E-GUIDE SERIES

Healthicity

The Price of Non-Compliance

Contributor: CJ Wolf

MD, CHC, CCEP, CIA, COC, CPC

Board of Directors

- The Board of Directors Role in Compliance
- Case Study: Caremark International
- OIG Publications for Your Board of Directors
- The Bottom Line: Know Your Responsibilities

Learn more on Page 2 >

CFO

- Making an ROI Case for Compliance
- Case Study: 21st Century Oncology
- Finding Value in Compliance Culture
- The Bottom Line: Cost Avoidance Equals Long-term Revenue

Learn more on Page 6 >

Privacy & Security Officers

- Protecting PHI
- Case Study: Anthem Health
- 5 ePHI Protection Controls You Can Implement Right Now
- The Bottom Line: Avoid Financial Pitfalls by Protecting ePHI

Learn more on Page 10 >

HR Directors

- Onboarding in Compliance
- Case Study: Employing Excluded Individuals
- Onboarding Checklist
- The Bottom Line: HR Plays an Integral Role in a Culture of Compliance

Learn more on Page 16 >

Introduction: Millions Lost to False Claims Allegations

In September of 2024 a surgical center and two physician groups agreed to pay approximately $12.76 million to resolve alleges they violated the False Claims Act because of improper financial relationships between the surgical center and the physician groups. What could these organizations have done differently to protect themselves from such a devastating financial blow?

The adoption and implementation of an effective compliance program significantly advances the prevention of fraud, abuse and waste, while at the same time furthering the fundamental mission of all healthcare organizations, to provide quality care to patients while remaining financially viable. But, compliance isn't a one person show and it's not something that one individual can tackle on their own. It requires buy-in from the entire organization from staff and physicians to the Board of Directors and CFO.

The purpose of this toolkit is to share the importance of compliance to everyone in your organization, and to express how everyone bears responsibility in protecting your organization from a damaged reputation, financial devastation, and legal actions.

Board of Directors

The Board of Directors' Role in Compliance

If a board fails to reasonably oversee a compliance program, it could put the organization at risk and, under extraordinary circumstances, expose individual directors on the board to personal liability.

Case Study

Caremark Board of Directors Sued for Breach of Fiduciary Duty.

One of the landmark legal decisions, the Caremark decision, elaborated upon the many roles and responsibilities of the directors of a governing board and explained a board's compliance oversight responsibilities.

In re Caremark International Inc. Derivative Litigation, 698 A.2d 959, a shareholder sued the Board of Directors for breach of the fiduciary "duty of care." This shareholder lawsuit came after a multi-million-dollar settlement pertaining to the payment of kickbacks to physicians and improper billing under federal healthcare programs. Of the principal fiduciary duties of board members, the one duty specifically implicated by corporate compliance programs is the duty of care.

Essentially, Caremark clarified that a director of a board "has a duty to attempt in good faith to assure that (1) a corporate information and reporting system exists, and (2) this reporting system is adequate to assure the board that appropriate information as to compliance with applicable laws will come to its attention in a timely manner as a matter of ordinary operations." https://oig.hhs.gov/fraud/docs/complianceguidance/040203CorpRespRsceGuide.pdf

Board of Directors Oversight Responsibilities

So, how should a board go about overseeing a compliance program? A few foundational documents are a very helpful place to start to understand and establish responsibilities.

These documents include:

- The Federal Sentencing Guidelines
- OIG compliance program guidance documents
- OIG corporate integrity agreements (CIAs)

OIG Publications for Your Board of Directors

As a board member, you have a lot at stake if your organization is found noncompliant. Your organization can lose a great deal of money and you can be found personally liable. Educating yourself and your fellow board members is crucial for protecting yourself and the interests of your organization as a whole.

NOVEMBER 2023. *General Compliance Program Guidance.* "The board should ensure that the compliance officer has sufficient power, independence, and resources to implement, maintain, and monitor the entity's compliance program and advise the board about the entity's compliance operations and risk."

"The board also should periodically evaluate the effectiveness of the Compliance Committee's risk assessment process."

The United States Sentencing Commission's Guidelines require that an entity's "governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program."

