 • Nashville, TN

### **Creating Effective Compliance Training Workshop**

Take a deep dive into the key elements of an effective compliance & ethics training program and learn how to best motivate your workforce.

October 14–15, 2025 • Virtual (CT)

### **Compliance Auditing & Monitoring Workshop**

Learn best practices and strategies for implementing and maintaining an effective auditing and monitoring process.

November 12–13, 2025 • Virtual (CT)



## Compliance risk assessment: Mandatory or not?

*Melinda Shapiro and Ximena Restrepo (page 14) CEU*

- » Often, an effective compliance program is recommended as a condition of probation.
- » An organization that does not regularly conduct a compliance risk assessment (RA) is missing the opportunity to optimize and empower its decision-making, resource allocation, and overall risk management strategy.
- » Compliance RAs are integral tools for checking your organization's risk temperature. A high temperature score may indicate a lack of internal controls.
- » Take a proactive approach to risk mitigation rather than a reactive approach.
- » Prevent internal control failures, unexpected fines, and reputational damage by conducting your compliance RAs on a regular basis.

## False Claims Act: Preparing for and navigating internal complaints

*John Eason (page 20)*

- » The U.S. Department of Justice enforcement actions and qui tam whistleblower lawsuits under the False Claims Act (FCA) are at an all-time high, remain largely targeted at the healthcare industry, and can leave defendants with significant costs.
- » For most healthcare providers, it is a matter of when—not if—an FCA-related complaint will arise. Take proactive steps now to establish investigation protocols to ensure a quick and thorough response when such a complaint does arrive.
- » Dismissing internal compliance complaints or creating a culture where internal complaints are discouraged can lead to increased liability, scrutiny from government agencies, and reputational harm, particularly as it relates to the FCA. Every internal allegation of FCA violations should be treated with the utmost seriousness and initially viewed with an open mind.
- » Healthcare providers must act quickly to assess and scope any internal allegations implicating the FCA and determine how to staff an investigation, including the involvement of outside counsel.
- » Use any investigation as an opportunity to strengthen compliance practices, educate staff, and reduce future risk.

## Your role as an ACO compliance officer: Essential knowledge and strategies

*Divya M. Schavio and Joseph Grant (page 28) CEU*

- » **Master the Alternative Payment Models (APM) agreement:** Ensure full compliance with payer requirements by understanding financial models, maintaining audit readiness, and establishing clear documentation and reporting practices.
- » **Understand governance structures:** Know your APM's governance framework, including oversight responsibilities, voting rights, conflict-of-interest policies, and board accountability.
- » **Navigate notification requirements:** Effectively manage complex notification rules to ensure timely and compliant communications with beneficiaries, providers, and the public through approved channels.
- » **Foster cross-departmental collaboration:** Work in conjunction with finance, billing, and quality teams to align payment structures, coding practices, reporting standards, and reimbursement goals.
- » **Leverage payer support:** Engage payers early by asking precise questions through official channels to prevent compliance missteps and streamline operations.

## Maintaining compliance in the face of disaster

*Jerry Kaner (page 34)*

- » Natural disasters expose healthcare IT vulnerabilities, threatening both patient safety and data security; however, HIPAA compliance is still mandatory even during crises.
- » While digital records help mitigate disruption, their effectiveness depends on stable power, connectivity, and infrastructure.
- » Disaster preparedness must be continuous; regular simulations, audits, and updated protocols are essential for maintaining compliance and readiness.
- » Relying solely on cloud or on-premises systems is risky; a hybrid model ensures better accessibility during outages.
- » Cyberattacks spike during disasters as threat actors exploit weakened defenses; having strong access controls, employee awareness, multi-factor authentication, and segmented networks helps reduce the risk of breaches.

## When public voices vanish: Legal risks to health transparency

*Stacey Lee (page 40)*

- » Public input in regulatory development provides legal safeguards that directly impact the effectiveness of compliance programs.
- » Recent actions by federal health agencies have reduced transparency and stakeholder engagement in regulatory development.
- » Organizations face increased compliance risk when regulations are developed without adequate public input.
- » Compliance officers should enhance monitoring, documentation, and legal coordination to mitigate regulatory uncertainty.
- » Proactive engagement in pre-rulemaking activities can help identify compliance risks before regulations are finalized.

## Ransomware risk readiness

*Ali Pabrai (page 46) CEU*

- » Examine key phases of a ransomware attack so the organization can be better prepared to identify such events with automated, near real-time capabilities.
- » Review the disruptive impact of a ransomware attack on business operations and priorities, including data. Such awareness will provide opportunities to enhance enterprise recovery processes.
- » Gain insight into the value of a ransomware readiness plan, one that aligns with industry standards, such as the National Institute of Standards and Technology IR 8374, which provides a framework to address compliance mandates.
- » Establish key components of a ransomware readiness program, including controls and capabilities.
- » Implement steps for ransomware attack resilience to ensure confidence in managing such events.

