WHITE PAPER SERIES

Healthicity

The Seven Keys to Compliance

CJ Wolf MD, CHC, CPC, CCEP, CIA

The Seven Keys to Compliance

Summary

An effective compliance program is essential for every healthcare organization. Compliance programs not only meet legal and contractual requirements but also help ensure efficient operations and financial security. In this white paper, we outline a step-by-step plan to help your organization create a compliance plan that is in accordance with the seven elements recommended by the OIG.

Creating an Effective Compliance Program

An effective compliance program is essential for every healthcare organization. Compliance programs not only meet legal and contractual requirements but also help ensure efficient operations and financial security.

Compliance programs are often formalized as a written compliance plan that details specific protocols and procedures. A complete compliance program must encompass a number of areas, from appropriate submission of healthcare claims to workplace safety, and from fair labor practices to the protection of patient health information. In some cases, organizations are required to implement compliance safeguards. For example, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities enact specific administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of electronic protected health information (ePHI)[1]. In other cases compliance efforts are voluntary, though government agencies responsible for oversight recommend a series of core elements to ensure compliance best practices.

Regarding medical claims submission and payment, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) has outlined several model compliance programs specific to provider/organization type and size[2] in order to help providers minimize post-payment recoupment and civil or criminal false claims risk. Healthcare organizations would do well to heed these models as government entities and private insurers aggressively monitor claims in their effort to curtail healthcare fraud, waste, and abuse (FWA) and to aid in the recovery of improper payments. Outstanding returns on investment of these improper payments have further incentivized payers and government entities to expand their recovery efforts.

> "For Every $1 Spent, the Federal Government Recovers $8.10"

From early 2011 to early 2014, the Federal government has recovered $8.10 for every dollar it spent on healthcare-related FWA investigations.[3] The Department of Health and

Human Services (HHS) Office of Inspector General (OIG) expects to return $4.9 billion to the government for fiscal year (FY) 2014,[4] surpassing previous record recoveries in 2012 ($4.2 billion) and 2013 ($4.3 billion).[5]

In addition to returning overpayments, providers may potentially face substantial civil, criminal, and financial penalties for fraudulent or abusive coding and billing. Under the False Claims Act (FCA), penalties can total three times the amount of the claim, plus fines of $11,000, per claim. Three recent settlements under the FCA include:

- A chain of addiction treatment clinics and a clinical laboratory in Kentucky paid $15.75 million to settle allegations that they fraudulently billed for medically unnecessary and excessive urine tests.[6]
- A Baltimore billing company paid $3.3 million to settle false billing allegations, including allegations that their coders reported each service twice, inappropriately using a CPT® modifier meant to indicate that the same physician performed the service twice.[7]
- Duke University Health System paid $1 million to settle allegations it submitted false claims based upon unbundling physician assistant services.[8]

To underscore the importance of incorporating a compliance program, consider that healthcare entities may be held liable for the conduct of its individual employees or contracted entities—regardless of whether the organization has actual knowledge that either was engaged in the preparation or submission of fraudulent claims.[9]

COMING SOON: MANDATORY FWA COMPLIANCE

The Patient Protection and Affordable Care Act (ACA) §6401 directs the Secretary of HHS to implement screening requirements for new and existing providers. The ACA also directs the Secretary to establish a timeline to require formal compliance plans as a condition of Medicare enrollment; however, the ACA gives the Secretary the flexibility to designate an appropriate timeline based on the type of provider or supplier within a particular industry or category.

In a September 2010 proposed rule, HHS OIG asked for comments regarding the potential use of seven elements described in Chapter 8 of the 2010 U.S. Federal Sentencing Guidelines Manual (FSG)[10] as the basis for establishing the requisite core elements mandated by §6401. To date, HHS has not addressed the core elements in the final rulemaking for medical practices, suppliers, and billing companies. Given the ACA directive that the Secretary develop core elements in consultation with the HHS OIG, the eventual core elements will likely mirror those provided by the HHS OIG in its model compliance guidance, which provide elements specific to the entity type.[11]