APRIL 2015. *Practical Guidance for Healthcare Governing Boards on Compliance Oversight.* Learn how quality, patient safety and compliance information flows to the board. Educate your board on the structure of the compliance program.

The Bottom Line: Know Your Compliance Responsibilities

The Caremark decision established that the board of directors has a legal obligation to oversee an organization's compliance program. If they fail to do so, individuals on the board could be found personally liable. The most important thing that the board of directors can do to protect themselves, and their organization, from legal liability is to solicit a compliance expert to be on their board and become well versed on compliance themselves, including their oversight responsibilities.

CFO

Making an ROI Case for Compliance

86% of healthcare compliance professionals reported that their organization’s compliance program had prevented one or more incidents in the last two years, according to a joint survey taken by HCCA and SCCE.

Just one compliance incident can cost your organization millions in legal and compliance expenses. By proactively investing in compliance, your organization can potentially avoid devastating costs while protecting your reputation and bottom line.

Case Study

Nationwide Cancer Care Provider Settled for 20 Million Dollars

A nationwide provider of integrated cancer care services that is headquartered in Fort Myers, Florida., settled with the DOJ for $20 million dollars reported Justice.gov. The allegations against the provider included billing for medically unnecessary laboratory tests known as FISH (fluorescence in situ hybridization) tests.

“Today’s settlement demonstrates our unwavering commitment to protect the Medicare trust fund against unscrupulous providers. Providers who waste taxpayer dollars by billing for unnecessary services will face serious consequences.” Said Principal Deputy Assistant Attorney General Benjamin C. Mizer, head of the Justice Department’s Civil Division, wrote Justice.gov.

The settlement resolved allegations that the provider submitted medically unnecessary claims to Medicare and Tricare for FISH, tests, a urine tests used to detect genetic abnormalities associated with bladder cancer. All of the tests were ordered by four physicians.

“These tests were ordered to increase profits, not improve the healthcare of patients,” said Special Agent, Shimon Richmond of the Department of Health and Human Services Office of Inspector General (HHS-OIG), according to justice.gov. “This kind of unvarnished fraud is an attack on Medicare by unscrupulous providers and the OIG and its federal partners will take whatever steps are necessary to stop them.”

Government ROI

There’s no denying it, the government is dedicated to combating healthcare fraud and noncompliant healthcare organizations will lose money. According to Justice.gov, the government recovered $2.9 billion under the False Claims Act in Fiscal Year 2024. FY 2024 also recorded the highest number of qui tam actions (aka whistleblower lawsuits) which accounted or $2.4 billion of the $2.9 billion recovered that year.

It's not just healthcare organizations that need to worry. There are consequences for individuals working in an organization found guilty of fraudulent activity. The Civil Monetary Penalties Law gives the Office of Inspector General (OIG) the authority to seek civil monetary penalties (CMPs), assessments, and exclusion against an individual or entity based on "a wide variety of prohibited conduct," according to the OIG. The CMPL is an alternative or companion case to a criminal or civil healthcare fraud action that can apply to physicians, owners, or executives when there is preponderance that they either knew, should have known, or had actual knowledge, deliberate ignorance or reckless disregard of wrongdoing. The OIG has authority to exclude individuals and entities from participating in federal healthcare programs.

The various states' Medicaid Fraud Control Units also report the dollar amount of recoveries from the result of their work. In their fiscal year 2024, they reported $7.13 billion in expected recoveries and receivables. This equates to an ROI of $3.46 for every $1 they spend on recovery efforts.

Finding Value in Compliance Culture

Healthcare organizations with an organizational culture that values compliance are more likely to have effective compliance programs and, thus, are better able to prevent, detect, and correct problems. Plainly put, preventing compliance incidents protects your revenue.

Building and sustaining a successful compliance program is unique to each and every organization. However, such programs generally include: The commitment of the organization's governance and management at the highest levels; structures and processes that create effective internal controls; and regular self-assessment and enhancement of the existing compliance program.