## Is your cybersecurity program really valuable? Three questions to explore

*Eric Shoemaker (page 50)*

- » Understand the current cybersecurity landscape as well as certain complexities that make cybersecurity strategy a must-have at any healthcare organization, regardless of size.
- » Discover what value means for your organization from a healthcare cybersecurity perspective and how to put an achievable plan in place.
- » Remember that cybersecurity is not limited to one individual or department but instead requires a multipronged approach from the entire organization.
- » Learn how to measure the value of your organization's cybersecurity strategy, such as increased vendor, risk, and data and vulnerability management, to name a few examples.
- » Seek out tools that can ensure your teams stay accountable to cybersecurity goals while also providing an edge over competitors in the market.

# HCCA upcoming events

JULY

July  
8

AI Risk Management with HIPAA Compliance  
WEBINAR

July  
9

How to Actually Do an Audit  
WEBINAR

July  
10

The Coming Reckoning: How AI Tests  
Healthcare Regulation  
WEBINAR

July  
15–16

Fundamentals of Compliance Investigations  
Workshop  
VIRTUAL

July  
21–24

Healthcare Basic Compliance Academy  
NASHVILLE, TN

July  
30

Call Compliance...We Added Another Entity to  
Our Health System  
WEBINAR

July  
31

Compliance in Smaller Organizations  
VIRTUAL

AUGUST

August  
5

Compliance, Ethics, and Organizational Culture  
VIRTUAL

August  
18–21

Healthcare Compliance Essentials Workshop  
VIRTUAL

August  
11–14

Healthcare Basic Compliance Academy  
JERSEY CITY, NJ

August  
11–14

Healthcare Privacy Compliance Academy  
JERSEY CITY, NJ

**2025** We continue to add events and dates to our schedule. Please check the website for details.

## Fundamentals of Compliance Investigations Workshop

July 15–16 • Virtual (CT)  
December 3–4 • Virtual (CT)

## Compliance in Smaller Organizations

July 31 • Virtual (CT)

## Compliance, Ethics, and Organizational Culture

August 5 • Virtual (CT)

## Healthcare Compliance Essentials Workshop

August 18–21 • Virtual (CT)

## Compliance Risk Assessment and Management Workshop

September 18–19 • Nashville, TN

## Experienced Investigator Workshop

September 18–19 • Nashville, TN

## Compliance Auditing & Monitoring Conference

September 25 • Virtual (CT)

## Creating Effective Compliance Training Workshop

October 14–15 • Virtual (CT)

## Behavioral Health Compliance Conference

October 21 • Virtual (CT)

## Physician Practice Compliance Conference

October 28 • Virtual (CT)

## Healthcare Enforcement Compliance Conference

October 29–30 • Virtual (CT)

## Healthcare Privacy Compliance Conference

November 5 • Virtual (CT)

## Compliance Auditing & Monitoring Workshop

November 12–13 • Virtual (CT)

## Intersection of Compliance & Quality

November 18 • Virtual (CT)

## AI & Compliance

November 20 • Virtual (CT)

## Compliance & Post-Acute Care

December 2 • Virtual (CT)

## Healthcare Basic Compliance Academy

July 21–24 • Nashville, TN  
August 11–14 • Jersey City, NJ  
September 8–11 • Scottsdale, AZ  
October 6–9 • San Antonio, TX  
December 8–11 • Anaheim, CA

## Healthcare Privacy Compliance Academy

August 11–14 • Jersey City, NJ  
December 8–11 • Anaheim, CA

## Healthcare Research Compliance Academy

September 8–11 • Scottsdale, AZ

## Regional Healthcare Compliance Conference

September 11 • Minneapolis, MN  
September 12 • Boston, MA  
September 19 • Indianapolis, IN  
October 10 • Louisville, KY  
October 10 • Pittsburgh, PA  
October 17 • Denver, CO  
October 23–24 • Honolulu, HI  
November 7 • Philadelphia, PA  
November 7 • Scottsdale, AZ  
November 14 • Nashville, TN  
December 5 • Houston, TX  
December 5 • San Francisco, CA

