



ahia

Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org

Journal of the Association of Healthcare Internal Auditors

Vol. 42, Number 6, 2023

Cybersecurity Awareness

Protect the privacy and security of your data
page 7

Telehealth Claims

Mitigate risks with auditing and monitoring
page 12

Underwriting

Audit a risky health plan activity
page 17

Credit Balances

Satisfy the obligation for refunds
page 22



HEALTHCARE TOP RISKS FOR 2023

2023 Top Risks for Healthcare identified from new survey conducted by Protiviti and North Carolina State's Enterprise Risk Management Initiative

For the complete list of Top Risks for 2023 and 2032 facing the Healthcare Industry, download the results here:

[Protiviti.com/us-en/top-risks-2023-healthcare-insights](https://protiviti.com/us-en/top-risks-2023-healthcare-insights)

protiviti.com

© 2023 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0223

ahia
Assoc. of Healthcare Internal Auditors

protiviti[®]
Global Business Consulting

FROM THE EDITOR Efficiency in Internal Audit.....4

By Mike Fabrizio, CHIAP®, CIA®, CPA

FROM THE CHAIR Gratitude and Recognition.....5

By Christy Decker-Weber, CHIAP®, CIA®, CPA, CFE, CRCR, CRMA, COSO ERM



FEATURE Cybersecurity Awareness.....7

Protect the privacy and security of your data

By Scott Wrobel and Debra Geroux, JD, CHC, CHPC



FEATURE Telehealth Claims.....12

Mitigate risks with auditing and monitoring

By Holly Hester, PT, DPT, CHC, CHPC, and Yolunda Dockett, OTD, MOTR, M.Jur., CHC, CHPC



FEATURE Underwriting.....17

Audit a risky health plan activity

By Megan DeVries, CHIAP®, CIA®



FEATURE Credit Balances.....22

Satisfy the obligation for refunds

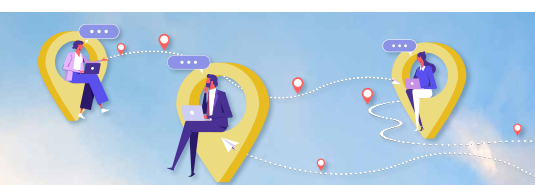
By Symone Rosales, RHIT, CHPS, CHC



CONTROLLED SUBSTANCE SECURITY Make Patient Safety Your Diversion Program Priority.....26

Beware of counter priorities

By Kim New, JD, BSN, RN



FEATURE Remote and Out of State Workers.....28

Audit the tax implications

By Louise Labrie, Mary Torretta, JD, and Hayley Oakes



HEALTHCARE FRAUD Fraud Risk Management.....32

Recognize the need for a formal program

By Brandi Steinberg, CPA, CFE

MEMBER Spotlight

MEMBER SPOTLIGHT Alicia Capps, CIA®, CPA.....35

Chief Audit Executive

Intermountain Healthcare

Efficiency in Internal Audit

By Mike Fabrizio, CHIAP®, CIA®, CPA

Are internal auditors as efficient as they expect others to be?

– Richard Chambers

A well-meaning provocative statement is usually targeted at the open-minded and is meant to challenge conventional thinking, foster self-examination and critical thinking and, more importantly, prompt change where needed. Richard Chambers, a career internal auditor and former president of The Institute of Internal Auditors, should be taken seriously on suggesting improvement opportunities. He speaks from an authoritative and insightful position on internal audit topics.



[His article](#), which uses the quote as its title, says that internal auditors need to continuously examine their service delivery model to look for improvements in efficiency. Objectives that justify consideration include more timely reports and greater internal audit productivity.

New and better methods, tools and resources need to be deployed, such as agile auditing, more technology and the best subject matter expertise. Richard encourages you to work smarter by increasing your focus on the risks that matter most to your stakeholders.

New Perspectives looks to deliver information and resources that advance your efforts to become more efficient. Our authors bring you insightful information that helps you choose meaningful and relevant areas and then conduct efficient audits with the knowledge that their articles provide.

In “Cybersecurity Awareness,” Scott Wrobel and Debra Geroux provide an overview of the current state of cybersecurity threats. They outline how to build a comprehensive cybersecurity program and train your workforce to have the essential preventive activities. Links are provided to resources that the federal government has developed to keep us up to date on current threats and threat actors.

Holly Hester and Yolunda Dockett in “Telehealth Claims,” cover the growth of this very necessary and viable service option for outpatient providers and the need for auditing and monitoring. They disclose the Office of Inspector General’s data mining method to identify indicators of fraud, waste and abuse. The approach can be adopted with data analytics to audit and monitor claims in your organization.

continued on page 6

NEW PERSPECTIVES

Published by AHIA, Inc.

EDITOR:

Michael Fabrizio, CHIAP®, CIA®, CPA
410-707-3274
Mike.Fabrizius@gmail.com

EDITORIAL BOARD:

Robert Michalski, CHIAP®, CHC, CHPC,
CHRC, CCE
Editorial Board Chair
University of Florida Health
Gainesville, FL
RMic0006@shands.ufl.edu

Cavell Alexander, CHIAP®, CPA, CIA, CFE
UCHealth System
Aurora, CO

Robin Cannon, CHIAP®
Wellspring Health
York, PA

Megan DeVries, CHIAP®, CIA®
Corewell Health
Grand Rapids, MI

Samantha M. Frost, CHIAP®, CPA
Ochsner Health System
New Orleans, LA

Alton F. Knight, Jr., CHIAP®, MS, MBA, CHE,
CFSA, CICA, CFE, CCE, CRMA, FACHE, CHC
Capital Blue Cross
Harrisburg, PA

Jennifer Conley, CIA®, CPA, CFE, MBA
AHIA Board Liaison
Salt Lake City, UT

Joanna Rakers, CHIAP®, MBA, CPA
BJC HealthCare
St. Louis, MO

Amy Lee Smith, CHIAP®, CIA®, CPC, CPMA
Bon Secours Mercy Health
Newport News, VA

Jared S. Soileau, PHD, CIA®, CPA, CISA, CCSA
Louisiana State University
Baton Rouge, LA

Scott Thompson, CHIAP®, CHC, CHPC
Catholic Health Initiatives
Birmingham, AL

Joshua Wallner
Stryker
Grand Rapids, MI

Jonathan West, CIA®, CISA
Intermountain Healthcare
Salt Lake City, UT

Gratitude and Recognition

By Christy Decker-Weber, CHIAP®, CIA®, CPA, CFE, CRCR, CRMA, COSO ERM

As I stand at the conclusion of my tenure as Board Chair of our extraordinary organization, my heart is brimming with gratitude and appreciation for the remarkable journey we have collectively embarked upon. Serving as your leader has been an honor and a privilege, one that has been made even more enriching by the unwavering dedication and support of our esteemed members and volunteers.



Throughout my time in this role, I have witnessed the true collaborative spirit and selflessness of our 100-plus dedicated volunteers. They define our organization and provide you, our members, the many deliverables that an AHIA membership entails, and we all appreciate.

Year in review

The passion and tireless efforts of our volunteers have driven the success of numerous initiatives this year. We launched a new and improved AHIA website and achieved a 90 percent renewal rate of our Certified Healthcare Internal Audit Professional® (CHIAP®) credentialed members. We executed on our commitments to our valued Annual Partners in the second year of the program.

We achieved nirvana in Seattle with our 2023 Annual Conference, which was attended by over 400. In-person Chief Audit Executive roundtables were held in conjunction with the Nashville and Southern California regional seminars. Numerous webinars and tech talks were held virtually.

A new affiliation program—the Health Plan Alliance (HPA)—facilitates partnerships on membership and learning opportunities in the payer sector. Engagement with members and others increased on LinkedIn. Gaps were addressed in the Audit Resource Center by mapping additional articles and webinars to the Body of Knowledge. Our editorial efforts resulted in new white papers and six issues of our *New Perspectives* journal.

Our volunteers have demonstrated an unmatched enthusiasm and willingness to contribute their time, skills and expertise. Their selfless contributions have been instrumental in shaping the success of our events, services, partnerships and affiliation efforts, and the value provided to you.

As I pass the baton to my successor, Tammy Rice, I am confident in the bright future that lies ahead for AHIA. The legacy we have cultivated, the relationships we have fostered, and the member value we have provided are the hallmarks of our collective endeavors. I have no doubt that with the continued dedication and commitment of our members and volunteers, the AHIA will scale to even greater heights.

Recognition

Please join me in extending our sincere thanks to our outgoing AHIA Board members: Todd Havens, Jackye Thompson and Jennifer Conley. They have given countless contributions and years of service supporting the mission and vision of the AHIA.

ahia

Assoc. of Healthcare Internal Auditors

2023 BOARD OF DIRECTORS

Chair

Christy Decker-Weber, CHIAP®, CIA®, CPA, CFE, CRCR, CRMA, COSO ERM
Sharp HealthCare
Christy.Decker-Weber@sharp.com

Vice Chair

Tammy Rice, CHIAP®, CIA®, CPA
AvMed, Inc
Tammy.Rice@avmed.org

Secretary/Treasurer

Heather Zundel, CPA, CGMA
Presbyterian Healthcare Services
HeatherZundelcpa2022@gmail.com

Immediate Past Chair

Todd M. Havens, CHIAP®, CIA®, CRMA
Vanderbilt University Medical Center
Todd.Havens@vanderbilt.edu

Directors

Jennifer Conley, CIA®, CPA, CFE
Jenfromwyo@gmail.com

Megan DeVries, CHIAP®, CIA®
Corewell Health
Megan.DeVries@corewellhealth.org

Jerod Holloway, CHIAP®, CIA®, CFE, CHC
KPMG
JerodHolloway@kpmg.com

Renee Jaenicke, CHIAP®, CIA®, CPA, CFE, CHC
Salinas Valley Memorial Healthcare System
R.Jaenicke@svmh.com

Amy Lee Smith, CHIAP®, CIA®, CPC, CPMA
Bon Secours Mercy Health
Amy_Smith@bshsi.org

Mary Thomas, CIA®
Health First Inc
Mary.C.Thomas@hf.org

Jackye Thompson, CHIAP®, CPA, CRMA®
Banner Health
Jackye.Thompson@bannerhealth.com

Executive Director

Erin Erickson
720-881-6118
EErickson@ahia.org

Gratitude and Recognition

continued from page 5

Todd has been a long-time AHIA board member, having served an initial three-year term as a Board Member and a subsequent four-year term as a Board officer.

Jackye spent her first year as the Board Liaison for the Professional Practices Committee and her subsequent two years as the Board Liaison for our Annual Conference Committee, which delivered in-person events in Miami (2022) and Seattle (2023).

Jennifer has served as our Board Liaison for the Publications Committee for three years, supporting the issuance of valuable resource materials, such as the *New Perspectives* journal, whitepapers and eNews.

Many thanks to all three of you for your steadfast dedication, guidance, mentorship, support, and many contributions to the continued success of the AHIA! I also want to extend an enormous amount of appreciation and kudos to my fellow Board Members and all of AHIA's dedicated volunteers for doing what you always do, meeting the needs of our members.

A warm welcome goes to our newly elected Board members. Cally Cass from Peace Health is joining as your

2023 AHIA Treasurer and Secretary, which begins her four-year term in the Board executive track. Darryl Rhames from University Health and Kelly Rollins from Ochsner Health are joining as Board Members At Large for three-year terms.

As you can clearly see, your volunteer-led Board and committees, with support from Kellen staff, have been working hard throughout the year. I extend my deepest gratitude to each one of you for being a part of this incredible journey. Your passion, dedication and support have left an indelible mark on my heart, and I am proud to have been in your esteemed company.

We all have a lot to be proud of and could not be more excited to see what 2024 holds for us. As Chair of the Nominating Committee in 2024, I look forward to bringing you another well-qualified slate of Board candidates to continue advancing our organization and supporting the future success of the healthcare internal audit profession.

Thank you once again for allowing me the privilege of serving as your Board Chair of our incredibly special and valuable organization. **NP**

Efficiency in Internal Audit

continued from page 4

Kim New, our Controlled Substance Security columnist, continues to deliver important subject matter information in her column. In "Make Patient Safety Your Diversion Program Priority," she explains how contrary influence by those who turn a blind eye to diversion can supersede the patient safety objective.