The Bottom Line: Cost Avoidance Equals Long Term Revenue

Just one compliance incident can financially devastate your organization. By investing in compliance, you can prevent revenue loss and a PR nightmare that will further impact your bottom line. Cost avoidance keeps revenue where it belongs: within your organization.

Privacy & Security Officers

Protecting PHI

Privacy and Security professionals are integral players in compliance. They ensure that an organization meets compliance requirements that have been legally mandated and are relevant to the privacy and security of patient information. This has proven to be a challenge in an industry where legislative and regulatory environments are constantly changing. For example, and probably the most notable, the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA).

The HIPAA privacy rule launched a new era of privacy compliance. Prior to the HIPAA privacy rule, healthcare providers were primarily governed by the privacy laws of their state. These laws often focused on highly sensitive information such as behavioral health and HIV/AIDS. Although federal privacy laws existed, they were mostly limited to the Privacy Act of 1974 as well as the protection of substance abuse information, neither of which broadly affected health information. Although the Privacy Act of 1974 is expansive, it only governs federal agencies and contractors, and is therefore not applicable to many healthcare providers.

Case Study

Anthem Health: $115 Million Data Breach Settlement

Anthem, the largest health insurance company in the US, settled a class action lawsuit for a record $115 million as a result of a data breach. Hackers gained access to Anthem's IT system and stole personal information from 78.8 million employees and members, both past and current. They stole the names, birthdates, Social Security numbers, addresses, and other information of tens of millions of people.

The Anthem settlement is the largest to date. As part of the deal, Anthem will offer two years of credit protection to affected individuals. The company has also agreed to set aside funding for cybersecurity improvements, including improving its current systems. $15 million from the settlement will be designated to pay plaintiffs for out-of-pocket costs due to the breach.

"As we have seen in cyberattacks against governments and private sector companies including Anthem over the past few years, many cyber threat actors are increasingly sophisticated and determined adversaries." Anthem wrote in a statement, "Anthem is determined to do its part to prevent future attacks."

Hackers Targeting Healthcare

88% of all ransomware attacks in the U.S. last year targeted the Healthcare Industry. Why? Healthcare organizations are in a precarious position and generally pay the ransom for ransomware attacks.

According to a recent report () in 2024, the average cost of a cybersecurity breach for a healthcare organization was $10 million in 2024. The same report confirmed that 83% of respondents reported a material security breach with 50% of those within the last year and 75% within the last 18 months.

5 Best Practices for Protecting ePHI

There are a number of controls and solutions that are crucial to protecting ePHI and they become increasingly important as the OCR announces higher fines for violations related to breaches.

1. Ditch Your Weak Passwords

The HIPAA Security rules require covered entities and business associates to provide a "unique identifier" of all users in its information systems. There's also a rule related to "authentication," which ensures that a person using a computer is a) who they claim to be and b) the use is appropriate for that individual. In healthcare, more often than not the method used for authentication is a username and password. While authentication is important for security, it can make difficult demands on users. Many users need to memorize half a dozen usernames and passwords or more. And for security purposes, passwords should be complex so that they're not easily guessed or subject to a breach by dictionary attack and other brute force methods.

The ideal method that organizations can use to reduce the need for multiple passwords is two-factor authentication with single sign-on (2FA/SSO). In fact, 2FA/ SSO is a control that can simultaneously improve security and workflow because using more than one factor (2FA) for authentication is always more secure. A bank ATM card uses two factors: something you know, a PIN, and something you have, an ATM card. Single sign-on is a method that uses software to log into and authenticate multiple systems with the use of one very secure authentication method (2FA for example). When SSO is combined with 2FA, it can greatly reduce the number of passwords that need to be memorized down to just one. And because it's only one, it can be a complex password.

2. Conduct a HIPAA risk analysis

Risk analysis is the cornerstone of any HIPAA Security compliance program. It's the very first security safeguard (within the security management process standard) and is also required under the HIPAA Security Rule. Risk analysis is important and given prominence because it's the rule that requires covered entities to proactively discover and document the "risks and threats to the confidentiality, integrity and availability of ePHI," so they can be properly identified and mitigated. It's the rule that holds covered entities accountable for ignorance. Failure to conduct an appropriate risk analysis is one of the most commonly cited areas of non-compliance by the OCR when announcement settlements and corrective action plans.