## Webinars

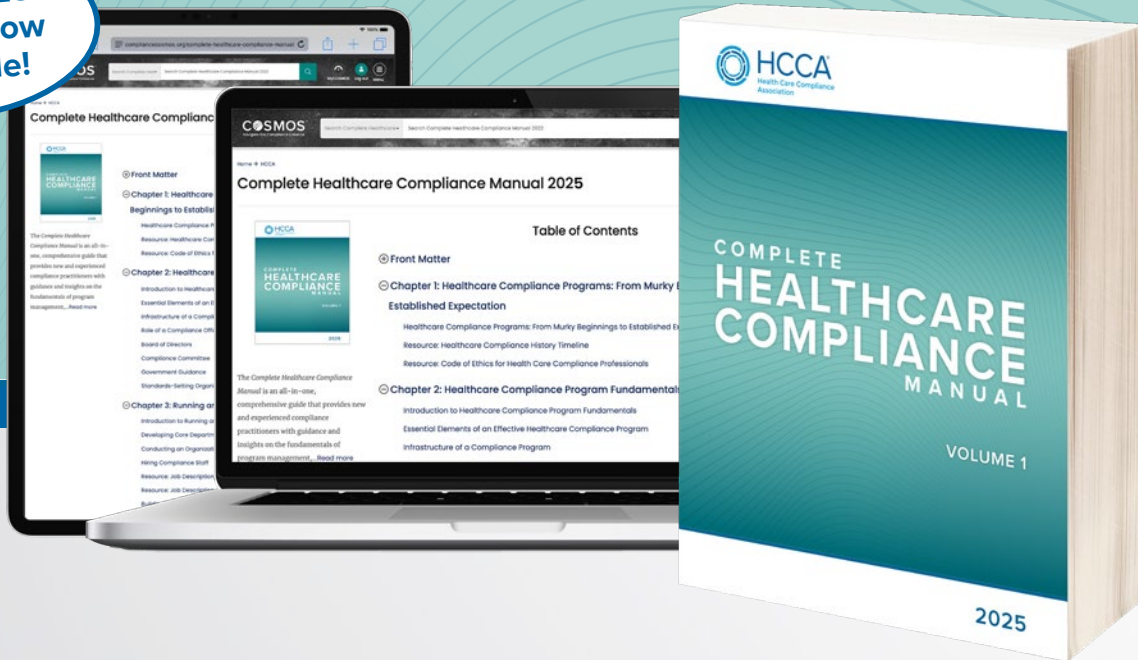
HCCA offers convenient virtual compliance education with a robust calendar of time-conscious webinars. Attending a webinar allows you to stay up to date on current topics specific to the healthcare industry and earn CCB CEUs wherever and whenever it works best for you (one login per registration).

Event dates are subject to change.  
Visit [hcca-info.org/events](https://hcca-info.org/events) to learn more.



# New and updated content for 2025 – keep your program up to date!

New 2025 edition now available!



Our essential resource for healthcare compliance professionals, the *Complete Healthcare Compliance Manual* provides authoritative information and actionable tools for successful compliance program management. Discover the latest expert insights + policy templates, checklists, sample forms, and more!

## Available in three purchasing options



One-year  
online  
subscription



Two-volume  
softcover  
book set



Money-saving  
print + online  
bundle

With content written and designed specifically for use by practicing compliance professionals, the 2025 edition features new articles and updated content throughout the manual, including:

- Enterprise risk management **(new!)**
  - New tool: Example Questions for Department Specific Risk Identification
  - New Tool: 10 Examples of Risk Appetite Statements
- Anti-Kickback Statute
- EKRA
- Evaluation of Corporate Compliance Programs **(new!)**
- Health information management: Compliance and Non-traditional Third Parties **(new!)**

Learn more and purchase  
[hcca-info.org/chcm](https://hcca-info.org/chcm)



*Convenient virtual format!*

# Healthcare Enforcement Compliance Conference

October 29–30, 2025 • Virtual (CT)



CRIMINAL  
ENFORCEMENT



CIVIL  
ENFORCEMENT



OIG UPDATES



CMS OVERSIGHT



FALSE CLAIMS ACT

## Take a proactive approach to enforcement challenges

Offered this year as a two-day virtual event, our annual enforcement conference is designed to equip attendees with the knowledge they need to navigate today's shifting healthcare compliance enforcement landscape.

As a participant, you'll earn live CEUs and learn from experienced attorneys and consultants, compliance professionals, and experts in healthcare law — gaining guidance on:

- Managing enforcement and fraud & abuse compliance challenges
- Responding to investigations, prosecutions, and FCA cases
- Navigating privacy compliance and breach response
- Understanding evolving risks in managed care, clinical research, and behavioral health

Save \$100 when you register by August 20. Group discounts are available for groups of 3 or more: invite your team!

**View the agenda and register**  
[hcca-info.org/2025HECC](https://hcca-info.org/2025HECC)