Let me know what you like about this issue and how *New Perspectives* can be improved. We want to continuously examine our service delivery model by pursuing improvements in efficiency that benefit you. You can reach me at Mike.Fabrizius@gmail.com and 410-707-3274. **NP**

About *New Perspectives*

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

NP is published in an electronic format in February, April, June, August, October and December. Issues are accessed by online viewing or through download. See the *NP* archives at <https://ahia.org/new-perspectives-archive/> (login required).

For author guidelines or to submit an article, please contact Mike Fabrizio at 410-707-3274 or Mike.Fabrizius@gmail.com.

Yearly subscription rates, including postage, are \$100, payable in U.S. funds. No refunds or cancellations. Send publication and subscription inquiries, address changes and other inquiries to: Association of Healthcare Internal Auditors, Inc., 111 West Jackson Blvd, Suite 1412, Chicago, IL 60604 USA. Phone 303-327-7546 or email, ahia@ahia.org.

New Perspectives, its editors and the Association of Healthcare Internal Auditors, Inc. are not responsible for the opinions and statements of its contributors and advertisers. The authors do not necessarily reflect the official policies of AHIA nor does AHIA endorse any products. AHIA does not attest to the originality of the author's content. Reprints of any portion of *New Perspectives* may be used for educational or instructional purposes only, provided the following statement appears on each reprint: "Reprinted with permission from *New Perspectives*, Journal of the Association of Healthcare Internal Auditors, Inc. Volume/Number." Copyright 2023, Association of Healthcare Internal Auditors, Inc.

Cybersecurity Awareness

Protect the privacy and security of your data

By Scott Wrobel and Debra Geroux, JD, CHC. CHPC

Celebrating the 20th year anniversary of October as National Cybersecurity Awareness Month, the [Cybersecurity & Infrastructure Security Agency \(CISA\)](#) announced a new enduring cybersecurity awareness program, [Secure Our World](#). However, for the healthcare industry and its internal auditors, every day should focus on cybersecurity. Cybersecurity risks to your organization's operations and compliance and to your patients and their safety and privacy are real.

The federal government, through collaborative efforts of its various agencies, continues to follow threat actors and cybersecurity incidents. The agencies provide guidance to healthcare leaders and internal audit professionals on what they can do to avoid being the next big data breach.

Beginning October 28, 2020, a [joint cybersecurity alert](#) ("2020 Joint Alert") was issued by CISA, the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), and other federal agencies. Since then, they have provided additional joint alerts, public service announcements (PSAs), advisories and other guidance.

The communications warn of various cyberthreats and threat actors. This article provides further insight into who these threat actors are, how they are attacking the healthcare industry, and what you and your organization can do to mitigate the risks of a cyberattack.¹

Privacy as an element of security

In addition to remaining vigilant for cybersecurity threats of all types, healthcare entities should also be familiar with their obligation to protect their patients' healthcare information, thanks in large part to the Health Insurance Portability Act of 1996 (HIPAA). Also, HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its related regulations that include the HIPAA Privacy, Security and Breach Notification Rules.

The Act and its regulations are collectively referred to herein as *HIPAA*.²

Often overlooked are other laws and regulations that affect healthcare entities and the information that they maintain. For instance, every state in the U.S. has some level of data privacy legislation that is implicated when an individual's personal data is affected by a cyberattack.

In recent years, many states have strengthened the protections afforded personal information through comprehensive privacy laws, starting in 2018 with the [California Consumer Privacy Act of 2018 \(CCPA\)](#), as amended by the [California Privacy Rights Act of 2020 \(CPRA\)](#). To date, 11 additional states have enacted comprehensive privacy laws protecting personal information, including health information, with effective dates ranging from January 1, 2020 to July 1, 2026.³

Another state—Washington—has broadened the protection afforded consumer health data collected by entities that conduct business in the state that is not otherwise covered by HIPAA through the enactment of the [My Health My Data Act](#). Adding to the burden are the various federal laws and regulations that have been enacted to address the growing cybersecurity attacks on critical industries and public entities.

¹While the laws and regulations discussed in this article are focused on their application in the healthcare industry, many of the state and federal laws and regulations are applicable to a multitude of industries.

²45 CFR Parts 160 and 164, Subparts A, C, D and E.

³In addition to California, the following states have enacted comprehensive privacy laws: Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah and Virginia. See <https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/> for more detail.



Patients are increasingly suing healthcare organizations over data breaches.

Taking proactive measures to avoid a cyberattack will inevitably lessen a healthcare entity's anxiety over having to notify government regulators and avoid the costly expenses of mitigation, remediation and notification. Also, proactive measures can help avoid the costs associated with lawsuits that have been increasing in frequency over the years.

Cyberattacks by the numbers

This year was one of unprecedented cybersecurity incidents. Media accounts of significant cyberattacks have been on the rise, affecting a broad range of industries, including financial, legal, manufacturing, education, governmental and healthcare. These industries have been attacked because they have information that threat actors desire—such as patient data, financial information and proprietary information—that can be leveraged to carry out extortion campaigns.

The healthcare industry, which is largely based on digital platforms, unsurprisingly remains among the top industries that cybercriminals continue to target. According to the [FBI's 2022 Internet Crime Report](#), cybercrime losses were in excess of \$10.2 billion for 2022, nearly doubling the total losses reported in 2021, which does not take into consideration the cybercrimes that are not reported to the FBI.

In its [Cost of a Breach Report 2023](#), IBM shows that the average cost associated with a breach for healthcare entities is \$10.93 million, an increase of 53.3 percent from 2020. However, other factors, such as the size of the breach (records affected), can drastically increase the costs of breach response. For example, IBM reports that the 2023 global average data breach cost across all industries is \$4.35 million, although the costs associated with a “mega breach” (breaches involving 1 million to 60 million individuals) fell in all categories, ranging between a 3.8 percent decrease to a 26.5 percent decrease.

Why are cybersecurity incidents rising?

A number of reasons exist for the increase in cybersecurity incidents. Since the Covid-19 pandemic, remote work has increased, resulting in greater vulnerability to cyber incidents. According to a 2021 [global industry study commissioned by Tenable, Inc.](#), 74 percent of the organizations surveyed attributed at least one cyberattack to vulnerabilities in systems implemented during the Covid-19 pandemic, including:

- The lack of security visibility into remote workers' home networks
- Migration of business operations to the cloud

Similarly, the Ponemon Institute conducted an [October 2020 study](#) related to the risks of cybersecurity attacks due to increased remote work. The study revealed a significant reduction in the effectiveness of organizations' information technology (IT) security posture due to Covid-19, falling from 71 percent effectiveness pre-Covid to 44 percent due to Covid-related vulnerabilities.

In addition to the increased vulnerabilities—and increased accessibility for cybercriminals—the evolution of cybercriminals and the tactics they employ is also leading to the increase in cyberattacks. In the past, extortion was the primary tactic, and that is still the case.

The increased sophistication of cybercriminals means their effect is also elevated. In its [2020 Annual Report to Congress on Breaches of Unsecured Protected Health Information](#), the U.S. Department of Health and Human Services, Office of Civil Rights (HHS) reported a total of 656 large breach reports (those affecting 500 or more individuals) affecting over 37.6 million individuals.

As of July 31, 2023, HHS received 437 large breach reports, with the top three affecting nearly 26 million individuals. These three entities include a:

- Hospital system affecting over [11.2 million individuals](#)
- Pharmacy services provider affecting over [5.8 million individuals](#)
- Dental benefits administrator for state agencies and managed care organizations affecting more than [8.8 million individuals](#)

Further review of the reported large breaches clearly indicates that hospitals and other healthcare providers are not the only ones vulnerable to an attack. Indeed, HIPAA breaches have been reported by state and federal agencies, including the [Colorado Department of Health Care Policy & Financing](#) (DHCPF) and the [Centers for Medicare and Medicaid Services](#) (CMS).

Many of these incidents, including the Colorado DHCPF and a breach reported by CMS, were the result of a global cybersecurity incident affecting [Progress Software Corporation's MOVEit](#) file transfer program. The threat actor CLOP Ransomware Gang, a ransomware group known for using [zero-day vulnerability](#) campaigns, was able to [exploit MOVEit software vulnerabilities](#) in May 2023.

According to [KonBriefing Research](#), as of December 1, 2023, the MOVEit Transfer cyber incident has affected 2,591 organizations worldwide and between 77.7 - 82.5 million individuals. Given the widespread use of the MOVEit Transfer software, only time will tell the reach of the MOVEit cyber incident.

The reported incidents here are not isolated. As various government agencies warn, cyberthreats to the healthcare industry are a reality and will continue in the future.

The threat actors and how they gain access

Ransomware continues to be big business. [Ransomware as a service](#) (RaaS) has become a new business model for threat actors who create ransomware variants that increase the ease with which an individual can deploy an attack. The ransomware is packaged and ready for attack.

While the variations in ransomware are continuously changing, the underlying concepts remain constant, with BlackCat, Black Basta, Royal and Lockbit 3.0 topping the [list of threat actors](#). As of the second quarter of 2023, these four accounted for nearly 50 percent of the market share. And, despite [statements by certain ransomware operators](#)

that they would not be launching ransomware attacks on hospitals during the Covid pandemic, the threats continued and are still very much alive as evidenced by the incidents discussed above.

Measures to prevent an incident

With cyberattacks not diminishing, industries—and more notably, the healthcare industry—need to step up their efforts to be proactive. Knowing who the threat actors are and how they are attacking can greatly assist in avoiding these threats. Generally speaking, cyberattack deployment can be categorized into three specific vulnerabilities: human error, malicious attacks and system glitches, with malicious attacks leading the pack by more than 50 percent.

Knowing who the threat actors are and how they gain access is critical to reducing the vulnerabilities that can be leveraged to steal sensitive, protected and/or valuable information. Resources are available to keep abreast of these threats and how to avoid them.

CISA has developed various free resources and tools (see the sidebar on page 11) to assist in your cybersecurity efforts, including technical assistance, exercises, assessments and training resources. The topics include Indicators of Compromise, for example for [LockBit 2.0 ransomware](#), that provide mitigations for specific threat actors that can be used to ensure the security of their IT environment. The predominant risk areas that must be addressed are device security, cloud security and human errors.

Device security

Healthcare providers need to be cognizant at all times of the data that may be available on or accessible from devices, including diagnostic and other medical devices, and secure them accordingly. Knowing what data you have and where it is maintained is the first step in the analysis.

You must ask yourself what a threat actor could glean if they gained access to or overtook proprietary diagnostic tools. For example, would threat actors be able to extract firmware and source code information, then sell it to competitors? Or more problematic, if threat actors could leverage control over devices, could they interfere with the proper functioning of the device?

The average cost associated with a breach for healthcare entities is \$10.93 million.

Remote work has increased, resulting in greater vulnerability to cyber incidents.

Your inquiries about device insecurities are significant, as they can lead not only to financial damages, they also pose significant risks to patient health. All systems that can access devices containing information about patients and/or proprietary technology should be protected with multifactor authentication, and they should have both location tracking and remote wiping enabled. Your IT management team can be engaged to assist with these solutions.

Cloud security

Healthcare providers are increasingly using cloud storage for data, including for electronic medical records. While storing data in the cloud is convenient and cost effective, the data also needs to be secured. No sensitive information should be accessible without multifactor authentication.

Additionally, since these cloud vendors are [business associates](#)—an often-overlooked concept—you need to ensure that they are compliant with applicable privacy and security laws, including HIPAA and similar state laws, at all times.

Breaches of cloud and other electronic services providers, particularly Office 365 email accounts, are on the rise, as evidenced by the MOVEit global incident. Consequently, IT management teams must continually address security protocols used. Examples include:

- Multifactor authentication that requires users to have a second device to authenticate their identity
- Geoblocking enabled to stop any access from specific foreign countries
- Strong password policies to reduce the chances of compromise

The changes can be made at the organizational level to help mitigate the third and most dangerous vulnerability—human error.

Human error

With even the most effective security protocols in place, human error continues to negate an organization's best efforts. Phishing campaigns are still prevalent—where threat actors obtain information from a target that can be used to perpetrate some type of future scam. Phishing campaigns

typically occur not only through email, but also through phone calls (vishing) or text messages (smishing).

Newer campaigns, such as malvertising—malware in online advertisements—are adding to the threat actors' capabilities of breaching an organization's security. The threat actors are using more sophisticated efforts that utilize targeted emails (spear phishing). The content of the emails is based upon data found on the dark web that they use to develop an attack plan and perform targeted and more effective attacks. Understanding how spear phishing and other campaigns work is key to learning how to avoid them.