3. Secure Email And Texting

Many providers use email and texting to conduct business but are not aware that there are special requirements and rules governing their use. The HIPAA Technical standard requires that data must be encrypted during transmission as required under the Transmission Security standard. Encryption is the requirement that is missing in many covered entities use of email and text messaging while conducting business. The specification requiring encryption of transmitted ePHI is "addressable." Addressable specifications, as compared to "required" safeguards, must only be implemented if "reasonable and appropriate." However, given the ready availability of cost-effective solutions for encryption of email and text messages, this safeguard is reasonable and appropriate for almost all covered entities and business associates that use these means to transmit ePHI.

There are two types of services available for encrypting emails. On-demand and automated. On-demand services are ideal for smaller practices that don't send much email or only send ePHI via email sporadically. An on-demand service requires the user to be aware of the content they are sending that would require encryption and know how to encrypt it. Automated services check the contents of emails and attachments against a "library" of known terms, phrases, numbering systems and checks it for possible HIPAA content. If PHI is found, the system can be set to automatically encrypt the email, flag it for review later, or return it to the sender.

HIPAA compliant texting solutions are also widely available. In addition, messaging apps available for iPhones and Android phones provide encryption. For example, iMessage, the native messaging app, provides end-to-end encryption when sending messages to another iPhone user with iMessage enabled. WhatsApp, a third-party app, owned by Facebook, provides end-to-end encryption across platforms. A WhatsApp message sent from an iPhone to an Android phone will be encrypted from the sender's device and decrypted by the recipient's device. And, as an added bonus, WhatsApp is free. However, user beware. WhatsApp might be considered a business associate under the rules. Many covered entities are better served by going with a vendor that actively services the healthcare industry.

4. Ongoing Training

Training is a HIPAA requirement addressed in 45 CFR §164.530(b)(1) under the privacy rules and 45 CFR § 164.308(a)(5)(i) under the security rules. Training is a crucial component of any HIPAA compliance program because it helps mitigate the greatest risk to privacy and security: the human element. Regulations require covered entities to provide training so that workforce members can understand how HIPAA impacts employee's performance of their duties, so they can understand how to conduct those duties consistent with their job. The rules don't specify how training should be conducted, however, they do briefly describe what topics should be included in the training. Ideally, training content should be policy specific. Many organizations fail to provide initial HIPAA training or orientation. Even more, fail to provide ongoing or recurring training. But I've known a few organizations that developed and maintained their own training programs very successfully.

A simple way to implement training is to subscribe to a monthly HIPAA newsletter. Repurpose the content into monthly mandatory fifteen minute in-services. Log the participation and provide a short quiz that attendees take to ensure mastery of the material. The process of ensuring that all employees are receiving training and that participation is documented can be burdensome for many practices and hospitals. A solution to help manage and automate training requirements can help overcome these constraints.

5. Encrypt Your Fat-Client

A fat-client application loads an application on a local workstation and talks to the server to upload the databases with new data as it enters the software. Sometimes the data is stored on the hard drive of the client, especially if the client is not consistently connected to the network, then it syncs or uploads the data when a connection is established. This model is still quite common in some care settings, such as home health, since a network connection cannot always be established with a server for field caregivers. But in most care settings, a fat client application has a persistent connection and data is constantly being "written" to the server rather than storing it locally. However, a large concern with fat client applications is that most client server applications will cache data locally, i.e., it will save data into a temporary folder. If your organization is using fat-client applications, it's crucial to encrypt all workstations and laptops, even if the data is being saved to a server.

Encryption is usually extremely secure but it can sometimes affect the performance of applications, increase the boot-time of workstations and increase the latency, the time required to "paint" a screen once the "enter" or "save" key is used. A good alternative to full disk encryption is virtualization. Hardware and software can be "digitized" so that a digital version, exactly like the analog version, can be used. The virtual version is saved on a server and is accessed via a workstation with software to "invoke and use" the virtual version of the workstation. There are many advantages to a virtual desktop environment (VDE) such as easier access, simple restoration, and virtual environments are much more secure because ePHI and other sensitive data is always saved to the server where the virtual workstation exists.