THE SEVEN KEYS TO COMPLIANCE

Pending the need for a formal compliance plan, practices should consider the FSG Chapter 8 elements as a starting point. Practices should also look to the HHS OIG's compliance guidance, which outlines a variety of core elements depending on the type of entity.[12] For each entity type, seven core elements are identified. Although the core elements are similar for the various facility entities, OIG modified the guidance for physician and small group practices. This departure was based on OIG's "recognition of the financial and staffing resource constraints faced by physician practices."[13]

OIG has established the following seven core elements of a compliance program for facility-based entities:

1. Implementing written policies, procedures and standards of conduct;
2. Designating a compliance officer and compliance committee;
3. Conducting effective training and education;
4. Developing effective lines of communication;
5. Enforcing standards through well-publicized disciplinary guidelines;
6. Conducting internal monitoring and auditing; and
7. Responding promptly to detected offenses and developing corrective action.[14]

By comparison, the seven recommended components applicable to physician and small group practices include:

1. Conducting internal monitoring and auditing;
2. Implementing compliance and practice standards;
3. Designating a compliance officer or contact;
4. Conducting appropriate training and education;
5. Responding appropriately to detected offenses and developing corrective action;
6. Developing open lines of communication; and
7. Enforcing disciplinary standards through well-publicized guidelines.[15]

To ensure compliance and avoid harsh penalties and fines, entities of all size, should create and maintain compliance programs based on the OIG's seven core elements.

So that we might better understand the complexities of a compliance program, what follows is a detailed accounting of how practices can avoid pitfalls and initiate a plan for their own successful compliance program using the seven core elements.

1. IMPLEMENTING POLICIES, STANDARDS, AND PROCEDURES.

The first step to achieving compliance is: Have a plan. Policies, standards, and procedures prevent ambiguity and indecision and demonstrate a good faith effort to achieve compliance. Through staff awareness, standards and procedures reduce the prospect of fraudulent activity by establishing tighter internal controls to counter potential risks.

For smaller practices, a more informal approach may be appropriate according to the OIG model guidance. Even absent the formality of specific procedures, written policies that outline the goals of the practice's compliance program efforts can be beneficial.

The OIG expects healthcare organizations will enact, at minimum, standards and procedures to prevent erroneous or fraudulent conduct in the following areas:[16]

- Coding and billing
- Reasonable and necessary services
- Documentation
- Improper inducements, kickbacks, and self-referrals

To accommodate regulatory or organizational changes update your policies, standards, and procedures annually–or more frequently when regulatory or staffing changes occur. Practices must also devise a means to manage such revisions and archive out-of-date policies to ensure the most recent guidelines are readily available.

Many healthcare organizations have policy binders gathering dust on a shelf. This is not only ineffective, but also potentially harmful because non-compliance with the mandates of a written plan on-hand could translate to greater exposure to FWA risk. Regardless of whether procedures are written down, in order to make a compliance program's efforts effective, there must be a system in place to remind you when actions are due and a method for tracking those efforts.

Where formal policies, standards, and procedures are implemented, look beyond policy binders to software solutions that allow for easy communication and maintenance. Establish a central library of policies, standards, and procedures that allow you to create, update, share, approve, and archive these important documents. Link policies, standards, and procedures to laws and regulations and make them readily available and easily accessible to everyone in the organization. Enact a system of alerts to trigger reminders to update policies, standards, and procedures, when needed.

An organization's Code of Conduct reflects its commitment to comply with healthcare program requirements and outlines employees' obligations to report concerns without fear of retaliation. Present this document to each person in the organization to outline the expected behaviors and rules everyone must follow.

2. DESIGNATING A COMPLIANCE OFFICER AND COMPLIANCE COMMITTEE.

Compliance should be a job requirement for every member of your organization; however, to ensure the effectiveness of your program and to establish individual accountability you should designate a compliance officer. The compliance officer's primary function is the upkeep, oversight and implementation of the compliance program. He or she must be sufficiently trained to assess potential risks, follow through with the source of the concern and, where necessary, implement corrective action. Where the resources of a physician or small group practice do not permit the practice to hire such a person, designation of a compliance contact with appropriate training and certification is appropriate. For smaller practices it is also permissible to contract with a qualified organization or individual to act as the compliance officer.