More and more, employees are using their business email addresses in connection with their personal accounts on social media sites that have had data breaches (e.g., Evite, LinkedIn, Dropbox). Once compromised, that information goes up for sale on the dark web. Threat actors are utilizing the information they find on the dark web about these accounts to spear phish employees' corporate email accounts.

A spear phishing attack is launched when an employee clicks on a spear phishing email that appears to be from a known sender or organization. According to [Symantec's 2019 Internet Security Threat Report](#), spear phishing attacks are the most prevalent infection vector, representing 65 percent of the known groups carrying out cyberattacks.

The heightened effectiveness of spear phishing is due in large part to the sophistication of the email, which often include personal details that the recipient would not expect a threat actor to know. The threat actor is able to obtain access to the recipient's account when he or she clicks on a link or opens an attachment in the email, thereby launching the attack.

Once in, the virus quickly downloads all of the recipient's email searching for other victims and sends out an email to the recipient's contacts purporting to be from the recipient and spreading the link to a malicious website. Often, the threat actor stays inside the recipient's account to catch responses to the sent emails. For example, the email string may read:

- Recipient: "Is this email really from you?"
- Hacker: "Yes, it is, you can click on the link."

Once the victim clicks the link, the whole process begins again in a new recipient's account.

Similar phishing campaigns have included emails containing invoices that appear to come from an executive within an organization asking for payment(s). Not knowing the invoice to be from a threat actor, the recipient pays the invoice directly to the threat actor's untraceable account. Still another popular phishing campaign involves stealing usernames and passwords, known as credential phishing. In these campaigns, the attacks can be from spear phishing or may be the result of a [business email compromise](#).

The best way to combat any phishing attempt is to be vigilant against the known threats. Training is critical to avoiding a cyberattack. While knowing what the threats are is important, training on how to spot and avoid malicious emails should be done on a regular basis. Other proactive measures should include establishing strong policies about the use of corporate email addresses and accounts, informing users of the potential dangers of clicking on and engaging with content from unknown sources and known sources whose requests are inconsistent with standard procedure.

Likewise, employees should have a well-established protocol to follow regarding reporting potential threats to management and IT. Periodic training exercises are a simple way to ensure the workforce is aware of and can recognize threats. The use of table-top exercises and simulated phishing emails will enable management and IT to see how employees are reacting to potentially malicious/spoofed emails and alert them to any additional training employees may need.

Conclusion

Cybercriminals are not going away any time soon. Instead, they are only growing in their sophistication. Healthcare providers must remain vigilant in their efforts to avoid becoming the next victim.

Build a comprehensive cybersecurity program and appropriately train your workforce to have the essential preventive activities. Use the tools and resources that the federal government has developed to keep IT administrators up to date on the current threats and threat actors. Build

Resources

- CISA
 - [Official Alerts and Statements](#)
 - [Free Cybersecurity Resources and Tools](#)
 - [Resources against Ransomware](#)
- FBI – [Official Alerts and Statements](#)

relevant policies and review them regularly. Join lists from trusted sites, such as CISA and the FBI, to assist your organization in keeping abreast of the current landscape of cybersecurity.

While many attacks can be prevented with diligent IT management, such as patches in software and strong encryption practices, no patch exists for human error. You can only prevent human errors through regular training of your workforce. Maintain cybersecurity checklists and incident response plans to assist your organization in mitigating its risk and addressing an incident should it fall victim despite its best efforts. **NP**



Scott Wrobel is a co-founder of N1 Discovery and has accumulated over 20 years of experience implementing technology solutions for clients facing a wide variety of situations. He specializes in complex technology investigations and data breaches, including high-profile digital forensic investigations involving theft of intellectual property, fraud, child exploitation and white-collar crimes. Scott can be reached at Scott.Wrobel@n1discovery.com.



Debra Geroux, JD, CHC, CHPC, is a Shareholder and a Co-Chair of Butzel Long's Health Care Industry Team and member of the firm's Cybersecurity and Privacy Specialty Team, Government & Internal Investigations Team, and Litigation and Dispute Resolution Team. She can be reached at Geroux@butzel.com.

Telehealth Claims

Mitigate risks with auditing and monitoring

By Holly Hester, PT, DPT, CHC, CHPC, and Yolunda Dockett, OTD, MOTR, M.Jur., CHC, CHPC

With the onset of the Covid-19 public health emergency, telehealth quickly became a very necessary and viable service option for outpatient providers. The urgent need for the service necessitated a quick implementation, with no time for a thorough risk analysis or refining auditing and monitoring procedures. Now, you should make your assessment of your telehealth claims a priority.

The healthcare industry has identified several risks specific to telehealth billing that necessitate implementation and/or revisions to current auditing and monitoring plans. Three key risks areas that should be incorporated into your auditing and monitoring plan are:

- Licensure and scope of practice
- Billing, coding and documentation
- Quality of care

Licensure and scope of practice

Regardless of provider type—physician, nurse practitioner (NP), physician assistant (PA), physical therapist (PT), occupational therapist (OT), speech-language pathologist (SLP), etc.—start your assessment with licensure. Ensure eligibility to provide services to patients. Providers must hold an active and unencumbered license in the state in which they practice and generally in the state in which the patient is located.

Some states have specific exceptions that allow an out-of-state provider to provide services via telehealth in a state in which they are not located/licensed. Others make allowances for practicing in neighboring states or in certain situations where a temporary license may be issued.

Many states have adopted interstate compacts that allow providers to practice in states where they are not licensed, provided they hold a license in good standing in their home state. Compact examples include the:

- [Interstate Medical Licensure Compact](#)
- [Physical Therapy Compact](#)
- [Audiology and Speech-Language Pathology Interstate Compact](#)

To participate in an interstate compact, providers must meet specific requirements and apply (and pay) for compact privileges in much the same way as they would apply for licensure via reciprocity.

Each state's provider-specific practice act or administrative rules must be carefully reviewed for any requirements or regulations pertaining to telehealth or the delivery of services using technology, including requirements for supervision of nonphysician practitioners and/or supportive personnel. States differ in how they define the terms *telehealth* or *telemedicine* and may or may not specifically address telehealth regulations for specific provider types.

For example, the [Ohio Administrative Code](#) clearly defines *telehealth services* and specifies the healthcare professionals who may deliver telehealth within Ohio. The regulations go on to differentiate between synchronous and asynchronous communication technology, clarify documentation requirements, and outline expectations for emergency situations.

Stay abreast of state laws and licensure requirements for the states in which you do business:

Services delivered by unlicensed personnel do not meet billing requirements for payment.



- Subscribe to email updates from state licensing boards.
- Check the resources available from the [Center for Connected Health Policy](#) at least quarterly.
- Review state regulations carefully when expanding operations into new states or when adding new services or licensed professionals.

Perhaps the biggest and most immediate risk associated with licensure is rendering and billing for treatment without a license. Services delivered by unlicensed personnel do not meet technical billing requirements for payment. Healthcare professionals who practice without a license are also subject to liability and malpractice claims, permanent loss of licensure, and exclusion from participation in federal healthcare programs.

From a risk mitigation perspective, licensure should be confirmed upon hire via primary source verification to ensure the individual's license is active and in good standing. Licensure status should be checked at least annually and upon renewal. Include language in your organization's code of conduct that requires licensed employees to immediately notify human resources or the compliance officer of any issues or infractions against their license. Then issues and infractions can be fully vetted and addressed.

Your auditing and monitoring plan should include activities such as:

- To avoid any gaps, run a report monthly to see which providers are coming up for renewal.
- Ensure all employees review and acknowledge the code of conduct and relevant policies and procedures upon hire and annually.

Billing, coding and documentation **Leverage resources**

Use resources such as federal and state regulations, regulatory updates, enforcement trends, payer policies, and utilization data to identify telehealth billing, coding and documentation risks. The resources should be reviewed routinely for telehealth updates to guide the risk identification process.

The Office of the Inspector General (OIG) Work Plan offers insight into its telehealth focus areas. For example, as a [2023](#)

[Work Plan](#) action, the OIG announced an initiative to assess services such as evaluation and management telehealth visits to determine if the billed services meet Medicare requirements. OIG enforcement updates often highlight billing and coding noncompliance identified through audits, self-disclosures and qui-tam allegations.

Centers for Medicare and Medicaid (CMS) payment policies directly influence those established by private payers. So, reviewing the [CMS Benefit Policy Manual](#) is often the first step in defining medical necessity requirements. However, you should also be familiar with private payer policies as differences may exist in how medical necessity is defined.

Additionally, Medicare Administrative Contractor (MAC) guidelines should be reviewed. Review guidelines across multiple MACs to gain insight into both regional and national trends or focus areas. MACs provide both local coverage determinations and Targeted Probe and Educate resources (TPE) on their website. TPE findings offer insight into modifier, ICD-10, CPT, and place of service (POS) risks in both inpatient and outpatient settings. For example, a review of established outpatient office visits performed by [Novitas](#) identified that insufficient documentation to support billed claims was a major contributor to denials or partial denials.

Similar to CMS and MACs, private payers have established payment policies and offer billing and coding utilization trends to contracted providers. Remain abreast of all active private payer contracts and telehealth payment policies for routine risk identification. Utilization trend data provides professionals with their specific billing and coding trends compared to similar providers in their network.

Audit and monitor

Audit and monitor the following areas to mitigate telehealth billing, coding, and documentation risks:

- ICD-10 and CPT codes
- POS codes and modifiers
- Incident-to services

ICD-10 and CPT codes are the primary way of demonstrating medical necessity to a respective payer on submitted

claims by providing a general summary of the condition of the patient and the treatment provided. You must ensure the accuracy of these codes on all claims, including telehealth. Similar to ICD-10 and CPT codes, use of POS codes and modifiers provide further insight into treatment details. Payers often require healthcare providers to append the applicable modifier and/or POS code to identify professional telehealth service claims.

Telehealth auditing and monitoring activities to mitigate ICD-10, CPT and POS coding risks include:

- Routine telehealth utilization reviews using available

billing reports to analyze trends, and identify coding patterns and outliers.

- Medical necessity documentation audits to verify the accuracy of billed and documented telehealth visits. The frequency of these audits will depend on the monitoring results and may occur either proactively or retrospectively.

OIG billing risk indicators

The OIG developed seven measures that focus on different types of billing risk for telehealth that may indicate fraud, waste or abuse. Exhibit 1 summarizes the measures with

Exhibit 1 – OIG indicators of fraud, waste or abuse¹

Billing indicator	Threshold	Comments
Telehealth services billed at the highest, most expensive level for a high proportion of services	Providers who billed 100 percent of their telehealth services at the highest level in any service category	100 percent is a conservative threshold. To select a different threshold, review measures of central tendency (e.g., mean and median) and the distribution, including outliers in the data.
A high average number of hours of telehealth services billed per visit	A conservative threshold is providers who billed for an average of more than two hours of telehealth services per visit.	The median is 21 minutes of telehealth services per visit for all providers who billed Medicare.
Telehealth services billed for a high number of days in a year	A provider who billed telehealth services for more than 300 days in the year	The median is 26 days of the year for all providers who billed Medicare for telehealth services.
Telehealth services billed for a high number of patients	A provider who billed telehealth services for 2,000 or more beneficiaries in a year	The median is 21 beneficiaries for all providers who billed Medicare for telehealth services. The threshold can be changed to fit different needs and data.
Multiple plans or programs billed for the same telehealth service for a high proportion of services	A provider who billed both Medicare fee-for-service and a Medicare Advantage plan for the same service for more than 20 percent of their services	In the OIG analysis, most providers never billed this way.
Telehealth service billed and then medical equipment ordered for a high percentage of patients	Providers who billed for telehealth services for at least 50 beneficiaries	The median is three percent of Medicare beneficiaries.
Both a telehealth service and a facility fee billed for most visits	A provider with telehealth visits that include both a telehealth service and a procedure code for an originating site facility fee (Q3014) for the same beneficiary	In the OIG analysis, most providers never billed this way.

¹<https://oig.hhs.gov/oei/reports/OEI-02-20-00723.pdf>, beginning on page 10.

The OIG provides a toolkit for analyzing telehealth claims to identify billing risks.

the OIG threshold for further attention. You can apply data analytics to your reimbursement claims to identify charges that exceed your chosen thresholds and require further review.