The Bottom Line: Avoid Financial Pitfalls by Protecting ePHI

These five controls and solutions are crucial to protecting ePHI. As the OCR announces higher fines for violations related to breaches, it's more important than ever to improve the overall security of your organization. Remember, security controls are both Technical and administrative so to protect your organization, it's necessary to implement these five solutions, conduct risk analysis, and stay on top of training.

HR Directors

Onboarding in Compliance

Human resources (HR) is at the center of most healthcare organization's efforts to identify, hire and retain the right people the organization needs to achieve its goals. All roads start with HR, and that's why HR is a key player within the organization's compliance structure.

All federal and state healthcare programs are prohibited to pay for any item or service furnished, ordered, or prescribed by an OIG excluded individual or entity. Including prescriptions for medications and administrative or management services provided by the excluded individual. HR can prevent OIG fines and penalties by screening new hires against the exclusion list.

Case Study

Employing Excluded Individuals

The OIG requires healthcare organizations to neither hire nor do business with individuals or entities on the List of Excluded Individuals/Entities (LEIE). The OIG is required by law to exclude individuals and entities convicted of, amongst other criminal offenses:

- Medicare or Medicaid fraud,
- Patient abuse or neglect
- Felony convictions relating to unlawful manufacturing, distributing, prescribing, or dispensing of controlled substances

If an individual or entity is excluded, they are prohibited from participating in reimbursements for or from federally funded healthcare programs. And anyone who hires an individual or entity on the LEIE may be subject to civil monetary penalties. Below are some examples of such penalties.

⚠ After it self-disclosed conduct to OIG, Leroy R. Polite, D.M.D., P.A., d/b/a Economy Dentures and Economy Dentistry (Economy Dentures), Florida, agreed to pay $279,135 for allegedly violating the Civil Monetary Penalties Law. OIG alleged that Economy Dentures employed an individual that it knew or should have known was excluded from participation in Federal healthcare programs (OIG. HHS.Gov).

⚠ After it self-disclosed conduct to OIG, Apex Dermatology and Skin Surgery Center, LLC (Apex), Ohio, agreed to pay $125,070.71 for allegedly violating the Civil Monetary Penalties Law. OIG alleged that Apex employed an individual that it knew or should have known was excluded from participation in Federal healthcare programs (OIG.HHS.Gov).

In addition to monitoring for excluded individuals, employee onboarding is the best way to get the most out of your employees as quickly as possible. Effective onboarding can also be a useful tool for compliance. Integrating compliance into your onboarding process creates positive habits and total employee buy-in to your compliance culture.

Onboarding Checklist

8 Opportunities to Create a Culture of Compliance

Human resources (HR) is at the center of most healthcare organization's efforts to identify, hire and retain the right people the organization needs to achieve its goals. All roads start with HR, and that's why HR is a key player within the organization's compliance structure. HR can prevent OIG fines and penalties by screening new hires against the exclusion list.

1. Hiring:

Creating a culture of compliance starts with hiring the right person in the first place. Skills and education are important, but in the world of compliance, personality and adherence to company culture is equally as important.

- □ Hire a compliance-minded individual.
- □ Include the compliance culture of your organization in the job description.
- □ When conducting reference checks make sure to ask about the potential employees adherence to compliance guidelines.
  Screen new hire names in the OIG Exclusion Database.

2. Orientation:

Make compliance an important conversation during new hire or employee orientation.

- □ During orientation applicable employees should be required to spend time training with billing personnel to learn how to appropriately enter patient demographics and observe them working denied claims.
- □ Show the protocols followed in order to correct registration errors, and the financial impact caused by delaying the claim.

3. A Warm Welcome:

Send a welcome package to your new team member. Employees who feel valued are more likely to value their jobs and in return are more likely to follow rules and compliance protocols.

- □ Include a kind letter

- □ Important paperwork
- □ Employee handbook
- □ Benefits
- □ Code Of Conduct

4. Training:

Your employees cannot do what they have not been taught. For an effective compliance program, take the time to train new employees in your compliance policies and standards.