- A partial list of a compliance officer's job duties include:
- Responsibility for development of the corporate compliance program
- Review all relevant documents, perform, and coordinate an organization-wide audit, and review all areas of possible noncompliance within the organization
- Periodically review and update the compliance program, and for dissemination of any changes to the employees and agents of the organization
- Develop, coordinate, and/conduct the necessary training programs for all members of the healthcare organization
- Coordinate and/or develop policies and programs for reporting noncompliance issues

If your organization is large enough to establish a compliance committee, the compliance officer will be the chairperson and will coordinate member responsibilities. He or she also conducts or coordinates internal and external compliance audits; initiates and/or coordinates corrective and preventive action for areas of noncompliance; screens employees, agents, and independent contractors, and; generally handles all aspects of your compliance program, including the development of a compliance budget.

Entrust your compliance officer with the authority and resources necessary to carry out the duties required of the position. He or she should have the full support of management and answer directly to the CEO and board of directors as it is vital to

The OIG outlines three steps for educational objectives:[17]

- Determine who needs training, by job description and duties. Various aspects of compliance may apply more readily to some aspects of your organization, than to others. For example, the training appropriate for a coder or back-office biller may differ from that appropriate for clinicians, which will differ from that appropriate for human resources, and so on.
- Determine the type of training that best suits the organization's needs (e.g., seminars, in-service training, self-study, or other programs)
- Determine when and how often education is needed, and how much each person should receive

the organization's health that leadership be involved in the compliance program and ongoing activities.

3. CONDUCTING EFFECTIVE TRAINING AND EDUCATION.

Educate all personnel, employees, leadership, and agents of the organization on the significance of the compliance program. Everyone should know the goal is to ensure a culture of compliance within the organization.

Compliance training is recommended for new employees soon after they start and at least annually thereafter. Initial training should include complete education regarding the organization's compliance program. Typical topics will include the operation and importance of the compliance program, the consequences of violating the standards and procedures set forth in the program, and the role of each employee in the operation of the compliance program. Specific areas of training may include:

- Federal and State FWA laws
- Coding and documentation
- Duty of employees to report misconduct
- Non-retaliation policy for good faith reporting
- Stark and Anti-kickback statutes
- Specific job functions applicable to employees

Consider using a variety of teaching methods, such as:

- Interactive training
- In-person training sessions
- One-on-one training
- Group training
- Monthly newsletters or bulletins

Regardless of the training modality, ensure that education leads to a better understanding. This may mean editing education that is too long or confusing.

As you identify potential areas of weakness in your organization (discussed further, below), educate providers and staff about your findings and how to minimize vulnerabilities going forward.

Document all training and keep copies of any training materials. Maintain a training log and an attestation from the employee that he or she has received and understands the training. An organization will have greater protection if it can demonstrate that it provided employees with proper training and that employees have attested to the training.

Many offices now use online training software, whereby staff attests to the training by completing a test or quiz. The benefits include not only the ability to track all training assignments by due date, but also to identify quickly those employees who are overdue for training and those who have passed versus failed the training. Such a system allows everyone in the organization unlimited access to training materials and provides a convenient means to update policies and to alert every one of any changes.

The seven elements of an effective compliance program, as described here, are recommended for FWA compliance, but are also applicable to other compliance efforts. For example, training and education may cover compliance concerns beyond coding and billing, including Federal and State employment laws and regulations, HIPAA, and Occupational Safety and Health Administration (OSHA) requirements.

4. DEVELOPING EFFECTIVE LINES OF COMMUNICATION.

Healthcare organizations should cultivate open lines of communication and insist on a non-retaliation policy encouraging employees to participate in policing the organization and report non-compliance activities without fear of reprisal. Compliance is a group effort, requiring buy-in and vigilance from every member of your organization.

Effective communication starts with a culture that values ethics and doing the right thing. To help create such a culture, implement policies and training that:

- Require employees to report conduct that is erroneous, improper, or potentially fraudulent
- State that failure to report erroneous, improper, or potentially fraudulent behavior is a violation of the compliance plan and can lead to disciplinary action
- Identify methods that allow for anonymity
- Clearly state there will be no retribution for reporting improper conduct

Management must encourage this behavior by following these same policies.