Incident-to

Another important area to audit and monitor for medical necessity is incident-to services. The incident-to delivery model is quite popular in the outpatient setting and is often omitted from compliance work plans. *Incident-to* a physician's professional services means the services are furnished as an integral, yet incidental, part of the physician's professional services in the course of diagnosis or treatment of an injury or illness.²

The services must relate to an existing course of treatment and do not apply to new patients, or to existing patients for a new illness or injury. Unlike ICD-10 and CPT coding, this treatment approach is not easily tracked or readily available in standard reports.

You should monitor incident-to telehealth utilization through available or custom reporting and perform routine telehealth documentation audits for your nonphysician practitioners, such as PAs, OTs and NPs. The audits should verify that incident-to requirements were met and validate the medical necessity of the visits.

Quality of care

Regardless of the specific type of services delivered via telehealth, the level of care must be the same as if the service was rendered in person. Ensuring both provider competency and patient appropriateness is inherent to effective service delivery and quality of care.

Provider competency starts with training on your telehealth technology platform, state and/or payer requirements for obtaining informed consent, best practices for care delivery (e.g., private room or office, eye contact, appropriate lighting), applicable services, regulatory and payer requirements, and emergency preparedness. Patient appropriateness encompasses not only the patient's clinical or medical condition(s) but also the patient's demographics and any potential associated barriers, such as language and/or communication, cultural and environmental

considerations, and access to and competence with technology.

Auditing and monitoring for provider competency and patient appropriateness can be challenging. Suggested areas to monitor and track include:

- Competency checklists
- Clinical outcomes
- Patient satisfaction
- Incident trends

Competency checklists should be created for provider- and clinic-specific telehealth processes and policies that are taught and assessed as part of your organization's training or onboarding program. Monitoring that these checklists are complete and current is an important step.

Monitoring trends in clinical outcomes and patient satisfaction for patients receiving telehealth and those receiving in-person visits helps to identify outliers—both patients and providers. Monitoring also ensures that the standard of care is not compromised when providing services using technology.

Resources

- Centers for Medicare and Medicaid – [Telehealth](#)
- Center for Connected Health Policy – [Policy Resource Center](#)
- HHS Office of Inspector General –
 - [Telehealth](#)
 - [Toolkit: Analyzing Telehealth Claims to Assess Program Integrity Risks](#)

Tracking incident trends specific to telehealth may help identify opportunities to modify or revise emergency preparedness plans and give insight into telehealth appropriateness for a specific patient population or demographic. Incident frequency and type can also point to potential issues or challenges with provider competency and expertise.

Conclusion

Telehealth will remain a valuable treatment option for

²<https://oig.hhs.gov/oei/reports/OEI-02-20-00723.pdf>, page 9.

outpatient providers, and it presents both existing and new risks to healthcare organizations. As healthcare providers continue to use this approach to patient care, compliance

and audit professionals are encouraged to incorporate telehealth into their current auditing and monitoring work plans to mitigate risks. **NP**



Holly Hester, PT, DPT, CHC, CHPC, is the Senior Director of Strategic Client Partnerships at Net Health. Holly can be reached at Holly.Hester@nethealth.com and 412-515-8596.



Yolunda Dockett, OTD, MOTR, M.Jur., CHC, CHPC, is the Chief Compliance Officer at Anne Arundel Dermatology. Yolunda can be reached at YDockett@aadermatology.com and 571-839-1352.

*Truth is proper and beautiful in all times and in all places.
- Frederick Douglass*

Thinking about your business is a big part of ours.

PUT OUR HEALTH CARE INSIGHTS TO WORK FOR YOU.

Experience the power of being understood. Experience RSM.

rsmus.com/healthcare

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

RSM US LLP is the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

HEALTHCARE & LIFE SCIENCES

Advancing Innovation and Improving Outcomes During Moments of Incredible Change and Disruption

Comprehensive tailored solutions to thrive in today's complex healthcare environment backed by a global team of experts and advisors at your side.

- | Compliance | Billing & Coding Audit
- | Clinical Research & Life Sciences
- | Privacy & Cybersecurity | Real Estate
- | Investigations | Fair Market Value
- | Strategy & Performance

Learn more at ankura.com

ankura | PROTECT, CREATE, AND RECOVER VALUE

Underwriting

Audit a risky health plan activity

By Megan DeVries, CHIAP®, CIA®

If you work for or in an organization with a health plan, consider how many premium rates are determined as a result of the underwriting process. Underwriting determines the price of coverage, which is critical to revenue. Underwriting should help your health plan grow and achieve acceptable operating margins through fiscally responsible rate setting. Ensure that your health plan has an effective underwriting process.

Health plans often have multiple lines of business that include commercial, Medicare and Medicaid. Commercial plans are offered to employer groups and individuals.

When an employer group requests a quote for health insurance coverage, a health plan conducts underwriting to assess the application. The process determines whether to offer coverage, at what per member per month rate and with what exclusions or limits.

Rates for individual plans are set at a plan level and do not change based on the health status of individual enrollees. Similarly, Medicare and Medicaid rates are set by regulatory bodies such as the Centers for Medicare and Medicaid or individual states.

If you are planning to do an audit of the underwriting process, this article will provide you with some risks to consider during planning, and insight into applicable mitigating controls.

Objectives and risks

Underwriting is a risky activity. Most health plans have goals to grow membership while also maintaining a positive operating margin. If rates determined through the underwriting process are set too high, the organization is at risk of losing business. If rates are set too low, the plan is at risk of losing money because the amount of premiums cannot cover the cost of claims.

To help ensure a balance, the underwriting function will typically develop guidelines that should align with your

health plan's strategies and objectives. You can add value by reviewing the underwriting process, controls and technology in place to ensure premium rates are generated in accordance with organizational objectives and guidelines.

Plan development

During planning, in addition to the underwriting team, you will want to meet with staff in actuary, sales and information technology (IT) teams.

Actuary – Actuary is responsible for developing pricing factors with consideration to strategic business objectives. Pricing factors are filed with the state regulators and used during the underwriting process. Here are some questions you should consider:

- How frequently are rating factors filed?
- What are the deadlines for filing the rating factors?
- Once the rating factors are approved by the state regulators, how are they provided to Underwriting? Are they uploaded into a system, placed on a network drive or emailed?

Sales – Sales is the team that interacts with the employer group throughout the quoting process. They are responsible for obtaining information from the employer group and passing it on to Underwriting. Consider asking these questions:

- What type of information is obtained from the employer group?
- What turnaround times are communicated to the employer group when information is obtained?
- How is the information provided to Underwriting? Is the

Ensure premium rates are generated in accordance with organizational guidelines.



information uploaded into a software system, placed on a network drive or emailed?

- If a system is used, what type of access does Sales have? What types of activities can Sales perform in the system?

Underwriting – Consider asking these questions of Underwriting:

1. What is the process for underwriting a prospective employer group?
2. What is the expected turnaround time for producing quotes for prospective groups?
3. How does the process differ when quoting a renewing group?
4. How soon in advance of a group’s renewal date do you produce a new quote?
5. What systems or tools are used to produce the quote?
6. If a system is used, what type of access do underwriters have? What types of activities do underwriters perform?

If Underwriting uses a software application to support the underwriting process, you should engage IT early. Several complex calculations and factors usually exist that determine the rate. An application that is not working properly could produce an inaccurate rate. During planning, consider asking these questions:

1. How are changes to the system identified?
2. Are changes tested and approved before being moved into production? If so, by whom?
3. How is access to the system managed? Who approves access and who administers access?

4. Is user access reviewed periodically? If so, how frequently is the review performed and who performs the review?
5. What password settings does the system have?
6. Is system data regularly backed up?

If your underwriting team uses a different tool, such as spreadsheets, most of the previous questions would still apply. However, you may need to ask the questions of someone in the area that maintains or manages the spreadsheet template.

When you are determining your audit testing period, you will want to consider the most common effective or renewal dates of your health plan’s employer groups. Knowing this will help ensure your audit testing period includes the time period when the volume of quotes, both for prospective and renewing applications, is the highest. And consider that quotes, especially those produced for prospective groups, could be generated months in advance of their effective date.

Risks and controls

If the scope of your audit starts with rates being filed with the state by Actuary and end when the employer group’s quote is finalized, consider the following risks and controls.

Rating factors

Actuary generates rating factors that are used during the underwriting process. Rating factors are required to be filed with the state regulators before Underwriting can use them. Exhibit 1 summarizes the risks and potential controls of rating factors.

Exhibit 1 – Risks and controls for rating factors

Risks	Potential controls
Rating factors do not align with the organization’s strategic or financial direction.	Rating factors are approved by an appropriate individual prior to being filed with the state regulator.
Rating factors are not filed with the state regulators timely.	Filing deadlines are documented within policies and procedures.

Accuracy of quotes

Prospective employer groups – Sales obtains information such as historical premium rates and experience for existing coverage and prospective member information such as employee’s birth, sex and coverage status (single, double, family, etc.). The information is provided to Underwriting for use in producing a quote. Sales presents the quote to the employer group and relays changes or additional requests back to Underwriting. If the employer group accepts the quote, Sales works with the group to get the quote finalized.

Renewing groups – Underwriting will identify employer groups with upcoming renewal dates and use the past year’s claims and member data to produce a quote. Sales will provide the quote to the group for consideration. If the group requests a plan change, Sales will relay this information back to Underwriting for production of a new quote.

Some plans will have a process referred to as passive renewal. If the employer group does not respond to the renewing quote, Sales will assume the group accepted the renewal rate and extend their effective date.

Pricing exceptions – At times, Underwriting may choose to make an exception to the underwriting guidelines or offer rate relief (lower the rate) in an attempt to sell or keep an existing employer group. They could decide to take on the additional risk of losing money to support a strategic decision to grow membership in a particular area, gain a large well-known group, or gain market share by acquiring a group from a competitor.

Nonstandard pricing – Some groups will submit a non-standard request, or something that does not have an approved rating factor. In these cases, Actuary is required to file the new factor with the state regulator before the nonstandard request can be agreed to. If your health plan has nonstandard requests, you should get information on the volume of requests before you proceed with testing. If the volume of requests is low, you may not consider that testing is worthwhile.

Exhibit 2 summarizes the risks and controls for the accuracy of quotes.

Exhibit 2 – Risks and controls for quote accuracy

Risks	Potential controls
Approved rating factors used during the underwriting process are incomplete or inaccurate.	Rating factors loaded into the system (or other tool used) are tested for completeness and accuracy prior to being used in the underwriting process.
Employer group and member data used for quoting are incomplete or inaccurate.	Any system used is configured to require certain data elements before a quote can be produced. If using another tool, such as spreadsheets, policies, procedures or underwriting guidelines may define the data elements required to produce a quote.
Quotes do not align with your organization’s strategic or financial direction.	Employer group quotes are tracked against budget to ensure Underwriting meets their financial goals.
Pricing exceptions, including rate relief, are inappropriate or not authorized per underwriting guidelines.	Quotes are reviewed and approved by an appropriate individual prior to being released to the employer group.
Nonstandard requests are priced inaccurately or not authorized.	Nonstandard quotes are priced and approved by Actuary prior to being used by Underwriting.

Underwriting determines whether to offer coverage, at what rate and with what exclusions or limits.

Quoting timeliness – During planning, you should learn about the expected turnaround times for Underwriting to produce a quote once Sales collects the required information. Failing to return a timely quote to an employer group puts the organization at risk of losing business. Exhibit 3 summarizes the risks and controls for quoting timelines.

Fraud

Our internal audit standards require evaluating the potential

occurrence of fraud and how our organization manages fraud risk. You should brainstorm scenarios that could result in fraud. Exhibit 4 summarizes the risks and controls for certain fraud scenarios.

Technology

Whether Underwriting uses a specific industry software application or another tool such as spreadsheets to calculate the rates, you should consider the risks and controls In Exhibit 5.

Exhibit 3 – Risks and controls for quoting timelines

Risks	Potential controls
Quotes are not completed timely.	Quoting turnaround times are monitored by management.

Exhibit 4 – Risks and controls for fraud

Risks	Potential controls
Employer group or member data provided by a prospective employer group was intentionally misrepresented to obtain a lower rate.	Final quotes contain language indicating quotes can be adjusted in the event certain information changes once the group has enrolled.
An underwriter intentionally produces a lower rate in exchange for a kickback from the employer group.	Quotes are reviewed and approved by an appropriate individual prior to being released to the employer group.

