

Combatting Fraud in Healthcare Billing and Payment

Fraud in healthcare billing and payment continues to be a serious risk for payers and providers alike. Billions of dollars are misappropriated every year resulting in increasing costs throughout the healthcare delivery system.

Public and private payers are serious about rooting out fraud, waste, and abuse in the health care system wherever it may occur, given the magnitude of the problem.

Sizing up the Problem

The National Healthcare Anti-Fraud Association (NHCAA) estimates financial losses associated with healthcare fraud at nearly \$100 billion or 3% of the nation's total healthcare spend of \$3.6 trillion. This estimate (as a percent of total healthcare spend) has been steadily increasing over the last decade, driven by several factors.

Healthcare fraud is growing due to a combination of factors including the complexity and often opaque nature of the healthcare billing system, the increasing adoption of electronic health records (EHRs) which can be easily manipulated, the financial incentives for providers to maximize billing, the rise of telemedicine with associated potential for abuse, and the growing sophistication of criminal networks exploiting vulnerabilities in the system.

Most physicians and health care providers work ethically, provide high-quality care, and submit appropriate claims for payment, but there are unfortunately many instances where this is not the case. To address those cases where fraudulent activity takes place, an array of laws has been enacted to combat fraud and abuse and protect the integrity of the health care payment system.

Complex billing system – easily manipulated by providers who may up code services or submit false claims for services not rendered, wherein detection systems have not kept pace with growing complexity.

EHRs – can be used to alter medical records or generate fraudulent claims with relative ease. Availability of patient medical data can be exploited to create fake identities or fabricate medical information.

Organized crime – criminal networks are increasingly targeting healthcare systems due to the potential for large financial gains with relatively low risk of detection.

Telemedicine expansion – rapid growth of telemedicine creates new opportunities for fraud, including billing for non-existent consultations or using fake identities.

<i>The most important laws that apply to physicians:</i>	
<i>False Claims Act</i>	The False Claims Act (FCA) is a federal law that holds people and companies accountable for defrauding the government. It's the main tool the government uses to fight fraud against itself.
<i>Anti-Kickback Statute</i>	Is a federal law that prohibits the exchange of anything of value to influence patient referrals. The AKS is intended to protect patients and ensure that healthcare decisions are based on medical needs, not financial gain.
<i>Physician Self-Referral Law (Stark)</i>	Prevents physicians from referring patients to certain health services if they have a financial relationship with the health service provider. The law aims to prevent conflicts of interest and ensure that patient referrals are based on the patient's best interests.
<i>Exclusion Authorities</i>	Exclusion authorities are laws that allow the Office of Inspector General (OIG) to bar individuals and entities from participating in federal health care programs. These authorities are intended to protect program beneficiaries and the integrity of the programs.
<i>Civil Monetary Penalties</i>	Allows the Department of Health and Human Services' Office of Inspector General (OIG) to impose penalties on individuals and entities that defraud Medicare or Medicaid. The law also authorizes the OIG to exclude individuals and entities from participating in federal health care programs

Medicare, Medicaid, other federal health care programs and private payers rely on the medical judgment of health care providers to treat patients with appropriate services and to submit accurate and truthful claims for the services they provide. Most healthcare providers intend to do just that despite the complex and dynamic nature of payer coding and billing procedures which vary from payer to payer, policy to policy, state to state, and sometimes, month to month. In some cases, inaccurate claims may not be the result of an intentional effort to commit fraud, but moreover a lack of understanding or rigor with regard to applying payment rules to services provided.