> “Compliance is a group effort, requiring buy-in and vigilance from every member of your organization.”

Designate a method for employees to report an incident, including an option to report anonymously. Best practices for anonymous reporting include establishing a hotline, having a drop box, or using a third party, intra-office mail, or information sent via U.S. Postal Service.

Establish an effective tool to track and follow through with incident reports. Without a process to manage incident reports, it is possible to lose track of a reported issue that might expose your organization to significant liability. Also, without follow through, the benefits of open communication will not be realized. A frustrated employee may be motivated to turn outside the organization for satisfaction. In many cases, the decision by an individual to become a whistleblower, or qui tam relator, is made only after their concerns were ignored or not investigated properly.

Incident reports might encompass anything from an employee noticing that someone at the front desk is discussing a patient's protected health information (PHI) too loudly (a HIPAA compliance concern), to a biller in the business office noticing the improper use of a code for services performed (a coding compliance concern). Some reports will require minor staff education or policy updates; others may require full investigations including audits, disciplinary actions, self-reporting to CMS, or even refunding payments that were inappropriately billed.

It is possible that some concerns will be unfounded. In these cases, follow-through is especially important because it lets employees know their concerns were heard and evaluated and provides an opportunity to further educate staff.

Tools for managing incident reports range from Excel spreadsheets to paper files in a drawer to software solutions. A good compliance solution should effectively track incident reports, the investigations of the reporting, and all required follow-up actions. Effective tools allow not only for reporting and tracking of an incident but also the organization of investigations and follow-up assignments by offering reminders and task tracking.

Regular employee evaluations, as well as exit interviews with staff who leave, can help to identify compliance vulnerabilities. Employees may reveal concerns about a potential compliance issue during a performance evaluation, for example. Individuals will often divulge information when exiting they may not have been willing to reveal previously. Use a checklist when conducting employee interviews as a reminder to cover all relevant points. Include questions regarding any known activity of non-compliance in the interview checklist. This simple step can be important to minimize the risk of a former employee becoming a Qui Tam relator ("whistleblower"), in the future.

The purpose of open communication is to ensure that the entity has the benefit of everyone's eyes and ears to identify and correct compliance vulnerabilities. When a concern is identified, be sure to communicate the results—including any protocols developed to correct identified risks—to relevant staff, board members, and vendors. Completing this communication loop not only demonstrates the organization's commitment to compliance but also allows the appropriate parties to learn from the issue.

> "Systematic, consistent, and organized documentation of audits is required when managing an audit process."

5. CONDUCTING INTERNAL MONITORING AND AUDITING.

Periodic audits are essential to assess the effectiveness of your compliance protocols, educational efforts, and corrective actions. A Standards and Procedures audit enables you to determine whether office policies and day-to-day processes are in compliance. A claims submissions audit can determine whether physicians and staff are submitting claims in accordance with federal rules and payer policies. Implementing plans for corrective action and to prevent non-compliant activities from reoccurring will mitigate the potential of a large overpayment disclosures and refunds and of possible penalties and sanctions.

Systematic, consistent, and organized documentation of audits is required when managing an audit process. Establishing an annual audit work plan will help to schedule, track, and manage reoccurring audits. The work plan helps to organize ongoing efforts and can be an important resource when conducting an annual risk assessment (discussed further, below).

To begin, determine which standards and procedures apply to your organization. For example, information for proper documentation, billing, and coding for Medicare can be found on the CMS website (www.cms.gov). For private payers, the information can be found in your payer contracts. Most payers also make coverage and payment policies available on their websites.

In addition to the OIG-identified risk areas (coding and billing, reasonable and necessary services, documentation, improper inducements), consider these possible risks:

- Data entry accuracy
- Sufficient documentation to validate medical necessity consistent with carrier coverage and reimbursement standards
- Compliance with carrier documentation content standards
- Legibility
- Signatures
- Cloning/copy and pasting

Additionally, the OIG and the state's office of Medicaid Inspector General (OMIG) publish Work Plans[18] that inventory the vulnerabilities and risk areas they are targeting, each year. The OIG also publishes alerts[19] and advisory opinions.[20] Monitor these alerts, opinions, and annual work plans to identify potential vulnerabilities in your organization.