Exhibit 5 – Risks and controls for technology

Risks	Potential controls
The quoting system or tool does not reflect business rules or function properly due to improper changes being made.	Changes are reviewed, tested and approved prior to being implemented in production.
Unauthorized users gain access to modify data or applications.	All new users or changes to existing users' access rights require approval.
An inadequate deprovisioning process causes users to retain unnecessary access.	Accounts are disabled, locked or revoked upon notification of a user's termination. A user access review is periodically performed, and unnecessary access is removed.
Inadequate enforcement of password requirements leave the organization open to attacks that could corrupt data or deny access to the application.	Passwords are configured to systematically enforce password complexity, length, expiration, reuse and account lockout settings in accordance with organizational policy.
Backups are not available to restore data in the event of a system disruption or failure.	Backup software is configured to automatically perform database backups in accordance with a defined backup schedule. If backups fail, the appropriate team is notified. Errors are investigated and resolved.

A delayed quote to an employer group risks losing business.

Data analytics

Internal audit professional standards require that you consider the use of technology-based audit and other data analysis techniques. If a system is used during the underwriting process, you may be able to use data analytics to perform some of your testing.

For example, if the system contains data about each quote produced during the audit period, you may be able to recalculate the quoting timelines. You may be able to identify quotes produced that were not approved by the appropriate individual. Using data analytics not only provides greater coverage and assurance but can also save time during testing.

Conclusion

The rates determined through the underwriting process can have a huge effect on your health plan's bottom line. Engage

with the right stakeholders and ask the right questions during planning to get your audit on the right track. In addition to operational risks, do not forget about fraud and technology risks. Lastly, look for ways to use data analytics to provide greater assurance during testing. **NP**



Megan DeVries, CHIAP®, CIA®, is an audit manager at Corewell Health in Grand Rapids, Mich. Her 18 years in the healthcare industry have included managing the health plan's Model Audit Rule engagement, Megan also works with external auditors to issue the health plan's SOC 1 and SOC 2 reports. She is an AHIA board member and serves on the AHIA Editorial Board and the eNews Committee. Megan can be reached at Megan.DeVries@corewellhealth.org.



Internal audit is not a transaction, it's a process, and you can't afford to blink.

Learn more about PYA's Internal Audit Overwatch. Custom, Steadfast Vigilance



800.270.9629 | pyapc.com/overwatch



FORT HILL
Associates, LLC

- Pre-Construction Contract Reviews
- Construction Phase Contract Audits
- On-site Training

Empowering Owners to Eliminate Construction Overcharges



Construction Contract Auditing

864 631 2376 • www.forthillassociates.com
contact@forthillassociates.com

Credit Balances

Satisfy the obligation for refunds

By Symone Rosales, RHIT, CHPS, CHC

While credit balances in patient accounts receivable may occur during the normal course of business, they require consistent attention, monitoring and ongoing resolution to prevent accumulation. Neglect can result in penalties due to overpayments that occurred and were not returned. Perform internal audits to assess the compliance risks of credit balances and ensure internal controls are effective to mitigate risks.

Managing the revenue cycle of a healthcare organization requires oversight of many components, including credit balances. Healthcare entities, similar to other organizations, are considered creditors when offering or extending credit for services that result in debt.¹

One substantial risk within the healthcare revenue cycle is a *credit balance*, which is defined as an excess of payment on an account. Credit balances can exist for many reasons, such as incorrect coordination of benefits (COB), improper billing and duplicate payments. Credit balances can be classified based on the payer source.

Patient credit balances – Patient credit balances can occur from accepting incorrect payments from patients. In most cases, the overpayments result from a miscalculation of out-of-pocket costs or insurance benefits. Collection of a presumed contractual copay, deductible or co-insurance without an in-depth understanding of the insurance benefits may produce a credit balance on a patient account.

Commercial payer credit balances – Organizations may need to review credit account balances related to third-party payers. Commercial payer credit balances may occur when a private insurer makes an overpayment. The credit balances are often caused by systematic or contract issues.

Government payer credit balances – Government payer credit balances are excessive or incorrect payments made

by government programs such as Medicaid or Medicare. Overpayments from these payer sources often present the highest risk, because [failure to comply](#) with their requirements may result in a violation of the False Claims Act (FCA). To avoid misappropriation of funds and FCA violations, your organization must actively monitor and manage credit balances.

Common causes

Credit balances can arise in many ways. Causes of credit balances include instances where a provider is:

- Paid twice for the same service by Medicare or another insurer
- Paid for services planned but not performed or for noncovered services
- Overpaid by the patient because of errors made in calculating beneficiary deductible and/or coinsurance amounts
- Paid for outpatient services erroneously included in a beneficiary's inpatient claim.

You should note that federal payers consider that even small amounts of overpayments, such as \$1 or \$5, need to be returned to them.

More often than not, negative balances can also occur due to errors from the payers or within your organization's internal billing teams. Internally, manual or system posting errors could have an account appear to have a credit

¹ 15 U.S.C. § 1681m, <https://www.govinfo.gov/content/pkg/USCODE-2020-title15/pdf/USCODE-2020-title15-chap41-subchapIII-sec1681m.pdf>



balance. For example, incorrect postings of allowable rates or adjustments may result in a negative balance on the account. The negative amount would not be a true credit but rather an error that can be resolved.

Such errors could occur due to human error, but others could be a result of a computerized payment posting issue. Most organizations post receipts utilizing the [EDI 835 Healthcare Claim Payment and Remittance Advice](#); however, these files may contain miscalculations.

Another example of possible credit balances is a true overpayment from a payer due to system errors. Payers often rely on claim systems to process payments, but the system may not be configured properly and may issue an overpayment. Timely management of credit balances would allow your organization to promptly identify internal or external errors and correct overpayment causes.

Compliance requirements

Overpayments are regulated by the federal government as well as by requirements further defined by states. You should review applicable guidelines since the government entities provide specific timelines regarding how a credit balance must be handled and when the overpayment needs to be refunded.

Even when patient credit balances are identified, some healthcare organizations hold funds with the intent to apply the credit to any future balances that patients may owe. Holding the funds is not the best course of action.

Patient requirements – If explicit, formal patient requirements do not exist in your organization, consider incorporating them in policies. You can safely assume that your patients expect timely refunds. Embed that objective into your refund processes. Do not wait until patients request their refunds. Be proactive and end their experience with your organization on a positive note.

Conduct your audit by categories of payers—patient, commercial payer or government payer.

State requirements – Your organization may have an obligation to send the funds to your state controller's office. States have enacted escheat or unclaimed property laws that require organizations to be proactive in returning property including credit balances to the rightful owner. Laws could include written notices to the reported owner or return of the unclaimed property to the state controller. *Timelines vary* from jurisdiction to jurisdiction.

Commercial insurance requirements – Third-party payers also have requirements in the event of an overpayment. Commercial insurance plans are first governed by the terms of the contract and then by state statutes.

Federal requirements – While state statutes and contracts will apply, a federal statute also obligates a healthcare entity to return credits to a private insurer. [Theft or embezzlement in connection with healthcare](#) can result in penalties in cases where a person or organization knowingly and willfully embezzles, steals, or otherwise without authority converts to the use of any person other than the rightful owner, or intentionally misapplies, any of the moneys, funds, securities, premiums, credits, property, or other assets of a healthcare benefit program.

The term *health care benefit program* is defined in [18 U.S.C § 24](#) as any public or private plan. In this context, withholding overpayments from commercial insurance plans may also carry serious legal repercussions.

Overpayments, made by any government third-party payer, must be returned under strict time limits. In 2009, the [Fraud Enforcement and Recovery Act](#) (FERA) was enacted to aid in healthcare fraud enforcement. FERA is clear that retention of an overpayment results in a liability under the FCA.

Ongoing monitoring of credit balances allows for timely correction of overpayment causes.

More specific deadlines were established in 2010 under the [Affordable Care Act](#) (ACA). The act contained a stipulation that healthcare organizations identify overpayments received, report them, and repay them to the rightful owner within 60 days of identification. The [Medicare Credit Balance Report](#) (Form 838) is required when reporting and refunding overpayments.

The ACA also provides an in-depth definition of identifying a credit balance:

“[A] person has identified an overpayment when the person has or should have, through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment. Creating this standard for identification provides needed clarity, processes and procedures for providers and suppliers on the actions they need to take to comply with requirements for reporting and returning of self-identified overpayments.”²

The ACA statute specifies the allotment of time a provider is allowed for a good faith investigation, mandating a six-month due diligence execution of an investigation.

Perform audits

Aside from routine monitoring of balance reports as part of a provider’s business practices, you may want to conduct periodic independent audits for credit balances. An audit would ensure that proper internal controls are present and credit balances are being reviewed.

Sample selection may include credits in various stages from various payer sources. Remember that each payer source has different requirements governing the refund deadlines.

Best practices would include sorting negative balances by payer source—patient, commercial payer or government payer. Common account receivable reports often list outstanding accounts within 1 to 90 days past the date of service. By utilizing these reports, you can review identified credits within specific time frames. Overpayments must be

returned within 60 days to federal payers. Review credit balances for accounts with government third-party payers approaching and past the 60-day deadline.

During a credit balance evaluation, conduct a root cause analysis to determine audit findings. Ascertain if credit balances are truly due to an overpayment or a systematic error. A root cause analysis also assists in determining revenue cycle staff areas within your organization that need education if overpayments are due to over-collecting or a misunderstanding of insurance benefits. You should validate your audit results with the accounts receivable department due to variants in possible errors.

Additionally, determine if organizational policies and procedures identifying the requirements involving credit balances are present. Policies that could apply to the resolution of negative balances include:

1. Bad debt collections
2. Medicare Form 838
3. Patient credit balance
4. Payer credit balance/overpayment refund
5. Payment posting
6. Point-of-service collections
7. Unclaimed property
8. Voided charges
9. Small-dollar adjustment

Address findings

To mitigate risks, revenue cycle management may need to implement additional internal controls for credit account balances. Additional written policies and procedures and consistent monitoring of credit balances are often implemented as controls to identify and manage overpayments.

Improvements in processes should ensure that the proper steps are being taken to comply with state and federal requirements, including meeting prescribed timelines. Though new procedures may require additional staff resources, your revenue team should leverage their sophisticated electronic health record (EHR) systems to aid in account reviews by producing alerts and other reports.

²<https://www.govinfo.gov/content/pkg/FR-2016-02-12/pdf/2016-02789.pdf>, page 1

Many audits identify the need for staff training, which could include federal and state requirements regarding credit balance timelines. Training for the revenue team should also include payment reconciliation for both manual and computer-assisted posting.

Since the possibility of an account becoming a credit could be a result of posting errors, staff may need to be

trained to diligently identify possible credits on accounts. When staff are familiar with identifying credits and have an understanding of whether the balance was an error or a true credit, credit balances can be minimized.

Conclusion

Institutional providers, such as hospitals, need to monitor credit balances, extract data reports from their patient accounting and billing systems and submit their Medicare Credit Balance Reports. Also, your smaller providers and physician practices need to be familiar with FCA risks associated with lack of timely return of credit balances from overpayments and implement similar procedures. Avoid compliance and reputational risks when refunds are not processed and reported timely. **NP**

Resources

- Centers for Medicare and Medicaid Services - [Medicare Program; Reporting and Returning of Overpayments \(Final Rule\)](#)
- Ensemble Health Partners – [How to Resolve Credit Balances and Improve Patient Experience](#)
- Maynard Nexsen – [Provider Credit Balances Under the Microscope: Increased Enforcement Means Need to Review Credit Balance Procedures](#)
- MD Clarity – [Credit Balance Percentage](#)
- Plante Moran – [Resolve Credit Balances to Improve Compliance and Reporting](#)

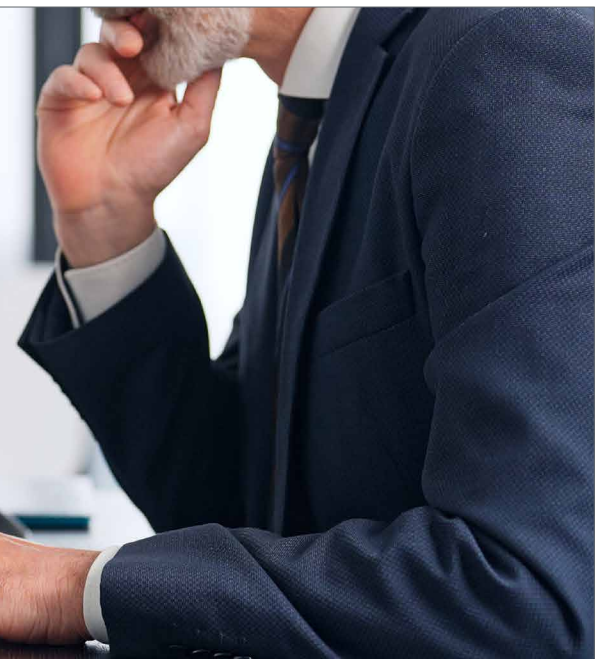


Symone Rosales, RHIT, CHPS, CHC, is the Revenue Regulations Manager at Multicare Health System. She has previously held a variety of leadership roles in revenue cycle management. Symone can be reached at Symone.Rosales@multicare.org.