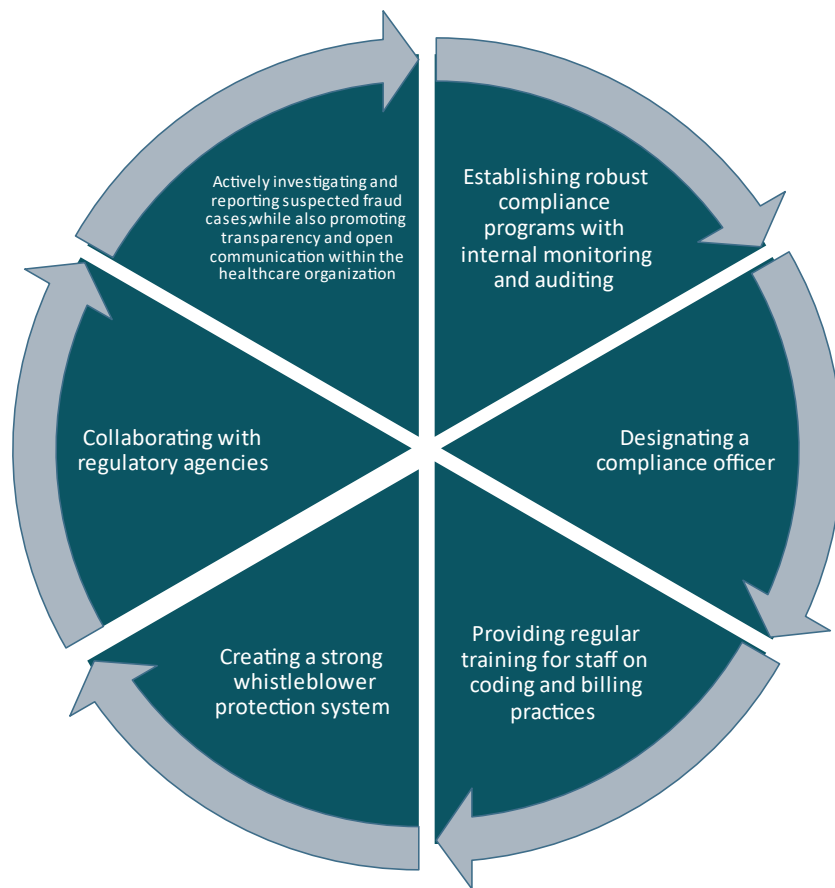
What Constitutes HealthCare Fraud

Healthcare Fraud typically includes any of the following:

- Knowingly submitting, or causing to be submitted, false claims or making misrepresentations of fact to obtain a health care payment for which no entitlement would otherwise exist.
- Knowingly soliciting, receiving, offering, or paying remuneration (e.g., kickbacks, bribes, or rebates) to induce or reward referrals for items or services reimbursed by health care programs.
- Making prohibited referrals for certain designated health services.
- Knowingly billing for services at a level of complexity higher than services actually provided or documented in the medical records.
- Knowingly billing for services not furnished, supplies not provided, or both, including falsifying records to show delivery of such items.
- Knowingly ordering medically unnecessary items or services for patients.

Taking Action to Counteract Fraud

To address fraud in the healthcare industry, organizations should consider implementing a comprehensive approach with elements like internal monitoring, data analysis, regular staff training, clear policies and procedures, and a designated compliance leader and team charged with proactive investigation of suspicious activity.



Key components of a comprehensive healthcare fraud, detection and remediation program should include the following:



Compliance Organizational Components:

- ✓ Develop written compliance policies and procedures covering all aspects of billing and coding practices.
- ✓ Assign a dedicated compliance officer to oversee the program.
- ✓ Conduct regular internal audits to identify potential areas of fraud.
- ✓ Implement a system for reporting suspected fraud.
- ✓ Conduct appropriate training and ongoing education.
- ✓ Respond appropriately to detected offenses and develop corrective action.
- ✓ Develop open lines of communication.
- ✓ Enforce disciplinary standards through well-publicized guidelines.



Staff Training:

- ✓ Provide ongoing training for all healthcare staff on proper coding and billing practices.
- ✓ Educate employees on relevant fraud and abuse laws (e.g., False Claims Act, Anti-Kickback Statute).
- ✓ Emphasize the importance of ethical conduct and reporting suspicious activity.



Whistleblower Protection:

- ✓ Establish a confidential whistleblower hotline for employees to report suspected fraud without fear of retaliation.
- ✓ Clearly communicate whistleblower policies and procedures to all staff.



Data Analysis and Monitoring:

- ✓ Utilize data analytics tools to identify patterns and anomalies that may indicate fraudulent activity.
- ✓ Monitor claim submissions for suspicious billing practices.
- ✓ Regularly review member records for inconsistencies.