Finally, you may wish to informally interview staff to gauge their knowledge and determine topics for further audit focus or staff education.

6. ENFORCING STANDARDS THROUGH WELL-PUBLICIZED DISCIPLINARY GUIDELINES.

Employees should understand that all incidents will be investigated and the consequences if they behave in a non-compliant manner. As a condition of employment, specify that any individual who violates the law, organizational policies, or guidelines described in the Code of Conduct and Compliance Manual—including the duty to report suspected violations—are subject to disciplinary action, including immediate termination. Additionally, adherence to compliance and ethical standards should be a part of job performance evaluation criteria for all personnel.

Your compliance officer is responsible to ensure all reports of non-compliant behavior are thoroughly investigated, documented, and resolved, and that disciplinary actions are taken by appropriate management and administrative personnel. Refer situations involving possible litigation or other legal action to legal counsel.

When faced with adversarial attitudes toward compliance activities—which should not be tolerated— seek to demonstrate how compliance efforts strengthen and benefit the organization, patient well-being, and staff and provider performance.

7. RESPONDING PROMPTLY TO DETECTED OFFENSES AND UNDERTAKING CORRECTIVE ACTION.

It is not enough to encourage reporting or auditing to uncover compliance vulnerabilities. In the face of a concern–even one that may be unfounded–it is important to immediately investigate to determine if an incident requires further action. Document the investigative process and the result. Regardless of whether the concern is founded, sharing the results and the corrective actions taken demonstrates the entity's commitment to transparency and its compliance efforts, and lets those with concerns know they are being taken seriously.

> "Failure to return payments puts the healthcare entities at risk of exclusion from the Medicare and Medicaid programs."

The Patient Protection and Affordable Care Act of 2010 (PPACA) requires healthcare providers to return overpayments to governmental payers–with an explanation of why the payment is being returned–within 60 days from the time that the provider identifies the overpayment.[21] According to regulation, an "identified" overpayment occurs when "a person has actual knowledge of the existence of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment."[22]

If an overpayment is retained beyond 60-days it becomes an "obligation" sufficient for reverse false claims liability under the False Claims Act and may become subject to treble damages and penalties if there is a "knowing and improper" failure to return the overpayment. Failure to return the payment within the 60-day window also puts the healthcare entities at risk of exclusion from the Medicare and Medicaid programs.

When commercial carriers are involved, look to your contract for any provision that requires disclosure. Regardless of the existence of such an obligation, the practice must also determine if any state False Claims Act or Insurance Fraud Act provision exists that mandates disclosure. Assistance from competent health law counsel may be necessary to correctly determine your liability. Even where disclosure is not required, voluntary disclosure and refund of monies you are not entitled to—although potentially painful in the short term—demonstrate the organization's commitment to compliance, and minimize the risk of future allegations of fraudulent conduct.

The OIG Self Disclosure Protocol (SDP)[23] allows organizations to self-disclose potential instances of fraud involving federal healthcare programs for which liability arises under the OIG's civil money penalty authorities. The SDP is not for reporting of potential or actual Stark (self-referral) violations, and is not a means to obtain an advisory opinion to determine if conduct is unlawful. For potential or actual Stark law violations, HHS provides a separate disclosure process called the Self-Referral Disclosure Protocol. Where errors result in overpayments for which there was no evidence of fraudulent conduct, an entity must voluntarily identify, disclose, and refund overpayments to avoid False Claims Act (FCA) liability.

OTHER AREAS OF RISK

Additional compliance standards are set forth in the federal Anti-Kickback Statute, the Stark Physician Self-Referral Law, the Exclusion Authorities, the Civil Monetary Penalties Law, the Criminal Health Care Fraud Statute, and more. Undiscovered failures to comply with any of these (or other) laws may lead to significant financial and civil or criminal penalties.

Unlike FWA compliance efforts, HIPAA requires covered entities to have formal policies and procedures that are specific to the entity. Non-compliance can result in severe financial penalties. As updated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, HIPAA violations may result in fines of up to $1.5 million, per year. The HITECH Act mandates that the Office of Civil Rights (OCR) conduct audits to ensure HIPAA compliance. These audits are focused on whether the entity has implemented appropriate policies and procedures as required by the law, suggesting that practices need to review existing policies and procedures and update them accordingly.