Gain recognition as a published author

Share your best work with us.

New Perspectives is looking for your most interesting audits. Check our writer's guidelines on the AHIA website or contact the editor at: Mike.Fabrizius@gmail.com



Make Patient Safety Your Diversion Program Priority

Beware of counter priorities

By Kim New, JD, BSN, RN



An often-asked question is how to determine if a drug diversion prevention, detection and response program is successful. Many indicators exist to signal an effective program that is centered on patient safety. Conversely, certain signs can suggest that a diversion program does not place patient safety as its highest priority. Be prepared to recognize the red flags of an improperly oriented program.

Common signs of an effective program include healthy self- and peer reporting and a decrease in diversion over time. Emphasis on a decrease over time is necessary because a substantial increase in the amount of diversion is initially identified when appropriate surveillance, monitoring and staff education are put into place.

Red flags

Unfortunately, several things can indicate that a drug diversion program is not effective from the outset, including not identifying any diversion at all. Reasons why this might happen include inadequate resources, poor monitoring and an ineffective or obstructive investigation process. An investigation process that is hindered can be particularly destructive. Suggestions and suspicions of diversion that are ultimately found to be unsupported are often seen as evidence of profiling or picking on a particular group of workers—most often nurses.

Nurse managers frequently close ranks in response to what they perceive as the diversion team picking on their staff with illegitimate allegations. Managers that might have been uncertain about what was occurring at the beginning of the investigation may become emboldened and even accuse diversion team staff of inappropriately targeting their nurses.

Staffing shortages and the fear of having to train replacement staff often contribute to a negative response. Situations often exist where legal considerations are used to detour an investigation, either by human resources staff or legal counsel.

In cases where diversion is not being identified or diversion is suspected but is ultimately unproven, one way of evaluating the reason is to examine the diversion investigation process. Investigative procedures that have become customary in the organization are often responsible. For example, management uses those who closely supervise staff, such as nurse managers or supervising physicians, to investigate

Guarding against potential reputational harm should never supersede patient safety.

concerns related to their staff. Managers and supervisors should absolutely be included in the process, but they are never in the best position to undertake the actual investigation.

Managers should usually be notified at the outset of any concerns relating to their staff. The manager or supervisor is in the best position to clarify workflows and unit-based practices and is generally the person who will have work schedules, assignments and the most up-to-date information about work performance.

Once he or she is provided with the findings of the investigation, the manager is ultimately the person, along with human resources staff, who will determine the employee's disposition. But because of inherent issues of bias, the manager should not conduct or be directly involved in the actual investigation.

Additionally, the investigation process should not be constrained by executive leadership, who may tend to focus heavily on potential legal or reputational harm. While leadership should be kept informed, allowing them to direct how the investigation is performed can also result in intimidation of investigating staff and ultimately an incomplete or inaccurate report or findings.

Case study

A very good example of the pitfalls of operating a diversion program is from a startling [case in the United Kingdom](#). A neonatal intensive care unit (NICU) nurse was accused and ultimately convicted of murdering seven newborns in her care.

While the circumstances of the case are clearly different from a case of drug diversion, several aspects are similar and many of the same risks exist. Unaddressed, diversion can result in patient suffering, harm and even death.

The case involved a nurse named Lucy Letby. Medical staff had raised concerns for months and those concerns were reportedly rebuffed as instances of doctors picking on a nurse. By all other accounts, she was a top performer in her unit. How could she be accused of such a serious offense?

The [hospital leadership](#) had been notified of concerns that associated Letby to unexplained and unusual neonatal deaths. The nurse manager over Letby performed an investigation when the concerns were raised and unsurprisingly found no evidence that Letby had contributed to unexplained deaths in the NICU. Her presence when the deaths occurred was attributed to coincidence. Concerns by the patients' families were also left unaddressed.

Members of the medical staff who raised this issue were made to apologize for raising concerns that Letby harmed her patients.

Ultimately external investigations led to the arrest and conviction of Lucy Letby. Testimony in the investigations included allegations that the hospital's director of legal services had said that involving the police would harm the hospital's reputation.

In looking back at the Letby episode and calling for change within the British National Health Service, an ombudsman cited some of the main failures in the case. The failures were among those commonly seen in diversion cases, which included:

- Defensiveness of leadership, who were described as placing a concern about potential reputational harm above patient safety
- A lack of initiative to ensure an independent investigation of the allegations
- Punitive measures against those who raised concerns

The failures noted in the Letby investigation are eerily familiar to me from my investigations of drug diversion. I have seen cases where allegations of drug diversion, including diversion with patient harm, were dismissed in the face of strong supporting evidence by nurse managers, senior executives, and general counsel. In one case, legal counsel to a state licensing board commented that no action could be taken absent a confession by the diverter.

Conclusion

Cases involving deliberate homicide in the medical setting are rare, but the culture of protecting the institution over patients and the fear of legal exposure extends into drug diversion, which is a far more common crime. Take the lessons from the UK case to heart in your organization to avoid patients and staff being harmed by diversion and by those who turn a blind eye to it. **NP**



Kim New, JD, BSN, RN, is the principal at Diversion Specialists. She is an expert in controlled substance security and DEA regulatory compliance, and works with healthcare facilities to set up and expand their drug diversion programs. Kim can be reached at KimberlyNew@orange.fr.

Remote and Out of State Workers

Audit the tax implications

By Louise Labrie, Mary Torretta, JD, and Hayley Oakes

Flexible and remote working arrangements that began during the Covid-19 pandemic have evolved into a sought-after benefit. In fact, a survey of 25,000 U.S. workers indicated that over 40 percent of healthcare professionals work remotely at least part-time. However, your organization is required to withhold taxes in the states where your employees work.

Healthcare organizations have always had two classes of workers—clinical and nonclinical. Most clinical workers need to live close enough to the location(s) where they provide direct patient care. But employees that can conduct the majority of their work remotely could be living anywhere, even internationally. In many cases workers moved temporarily during the pandemic and simply never moved back.

Much of healthcare work is performed by employees with nonpatient-facing, computer-based roles that can be performed remotely. Examples include employees in information technology, finance, accounting, human resources, administrative support, and most revenue cycle functions.

Remote work prior to the Covid-19 pandemic was limited among clinicians. Because of the need to see patients safely and reduce the spread of infection, remote work during the Covid-19 pandemic increased among certain clinicians. By leveraging telehealth and video visits, physicians and care teams were able to remotely conduct monitoring and management of patient care, which is much of the work they do at medical offices.

Healthcare system human resources (HR) departments became responsible for being aware of where physicians

were physically located while treating patients—and whether they are working outside their licensed states.

Payroll compliance

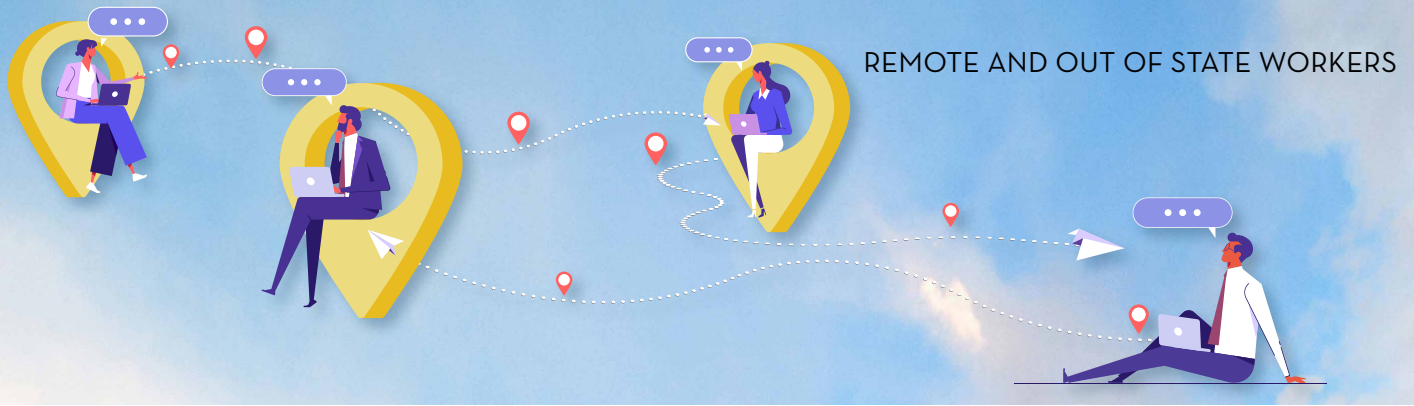
Healthcare organizations that employ remote staff who live in other states are required to register as employers in those states. Also, employees living internationally could also encounter additional tax and legal complexities, such as creating legal jurisdiction for labor requirements, tax and economic nexus, and perhaps requiring withholding taxes in foreign jurisdictions and compliance with international tax treaties.

Your organization needs to meet its compliance obligations by:

- Having processes and controls in place to track and update all the data needed about where employees are working
- Keeping current with tax updates and changes in the states and localities where remote employees are working

Physical locations – Recording the physical locations where your employees work matters, especially regarding state and local taxes. Even with an HR system with functionality that easily facilitates your employees' ability to keep their

Human resource departments need to know where employees are physically located while working.



Maintain accurate and detailed records of remote worker hours, compensation and tax-related documents.

address information updated, the onus will always be on the healthcare organization to ensure that employee location data is accurate and current.

Payroll taxes – State and local income and payroll tax laws govern how employees are taxed, and they vary greatly from state to state, adding considerable complexity to the task of managing the organization’s tax and compliance obligations.

Every state has its own rules. Additionally, many cities and counties have their own rules. Knowing what those rules are before you get started is very important. The filing obligations are immense, but a huge challenge also exists in capturing all the data needed about where your employees are working.

The rules governing payroll tax payments are complex, adding significant new administrative burdens for your HR department. The ultimate responsibility for meeting payroll tax reporting and payment requirements is on the employer and the penalties for not satisfying them can be severe.

During an internal audit conducted by Grant Thornton, a large healthcare system with employees in 20 states found that the records for those employees did not include the current locations for all remote employees. As a result, the organization was required to pay a penalty. You want to get ahead of similar situations to prevent hefty tax penalties.

To ensure compliance and avoid penalties, employers are ultimately responsible to withhold state taxes for all employees—including remote employees and those who live out of state and commute to work.

Our internal audits have identified common complications that arise when managing multistate payroll tax withholding:

- Some states require employers to withhold state unemployment taxes and pay them to the state.

- Employers are liable for errors in classifying employees as independent contractors.
- Some states require the employer to withhold additional funds for state benefits programs.

Employee benefits – Employee benefits can add another wrinkle when employees work far outside your organization’s established physical footprint. Your organization may have a great health plan coverage for employees in certain geographic areas but may not have coverage in other areas.

Your organization will need to think through what happens, for example, if an employee falls and breaks an arm while working at home. Is that worker’s compensation or homeowner’s insurance? Written policies should be in place that address all conceivable scenarios.

An internal audit approach

Nearing four years since the start of the pandemic, many healthcare organizations are still struggling to identify where their remote employees are located and mitigate the associated risks. While organizations are still facing challenges related to remote workers, your internal audits can play an important role in determining if your organization has appropriate controls in place to manage and monitor a remote workforce.

Given the significant potential for risk and penalties for noncompliance regarding remote workers, substantial value exists in conducting internal audits. Evaluate policies, processes and controls in place to confirm, update, and maintain and keep accurate and detailed records of remote worker hours, compensation and tax-related documents.

When you audit your organization’s population of remote workers, many elements exist to test and evaluate existing controls.