Collaboration with Regulatory Agencies:

- ✓ Maintain open communication with relevant government agencies like the Office of Inspector General (OIG).
- ✓ Report suspected fraud cases promptly to the appropriate authorities.



Member Education:

- ✓ Inform members about their rights and how to identify potential healthcare fraud.
- ✓ Encourage members to ask questions about their medical bills and report any discrepancies.

When making determinations about how to focus efforts, the following are supporting considerations:



Being Prepared to Actively Investigate Suspected Fraud:

- ✓ When a potential fraud case is identified, conduct a thorough investigation with appropriate documentation.



Establish Standard in Disciplinary Actions:

- ✓ Implement disciplinary actions for employees involved in fraudulent activities, including potential legal consequences.



Adapting to Changing Regulations:

- ✓ Stay updated on evolving healthcare laws and regulations to ensure compliance.

In addition to establishing an organization structure to combat fraud as described above, here are some further “best practices” as it pertains to ensuring success of these efforts.

Comprehensive Risk Assessment	Enhanced Collaboration with Law Enforcement	Strengthening Whistleblower Protections	Reinforcing the Role of the Compliance Officer
<ul style="list-style-type: none"> • Conduct a regular risk assessment of your organization’s systems and practices. Identify areas with higher vulnerabilities to fraud and prioritize mitigation efforts accordingly. • Use data analytics to proactively monitor suspicious patterns, focusing on outliers or discrepancies in claims, service utilization, and member demographics. 	<ul style="list-style-type: none"> • Develop relationships with local law enforcement and legal teams. Having a collaborative approach with agencies like the Department of Justice (DOJ) can ensure smoother handling of criminal investigations if fraud cases arise. • Encourage whistleblowers to partner with law enforcement, when necessary, as it can help resolve fraud cases faster. 	<ul style="list-style-type: none"> • Expand the whistleblower protection system to ensure confidentiality and safeguard individuals from retaliation. Consider implementing anonymous reporting tools or a thirdparty service to ensure complete privacy for whistleblowers. • In addition to a hotline, consider regular feedback loops for those who report, updating them on the status of investigations and actions taken. 	<ul style="list-style-type: none"> • The compliance officer should not only oversee fraud prevention but also serve as a trusted advisor to physicians and staff about billing and coding practices, providing guidance to avoid inadvertent mistakes. • Consider cross-training compliance officers in both clinical and administrative roles to improve their understanding of all aspects of the healthcare delivery process, making them more effective in identifying fraudulent activities.

Proactive Employee Engagement	Partnership with Members	Leverage Technology for Prevention and Detection	Regular Communication and Feedback
<ul style="list-style-type: none"> • Encourage employees to take an active role in identifying potential fraud by rewarding staff who bring forward valid concerns. • Organize regular "lunch and learn" sessions or webinars about recent changes in healthcare regulations, fraud detection techniques, and best practices. This keeps employees engaged and informed. 	<ul style="list-style-type: none"> • In addition to educating members about their rights, consider providing them with easy-to-understand tools or checklists for verifying their medical bills. For example, an online tool that allows members to compare their treatment history with the services billed. • Encourage members to keep a record of their visits and treatments, creating a transparent and collaborative environment between healthcare providers and members. 	<ul style="list-style-type: none"> • Invest in fraud detection software and machine learning tools to flag potential fraudulent claims or unusual billing patterns. These systems can quickly analyze large amounts of data and highlight red flags. • Integrate blockchain technology for secure and immutable record keeping of medical claims and transactions, ensuring data integrity and minimizing the risk of fraudulent alterations. 	<ul style="list-style-type: none"> • Provide frequent updates on the progress of the compliance program. This can include highlighting successes, areas for improvement, or challenges. • Create feedback loops that allow employees to voice concerns about the effectiveness of the current fraud prevention measures and suggest improvements.

By combining these strategies with a strong compliance framework, organizations can better combat fraud, waste, and abuse while ensuring a culture of transparency, trust, and integrity.

The Well Solutions Group brings extensive experience in developing fraud detection analytics and prevention strategies for payers. Our expertise includes data analysis and stratification, operational set-up and delivery, metrics and reporting, and analytic development. We have successfully executed our approach with payer clients ranging from small regional to national payers with incredible success.