A sample of recent settlements under HIPAA include:

- Washington State paid $215,000 to settle allegations that the county's public health department violated HIPAA regulations when patients' data were exposed electronically. This was the first HIPAA settlement involving a county government.[27]
- Concentra Health Services paid $1.7 million to resolve alleged HIPAA violations that included failing to encrypt laptops, desktop computers, medical equipment, tablet computers, and other devices. The case began with the theft of an unencrypted laptop.[28]
- Parkview Health System paid $800,000 to settle HIPAA privacy allegations, including that it left 71 boxes of medical records unattended in the driveway of a retired physician.[29]

CONCLUSION

Compliance is a cost of doing business; non-compliance can spell the end of doing business. By creating a compliance program that adheres to the seven core elements,

THE COST OF COMPLIANCE

In January 2014, CareFusion Corp. paid $40.1 million to resolve allegations that it paid kickbacks to physicians and promoted products for uses not approved by the FDA.24

In April 2014, All Children's Hospital of Florida paid $7 million to settle allegations that physician compensation arrangements violated the Stark law because salaries were above fair market value.25

In February 2015, the Seventh Circuit Court of Appeals upheld a conviction of a medical provider for violation of the Anti-Kickback statute where the government conceded that all of the services were medically necessary and also conceded that the provider did not direct patients to the particular home health agency that paid money to the provider. The certification of home health services and the receipt of money by the HHA chosen by the patient were found to constitute a "referral" sufficient for a violation.26

while being mindful of HIPAA and other standards, organizations will be well suited to identify risks before they occur and cause organizational harm.

As you enact your compliance program, keep in mind:

- A culture of compliance starts at the top. Treating compliance as a partnership, instead of a police action, will help to obtain buy-in from staff.
- A good compliance program that addresses vulnerabilities is analogous to practicing preventative medicine. Identifying and correcting potential vulnerabilities in your practice will speed and optimize proper payment of claims, minimize billing mistakes, reduce chances of an audit by CMS or the OIG, avoid potential allegations of civil or criminal misconduct, and avoid conflicts with Stark and anti-kickback statutes.
- Every practice is unique. "Out-of-the-box" compliance programs, even for your specialty, often do not work. In implementing an effective compliance program, look for tools that help you manage the process rather than those providing you with mere suggestions on policy and procedure content. The ultimate compliance program must be customized to the organization's activities and needs. Be practical, use common sense, and seek the help of experts and good compliance solutions. After you have established a foundation, with the right tools for tracking and management, you can make your program effective.

Finally, remember that compliance is a process, not a result. Implementing an effective compliance program is not about eliminating the potential for all error, but instead compliance is the practice of limiting the potential for significant liability associated with the negligent failure to detect non-compliance. By holding these seven core elements to heart and recognizing additional areas of risk, organizations will be well equipped to minimize risk and avoid financial dangers.