Exhibit 1 – States with special payroll requirements

No state income tax
Alaska Florida Nevada New Hampshire South Dakota Tennessee Texas Washington Wyoming
SUTA withholding
Alaska New Jersey Pennsylvania
Temporary disability deductions withholding
California Hawaii New Jersey New York Rhode Island
PFML deductions
Colorado Connecticut Delaware (effective 2025) Maryland Massachusetts New York Oregon Rhode Island Washington Wisconsin (effective 2024)
Retirement plans required
California Colorado Connecticut Illinois Maine Maryland Massachusetts New Mexico New York Oregon Vermont Virginia Washington

Know the rules

To track employees across state, local and international boundaries, you must understand the requirements.

Determine appropriate categories– Independent contractors are responsible for managing their own taxes, so an employer is not responsible for withholding payroll taxes for independent contractors, The [Internal Revenue Service provides guidance](#) on identifying when withholding is required and the consequences of mistakenly treating an employee as an independent contractor.

Identify withholding requirements – Identify the withholding requirements of the location of the residence for each remote worker. States vary widely in their withholding requirements.

Determine additional withholding requirements – Check for states that require any additional withholding. For example, some states require employers to withhold and pay SUTA (State Unemployment Tax Act) taxes. Some states tax all income received by residents, including income earned for work done in other states. Some states require employers to withhold temporary disability insurance deductions from employee wages, while others require employers to have PFML (paid family and medical leave) deductions from wages. In addition, some states require your organization to offer a retirement savings plan, which could mean another withholding category.

Exhibit 1 identifies states with special payroll requirements.

Evaluate policies

Ascertain that your organization has established a comprehensive remote work policy or has updated existing policies that require employees to disclose their work location(s). Also, verify that your organization has provided training to employees to inform them about the organization’s remote policies, procedures, and the potential implications and penalties in the event of noncompliance.

Ensure that your organization has established processes to prompt employees to validate their address and physical location throughout the year. The prompts can occur during times such as annual benefit enrollment, performance

Know the payroll withholding requirements of the state of residence for each remote worker.

The human resource system should communicate employee address updates to the payroll system.

reviews, and year-end tax information distribution communications.

Consider automation

Systems designed to automatically update when critical data changes occur can offer real value. Ideally, your HR system should note that an employee has made an address update and then contact the payroll system to update payroll deductions and withholding.


In addition, your organization may leverage a time-entry system that requires employees to validate the physical

location where they have performed their work. When the time-entry system requires employees to login via a VPN, an individual’s location could be easily captured.


For organizations with authority to access their employees’ IP addresses, the data can be used to validate their employee’s location and identify any potential implications.

Conclusion


You can conduct internal audits to ensure that monitoring controls exist, and procedures are being followed, so that payroll information is accurate at tax time. Ensure that current practices monitor the employee’s location in order to pinpoint any compliance risks and address them before any penalties are imposed. Proactive audits can go a long way in demonstrating your organization’s good faith efforts to comply. **NP**



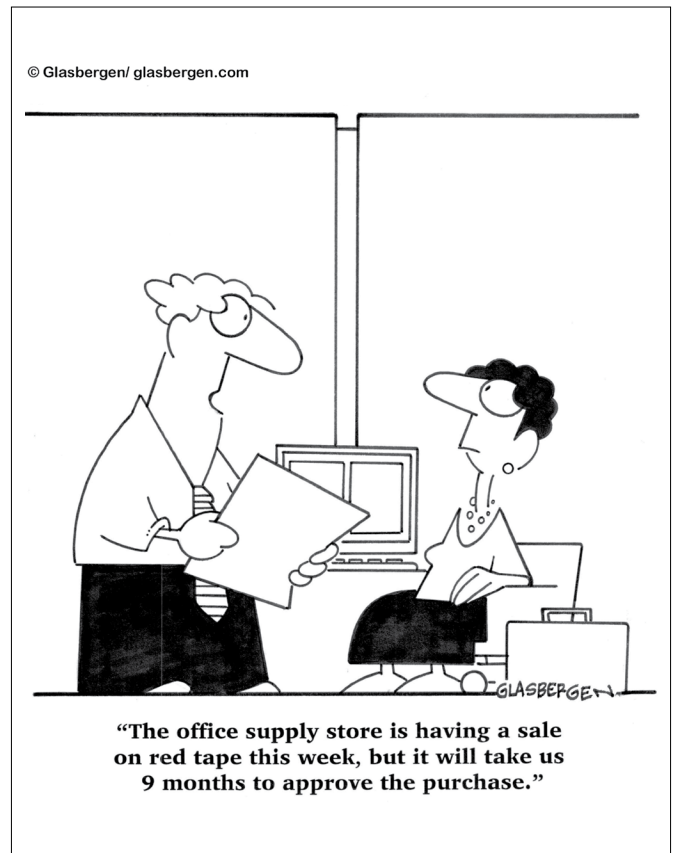
Louise Labrie is a Principal and Healthcare Risk Leader at Grant Thornton. Louise can be reached at Louise.Labrie@us.gt.com and 424-392-0122.



Mary Torretta, JD, is a Principal and Healthcare Tax Leader at Grant Thornton. Mary can be reached at Mary.Torretta@us.gt.com and 703-847-7659.



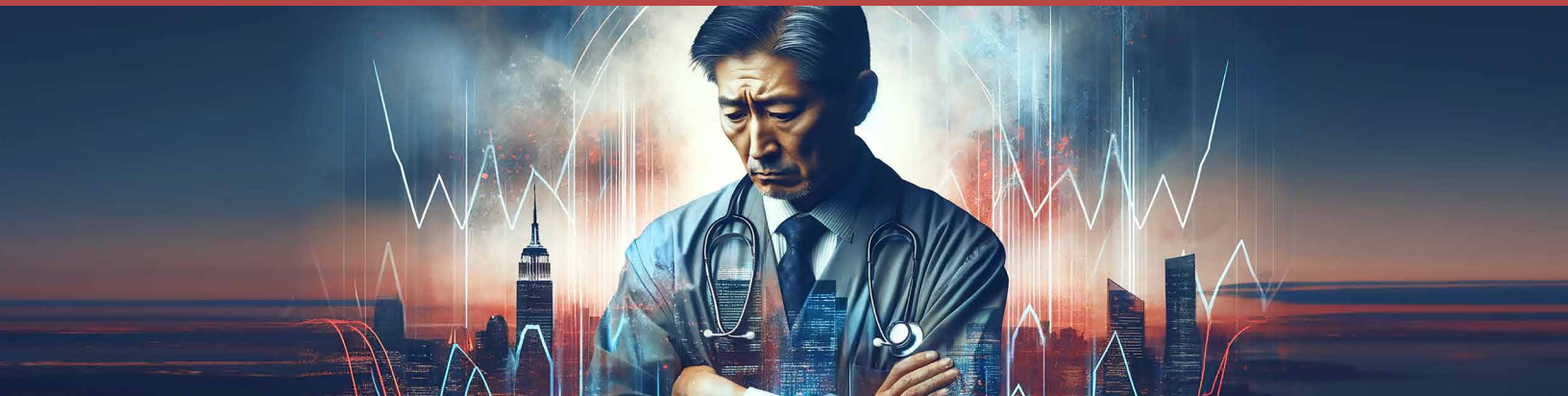
Hayley Oakes is a Senior Manager in Healthcare Risk at Grant Thornton. She can be reached at Hayley.Oakes@us.gt.com and 678-515-2307.



Fraud Risk Management

Recognize the need for a formal program

By Brandi Steinberg, CPA, CFE



Fraud is prevalent across every sector in the U.S., and healthcare is no exception. Understand how significant the threats—billing fraud, substandard care, theft, property destruction and bribes—could be to your organization. Consider how to better protect your organization with a formal, structured program to prevent and detect fraud.

The [National Health Care Anti-Fraud Association](#) (NHCAA) estimates that the financial losses due to healthcare fraud are in the tens of billions of dollars each year. A conservative estimate is 3 percent of total healthcare expenditures, and some government and law enforcement agencies place the loss as high as 10 percent of our annual health outlay, which could mean more than \$300 billion.

Government initiatives

To counter this threat, the U.S. Department of Justice (DOJ) has made a point to emphasize their plan to combat healthcare fraud. Because of the broad range of offenses and enforcement areas in healthcare fraud, the DOJ is casting a wide net to cover as many of these areas as possible.

DOJ has established a [Health Care Fraud Unit](#) (HCFU) consisting of 80 prosecutors and strike force teams

strategically located around the country. The strike forces bring together analytical and investigative resources of different agencies, such as the Federal Bureau of Investigation, Health and Human Services, Office of Inspector General, Centers for Medicare and Medicaid Services, Drug Enforcement Agency, and state and local law enforcement partners.

The DOJ's HCFU efforts include the following initiatives:

- [Telehealth fraud](#) – The initiative targets false and fraudulent claims submitted for telemedicine services. In 2022, this initiative charged 36 defendants in 13 districts for over \$1.2 billion in fraud losses.
- [Nursing homes](#) – The focus is nursing homes that provide grossly substandard care to their residents.
- [Sober homes](#) – The target is improper billing and kickbacks offered to individuals to enroll at treatment facilities that bill for medically unnecessary therapy and/

A fraud risk management program should prevent fraud before it occurs and detect fraud before it grows.

Have a process to review, investigate and resolve allegations and suspicions of fraud and misconduct.

or therapy never actually provided. Since inception, 28 individuals have been charged with over \$1 billion in false billings.

- [Business email compromise](#) – The focus includes emails from supposed healthcare providers to health insurers to fraudulently divert money by using spoofed email addresses and bank account takeovers.

Fraud by the numbers

In 2022 alone, the Health Care Fraud Unit prosecuted the following cases:

- \$1.4 billion [billing fraud scheme](#) at rural hospitals in Florida, Georgia and Missouri
- \$77 million [Covid-19 and allergy testing scheme](#) involving a Silicon Valley medical technology company
- \$463 million [genetic testing scheme](#) to defraud Medicare perpetrated by a Georgia man

According to the [U.S. Sentencing Commission](#), in fiscal year 2022, 64,142 cases were reported. Of those, 5,208 involved theft, property destruction and fraud. Of the 5,208, 8.4 percent of the offenses involved healthcare fraud (431 cases), which represents an increase of 1.4 percent since 2018.

Of the offenders, 61.3 percent were men, and their average age was 49 years. Over 90 percent were U.S. citizens, and 88.6 percent had little or no prior criminal history.

The median loss for these offenses was \$1,300,000. Of those offenses, 15.1 percent involved loss amounts of \$150,000 or less and 16 percent involved loss amounts greater than \$9.5 million.

Sentences were increased for:

1. The number of victims or the extent of harm to victims
2. Conviction of a federal healthcare offense involving a government healthcare program and a loss of more than \$1 million
3. Using sophisticated means to execute or conceal the offense
4. Using an unauthorized means of identification
5. A leadership or supervisory role in the offense
6. Abusing a public position of trust or using a special skill

7. A victim whom the defendant knew or should have known was vulnerable
8. Obstructing or impeding the administration of justice

Sentences were decreased for minor or minimal participation in the offense.

The top five districts for healthcare fraud offenders were:

- Southern District of Florida
- Eastern District of Michigan
- Central District of California
- Southern District of Texas
- Northern District of Texas

Punishment

- 78.7 percent were sentenced to prison.
- The average sentence for healthcare fraud offenders was 30 months.

Recognize and respond

The size, scope and frequency of healthcare fraud schemes indicate a threat that is too big to ignore. How you choose to respond will determine whether you can adequately protect your organization against fraud.

Internal auditors cannot get lost in the weeds of the routine and mundane tasks of day-to-day roles and forget the bigger picture on fraud. You must take the initiative to educate yourself on current threats and implement ways to combat the risks to your organization and the patients you serve. One proactive and systematic way to mitigate fraud risks for your organization is to implement a fraud risk management program.

Implement a program

The main goal of fraud risk management is to prevent fraud before it occurs or detect fraud before it grows. While the elimination of all fraud is impossible and the attempt is impractical, organizations must manage the risks associated with fraud. Organizations committed to fraud prevention and detection will address both internal and external fraud risks.

Five program components are necessary.

Governance – Governance addresses the manner in which the board of directors and management meet

their respective obligations to achieve the organization's goals. They should demonstrate their commitment to high integrity and ethical values.