- □ Appoint a compliance mentor for all new hires.
- □ Give the mentor a cheat sheet with tasks to cover for the first day and week.
- □ Make sure that during this time the mentor runs through compliance best practices, and explain all of the responsibilities for maintaining the integrity and accuracy of EHR information such as:
  - □ Personal responsibility for protecting system access information
  - □ Creating accurate records
  - □ Notifying management of problems that are discovered
  - □ Covering the proper use, features, and functions of the EHR system,
  - □ Address methods for preventing erroneous entry of information and the importance of preventing errors.
  - □ Cover penalties for falsifying any organizational records.
  - □ Provide instruction on how to use the system security features to prevent unauthorized access to systems.
- □ Inform all EHR users that their activities are being logged by the system.

5. Create an onboarding folder:

Give new employees a tangible compliance tool.

- □ Have a compliance officer create an onboarding folder for new team members.
- □ Include a compliance checklist.
- □ Include a FAQ compliance page.

6. Get staff involved:

Turn the entire staff into an educational tool. Getting staff involved also reminds staff of important compliance protocols on a regular basis. While they help the new employee, they're also getting a refresher course.

- □ Make a new hire announcement to introduce new staff to co-workers.
- □ Encourage the staff to help the new team member to correctly follow organizational guidelines for compliance best practices.
- □ Send out an email reminding employees how they can help newcomers embrace and follow compliance guidelines.

7. Expectations:

Don't leave new hires to figure out the organization's culture and rules on their own.

- □ Create a list of expectations. Make sure to cover:
    - □ Preferred methods of communication
    - □ Decision making processes
    - □ A new hire checklist for what employees are expected to do daily, weekly, and monthly for the first few months.
- □ Compliance officers can include organization-wide policies for the ethical, lawful, and regulatory use of EHRs.

8. Check Up/Check In:

Remember that starting a new job can be overwhelming. Make new employees feel comfortable asking any and all questions, especially related to compliance protocol.

- □ Schedule a meeting after the first day to give them a chance to ask questions.
- □ Follow up the first meeting at the end of the week.
- □ Schedule another meeting after two weeks. This is usually how long it takes new hires to really understand the new company and how things work.

The Bottom Line: HR Plays an Integral Role in the Culture of Compliance

HR plays an integral role in compliance by monitoring exclusion lists for new hires and onboarding new employees into your organization's compliance initiatives. Onboarding is a seamless, efficient way to ensure that the full spectrum of your compliance program is understood and embraced right from the beginning, and always.

In Conclusion: Maintaining Compliance And Your Bottom Line Takes a Village

Implementing an effective compliance program will significantly reduce your risks of fraud, abuse and waste and increase revenue by avoiding costs associated with fines and lawsuits. When your organization is compliant, members of your organization can do what they do best, take care of patients.

In order to maintain compliance, every employee in your organization, the CFO, Board of Directors, Security and Privacy Officers, HR, and Physicians, must come together with a common goal. Every department plays an integral role in your compliance goals.

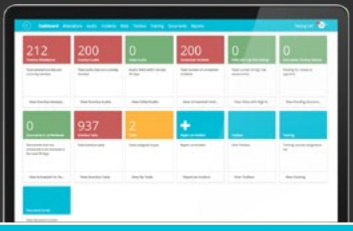
AUTHOR BIO

CJ Wolf MD, CHC, CPC, CCEP, CIA

CJ Wolf is a healthcare professional with more than 25 years of experience in hospital and physician revenue cycle, practice management, compliance, coding, billing, and client services. He has been providing healthcare consulting and solution services to hospitals and physician organizations throughout the country.

For more on Healthicity's Compliance Services and Solutions, please visit healthicity.com/compliance or call 877.777.3001

Compliance Manager



WATCH ON-DEMAND DEMO

Resource Center

How To Effectively Communicate Compliance Reports

By Brenda Chidester-Palmer, CPC, CPC-I, CCS-P

EXPLORE FREE RESOURCES

Healthicity

Learn more at
www.healthicity.com/compliance
877.777.3001