ENDNOTES

1. HIPAA compliance requirements are disscussed at greater length, below.
2. OIG Compliance Guidance: http://oig.hhs.gov/compliance/compliance-guidance/
3. "Departments of Justice and Health and Human Services announce record-breaking recoveries resulting from joint efforts to combat health care fraud," HHS Press Release (Feb. 26, 2014): http://www.hhs.gov/news/press/2014pres/02/20140226a.html
4. "Nearly $5 Billion to be Returned to Taxpayers as a Result of OIG Work in FY 2014," HHS Press Release (Dec. 10, 2014): http://oig.hhs.gov/newsroom/news-releases/2014/sar14fall.asp
5. "Departments of Justice and Health and Human Services announce record-breaking recoveries resulting from joint efforts to combat health care fraud," HHS Press Release (Feb. 26, 2014): http://www.hhs.gov/news/press/2014pres/02/20140226a.html
6. "Kentucky Addiction Treatment Center, Clinical Laboratory and Two Physician Owners to Pay $15.75 Million t Resolve Allegations of Fraudulent Urine Drug Testing," The United States Attorney's Office, Eastern District of Kentucky, Press Release: http://www.justice.gov/usao/kye/news/2014/2014-02-10-premiertox.html
7. "Three Medical Groups And A Medical Billing Company Agree To Pay $3,340,979 To Resolve Investigation Into Medicare Overbilling Scheme," The United States Attorney's Office, District of Maryland, Press Release: http://www.justice.gov/usao/md/news/2014/ThreeMedicalGroupsAndAMedicalBillingCompanyAgreeToPay3340979ToResolveInvestigationInto.html
8. "Duke University Health System, Inc. Agrees To Pay $1 Million For Alleged False Claims Submitted To Federal Health Care Programs," The United States Attorney's Office, Eastern District of North Carolina, Press Release: http://www.justice.gov/usao/nce/press/2014/2014-mar-21.html
9. "...to violate the FCA a person must have submitted, or caused the submission of, the false claim (or made a false statement or record) with knowledge of the falsity. In § 3729(b)(1), knowledge of false information is defined as being (1) actual knowledge, (2) deliberate ignorance of the truth or falsity of the information, or (3) reckless disregard of the truth or falsity of the information." "The False Claims Act: A Primer," United States Department of Justice (http://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf)
10. http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2014/CHAPTER_8.pdf
11. http://oig.hhs.gov/compliance/compliance-guidance/index.asp
12. http://oig.hhs.gov/compliance/compliance-guidance/index.asp
13. 65 F.R. 59434, 59435 (Oct. 5, 2000).
14. 65 F.R. 14289; (March 16, 2000)
15. 65 F.R. 59434, 59435; (October 5, 2000)
16. "OIG Compliance Program for Individual and Small Group Physician Practices," Federal Register, Vol. 65, No. 194 (Thursday, October 5, 2000): http://oig.hhs.gov/authorities/docs/physician.pdf
17. "OIG Compliance Program for Individual and Small Group Physician Practices," Federal Register, Vol. 65, No. 194 (Thursday, October 5, 2000): http://oig.hhs.gov/authorities/docs/physician.pdf
18. https://oig.hhs.gov/reports-and-publications/workplan/
19. https://oig.hhs.gov/compliance/alerts/index.asp
20. https://oig.hhs.gov/compliance/advisory-opinions/
21. Public Law 111–148, Section 1128J: http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf
22. 77 Fed. Reg. 9179, 9182 (Feb. 16, 2012). Medicare Program; Reporting and Returning of Overpayments, proposed rule: http://www.gpo.gov/fdsys/pkg/FR-2012-02-16/pdf/2012-3642.pdf
23. U.S. Department of Health and Human Services: https://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf
24. "CareFusion to Pay the Government $40.1 Million to Resolve Allegations That Include More Than $11 Million in Kickbacks to One Doctor," U.S. Department of Justice Press Release: http://www.justice.gov/opa/pr/carefusion-pay-government-401-million-resolve-allegations-include-more-11-million-kickbacks
25. "Hospital Settles Whistleblower Stark Act Case for $7 Million," Robert M. Wolff: http://www.littler.com/healthcare-employment-counsel/hospital-settles-whistleblower-stark-act-case-7-million
26. U.S. v. Patel, 2015 WL 527549 (February 10, 2015)
27. County Government Settles Potential HIPAA Violations, HHS Press Release: http://www.hhs.gov/news/press/2014pres/03/20140307a.html
28. "Stolen laptops lead to important HIPAA settlements," HHS Press Release: http://www.hhs.gov/news/press/2014pres/04/20140422b.html
29. "$800,000 HIPAA settlement in medical records dumping case," HHS Press Release: http://www.hhs.gov/news/press/2014pres/06/20140623a.html

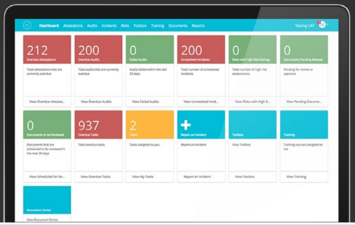
AUTHOR BIO

CJ Wolf MD, CHC, CPC, CCEP, CIA

CJ Wolf is a healthcare professional with more than 20 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