Risk assessments – The assessment of risk is an active and repeated process for identifying and evaluating fraud risks relevant to your organization. The risks include fraudulent reporting of financial and other information, asset misappropriation and corruption. The goal is to assess the likelihood and significance of these risks, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

Control activities – Control activities are generally classified as either preventative or detective, and the specific procedures or processes are intended either to prevent fraud from occurring or to detect fraud quickly when it does occur. The selection, development, implementation and monitoring of fraud preventative and detective control activities are crucial elements. The control activities are

documented with the descriptions of the identified fraud risk and scheme, the fraud control activity designed to mitigate the risk, and the identification of the personnel responsible for the fraud control activity.

Investigation and corrective action – Whenever fraud does occur, a process must exist for review, investigation and resolution of allegations of fraud and misconduct. The process must be prompt, competent and confidential, and also assist in improving the chances of loss recovery and minimizing exposure to litigation and damage to reputation.

Monitoring activities – Monitoring activities surveil the effectiveness of the overall fraud risk management program to ensure that the other elements are present and functioning as designed. Monitoring activities also allow your organization to identify any necessary changes to the program in a timely manner.

Exhibit 1 illustrates the components of a program.

continued on page 36

Exhibit 1 – Components of a fraud risk management program



Determine specific fraud risks related to each individual internal audit project.



Alicia Capps, CIA®, CPA

Chief Audit Executive Intermountain Healthcare

In the beginning of your career, you worked in a Big Four professional services firm. Tell us about the foundation you built in consulting and how it affected your career.

The greatest benefit I gained with a Big Four firm was exposure. As a consultant I worked with clients in various industries and advised them on distinct functions across their organizations. I began in 2003 during the adoption of the Sarbanes-Oxley 404 (management assessment of internal controls) requirement. As a new graduate, I was a sponge!

I assisted organizations in the development and implementation of compliance programs for the new regulations and then took the lessons learned to my next clients. The experience taught me how internal audit (IA) skills could be applied to any process in any industry. The work gave me the confidence to jump into healthcare knowing I would be able to add value in that industry's complex environment.

My time with the Big Four firm exposed me to several different leadership styles, both internally and externally. I had a front row seat to executive leaders from public, private and government organizations. I observed leaders that were connected to their business and valued insights from internal audit.

I learned how to navigate key relationships at all levels of an organization to position internal audit for success. As clients and teams rotate frequently in Big Four firms, I was able to develop and refine my own leadership and communication style as I progressed in my career and was assigned new responsibilities or clients. Many people from that time shaped me; some may not realize their effect!

Intermountain Health merged with SCL Health two years ago. What has been internal audit's role in merger-related activities?

The first year of integration activities for IA was inwardly focused. Two strong departments were combined that followed similar audit methodologies. However, the two were on separate systems and had differing operational processes.

The first few months were focused on developing the integration plan for IA and aligning our policies and procedures. We then began the process of selecting and implementing our audit management system. Now we are at the end of that journey and are working as a fully integrated department.

Thankfully, IA was included in the first integration phase. Early internal focus allowed us time to be positioned to assist in the organization's continued integration efforts where needed.

IA continues to partner with our operational counterparts as they continue down the path of integration. IA has reviewed their harmonized policies prior to publication, performed post go-live assessments for significant process changes and systems integrations, and provided current-state process mapping to provide an understanding of existing control environments.

How has your IA organization changed as a result of the merger? Anything noteworthy stand out from the integration?

The IA department has only gotten stronger due to the merger. We took the best attributes of two high-performing teams and incorporated them into the integrated department. I am honored to have led this group of individuals through the experience and I know the best work from our team is yet to come.

We were fortunate enough to retain the headcount of both legacy departments. The size of the newly formed group has allowed us to focus caregivers (auditors) on specific risk classifications and become subject matter experts rather than stretching everyone to cover all risk areas.

The concentrated expertise has allowed us to advance some strategies faster than anticipated. With the speed that risks change in healthcare, our caregivers are in position to monitor specific risks. They work directly with accountable leaders to understand how management is responding. Then we can align our services with organizational strategies without delay.

As a long-standing AHIA member, please speak to the value of an AHIA membership and your service to the organization.

Healthcare is a service used by all of us, and as healthcare internal auditors we strive to assist our organizations to operate at their highest potential. AHIA, a volunteer driven organization, creates a special environment for us to share our experiences, learn from others, and foster the future of our profession.

The significant learning opportunities and the availability of subject matter expertise and audit resources that are available for members is outstanding. Before I even attended my first conference, I expressed my interest in volunteering.

Volunteering with AHIA has been a highlight of my career. I have served on the Annual Conference Planning Committee, as a member at large on the Board of Directors, the chair of the Affiliations Committee and am currently a member of the Professional Practices Committee. Each role has given me much more than I gave.

I always find engaging with other professional colleagues provides me with a fresh perspective on our work. And I have been able to stretch my leadership skills while gaining additional industry knowledge.

What are your top-of-mind risks?

My top-of-mind risks going into 2024 are cybersecurity, business continuity and the current economic pressures facing healthcare organizations.

Healthcare organizations are more frequently becoming the victims of cyberattacks. I am focused on how IA can work with our counterparts in the second line of defense to not only prevent an attack, but also ensure that the level of preparedness to respond and operate should an attack occur is adequate.

Regarding financial pressures within healthcare. I often ask myself: Where can IA assist our operators who are implementing new strategies to align our organizations with high quality care at a lower cost with sustainable margins? IA has the opportunity to be a partner in all aspects of healthcare operations from clinical care delivery models to revenue cycle management as our organizations face a challenging economic climate. **NP**

This interview with Alicia Capps (Alicia.Capps@imail.org) was conducted by Terry Corcoran, Director, Protiviti. To nominate someone for the Member Spotlight, you can reach Terry at Terry.Corcoran@Protiviti.com.

Fraud Risk Management

continued from page 34

Final thoughts

If you are unaware of the specifics of your organization's program, inquire of management regarding what activities are in place to prevent and detect fraud.

You should compare your organization's fraud efforts to the five components and authoritative guidance of professional organizations (see the sidebar for resources) to:

- Evaluate the effectiveness of your fraud risk assessments
- Improve these assessments as necessary
- Determine specific fraud risks related to each individual internal audit project
- Identify potential control enhancements to minimize ongoing fraud risks

If your organization does not currently have a fraud risk management program, champion the initiation of a formal program. The regulatory, reputational and financial risks justify a robust program. **NP**

Resources

- Association of Certified Fraud Examiners (ACFE)
 - [Common Telehealth Fraud Schemes You Should Know About](#)
 - [Fraud Prevention Check-up](#)
- ACFE and Committee of Sponsoring Organizations of the Treadway Commission – [Fraud Risk Management Guide \(Executive Summary\)](#)



Brandi Steinberg, CPA, CFE, is a Forensics Manager in IAG's Forensics family law accounting practice. She assists attorneys on cases involving business litigation, shareholder disputes, corporate internal investigations, fraud allegations, family law, estates and trusts, and complex financial analysis. Brandi can be reached at 678-214-6628 and Brandi@iagforensics.com.

KODIAK

Making doing more with less, better.

Using data-driven tech, we're able to help clients cover risk faster and better.

We co-source and tech-source with solutions such as:

Audivate: Accelerate tasks and workflows with an innovative internal audit platform built by healthcare auditors, for healthcare auditors.

Financial Control Analytics: Identify cost savings while enhancing financial stability.

Continuous Auditing: Leverage data in audits to expand the coverage of certain risk areas within your health system. Stay ahead of schedule and in front of risk.

Opioid RX: Reduce harmful prescription behaviors.

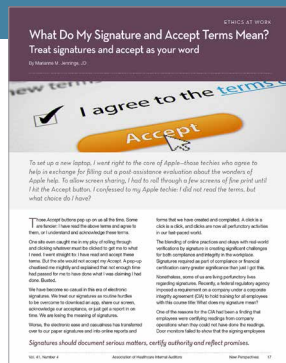
Reimagined AI-supported risk assessment: Get a customized plan for your specific situation that can mitigate your risks using people, data, and technology.

Smart solutions at your fingertips.

<https://linkedin.com/company/kodiak-solutions>

Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2023 Crowe LLP.

New Perspectives is a 2023 AZBEE Awards of Excellence Winner!



The Azbee Awards honor the best in business-to-business media, recognizing outstanding work by B2B, trade, association and professional publications.

Ethics at Work All Content > Regular Column, Contributed > Central Region

Awarded to: Marianne Jennings, JD, Author; Michael Fabrizio, Editor in Chief; Leslie Shivers, Editor; Steve Dunn, Design and Graphics

Q&A on
M&A

proud
bike
commuter

600+
hospital
beds



we speak health IT, EMR and **Helen**

Let's talk



Grant Thornton

Audit | Tax | Advisory | [gt.com](https://www.gt.com)

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd. In the U.S., visit [gt.com](https://www.gt.com) for details



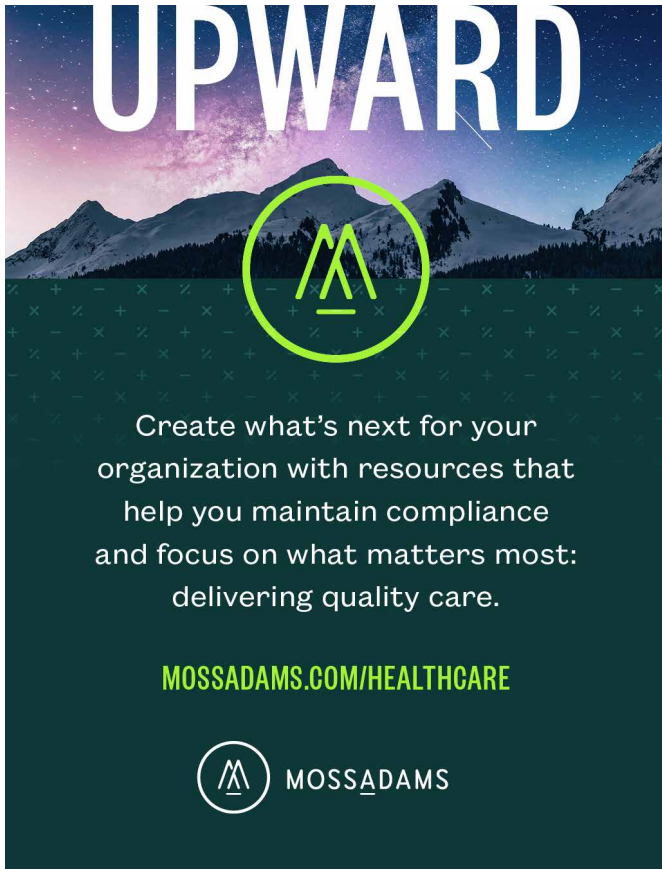
Can you navigate risk amid constant change?

As pressure increases to deliver higher-quality care at lower costs in a changing regulatory environment, the risks and challenges faced by healthcare providers and payors have never been higher. Let KPMG help you navigate today's complex healthcare environment, keep pace with rapid transformation, and employ a dynamic approach to risk management and regulation.

read.kpmg.us/navigatinghealthcare




© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



UPWARD

Create what's next for your organization with resources that help you maintain compliance and focus on what matters most: delivering quality care.

MOSSADAMS.COM/HEALTHCARE




pwc

The New Equation is where advanced tech, data and expertise come together.

Reimagine cyber, risk and regulation to build trust and drive sustained outcomes.

It all adds up to The New Equation.

Learn more at www.pwc.com/us/hirr

© 2023 PwC. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.



UNLOCK A STOREHOUSE OF KNOWLEDGE

Access the Audit Resource Center

Enhance your professional knowledge of internal auditing in the healthcare industry with this clearinghouse of AHIA resources. Find a variety of searchable practical and educational content from *New Perspectives* articles, educational recordings/presentations and CHIAP® Certification examination preparation materials. The collection is continuously updated with materials as they are developed.

Looking to gain expertise in a particular subject area? Want information on an audit topic? Can't find it?

Your answer is on the AHIA website! Try it out today.

- Search by topic (keyword)
- Search by title
- Search by author
- Search by Body of Knowledge category
- Search for any article that has appeared in *New Perspectives* over the past 15 years.

Go to the searchable database at www.AHIA.org.

[Click here!](https://www.AHIA.org) (login required)

Become **CHIAP**[®] Certified



Certify Your Expertise

Our certification sets a new **standard of excellence** for healthcare internal auditors.

Be recognized as a preeminent healthcare internal auditor with the **CHIAP**[®] certification.

ahia.org