Rethinking Fraud, Waste, Abuse and Compliance in a Changing Healthcare Landscape

In an era of new threats, regulations and risks, healthcare organizations must develop a more strategic approach to mitigation, using SMAC tools and next-generation services.

Executive Summary

As the healthcare business and technology landscape evolves, it is changing the rules for healthcare organizations and their partners to effectively manage fraud, waste and abuse (FWA), and minimize compliance risk. New risks, more sophisticated threats enabled by technology, and a host of new and complex regulations create major challenges for most healthcare organizations.

Mounting pressure to reduce the cost of care amid continuing margin shrinkage is resulting in intensified efforts by the healthcare industry to develop better FWA solutions. The Centers for Medicare & Medicaid Services (CMS) estimates that in 2012, the U.S. spent $2.8 trillion on healthcare.1 Fraud and abuse accounts for 3% of that annual expenditure, according to the National Health Care Anti-Fraud Association (NHCAA), and even up to 10%, according to estimates by other government and law enforcement agencies.2 This means that the cost of healthcare fraud and abuse is between $84 billion and $280 billion per year. In 2011, waste contributed an additional $476 billion to $991 billion, accounting for 17% to 35% of healthcare spending, according to a 2012 article published by the American Medical Association.3

With compliance failures only adding to these costs, it is clear that opportunities abound for improving FWA practices and reaping enormous cost savings.

Even as the urgency and complexity of successfully addressing FWA increases, new tools, technologies and approaches make it possible for healthcare organizations to craft more strategic, holistic approaches. Sometimes, a factor that introduces the potential for fraud, such as the transition to ICD-10, also creates opportunities for mitigating it.

This white paper provides an overview of the evolving healthcare landscape, as well as the associated new FWA threats and tools for mitigating them. We also discuss how the role of audit must evolve to use these tools effectively, both internally and with partners. The paper concludes with a strategy, plan and approach for deploying the next generation of investigative and audit services to successfully deal with these forces and greatly improve FWA practices.
Emerging Risks in the Shifting Healthcare Business Landscape

Three forces are combining to create new risks for the healthcare industry: major business model and economic shifts in the industry; continuously evolving regulations that create challenges for auditing; and technology advances that can be used for good and ill (see Figure 1). In order to prevent these risks from causing harm, organizations must devise a more strategic approach to audit.

Organizations must identify, prioritize and evaluate these emerging and existing risks and coordinate FWA efforts internally and with partners to craft effective responses. This means addressing both internal and external objectives, processes and governance, while ensuring that the benefits of the FWA strategy outweigh its costs. While many threats and risks are common to all healthcare organizations, individual entities must prioritize and target FWA mitigation efforts based on their mission, strategy and objectives. Risks evolve, so audit services must be positioned as a vital part of an organization’s overall business strategy. The complete threat landscape is illustrated in Figure 2.

Healthcare Threats and Impacts

![Figure 1](http://example.com/figure1.png)

![Figure 2](http://example.com/figure2.png)
The Evolving Healthcare Landscape

The risks arising from the healthcare industry’s evolution can have a direct impact on the financial results, quality of care and outcomes, and brand reputation for a healthcare organization. Here is a closer look at the business, technology and regulatory changes faced by the industry, as well as the risks they impose.

Healthcare Industry Business Changes Influencing FWA

New business and reimbursement models (see Figure 3) are giving rise to new types of risk:

- **Health insurance exchanges**: The Patient Protection and Affordable Care Act (PPACA) created health insurance exchanges (HIX) to help the uninsured find coverage. Risks include:
  - Eligibility fraud resulting from manipulated income levels to increase subsidies.
  - Members illegally buying insurance right before needing it and then canceling (“hit and run”).
  - Unauthorized access to data and data theft due to exposure to new entities such as navigators.
  - HIX-specific fraud and abuse (e.g., identity or data theft by unauthorized navigators).
  - Unhealthy and expensive membership that is not effectively risk-adjusted.
  - Meeting compliance requirements such as Minimal Acceptable Risk Standards for Exchanges (MARS-E), and Health Insurance Portability and Accountability Act (HIPAA) privacy and security.
  - Inaccurate risk adjustment resulting from, for example, inaccurate reporting of enrollments.

- **New reimbursement models**: Accountable care organizations (ACO) and patient-centered medical homes (PCMH) are two new reimbursement models designed to incent lower costs, improve quality and enhance patient satisfaction. Risks include:
  - Failure to comply with ACO audits per standard agreement with CMS and the supporting Medicare Shared Savings Program (MSSP).
  - Failure to comply with ACO waivers to facilitate development of ACOs and dealing with resulting FWA challenges.
  - Guiding beneficiaries to providers or suppliers based on factors other than patients’ medical best interests.
  - New and different opportunities for kickbacks and other violations enabled by new payment models as providers and payers become more closely linked and providers aggregate into physician groups.

Industry Changes Spark Threats

![Figure 3](image-url)
• **Provider consolidation and continuum of care expansion:** Providers are consolidating and expanding the continuum of care they offer to gain competitive critical mass and realize economies of scale. This creates challenges and risks around integrating disparate systems. Risks include:
  > Patient data privacy and security.
  > New opportunities to violate anti-kickback, Stark (i.e., limitations on certain physician referrals) and other laws.

• **Emergence of new provider contract types:** New provider contract types — based on episodes and outcomes — incent providers to work together to improve efficiency and outcomes, resulting in new risks:
  > Bundled payments, increasing collusion opportunities and inappropriate claim coding practices to realize higher payment rates, longer episode duration and greater episode payments.
  > Loss of effectiveness of existing FWA rules that assess individual claims for a provider-member combination to establish fraud, abuse and waste.

• **ICD-10:** ICD-10 is the new diagnosis and procedure coding system scheduled to replace ICD-9 on October 1, 2015. Eventually, ICD-10 is expected to benefit organizations by increasing specificity and accuracy, enabling increased automation — including for FWA. Risks include:
  > Provider upcoding to increase reimbursement.
  > Identifying coding errors and differentiating these from FWA.
  > Incompatibility of existing ICD-9 FWA with ICD-10. Recoded rules will be less effective until behaviors and trends using the new codes are understood.
  > Effectively dealing with both ICD-9 and ICD-10 codes during the runout period and for historical purposes.
  > Increased FWA costs resulting from learning curve, increased false positives and increased investigation.

• **Electronic health records:** Electronic health record (EHR) risks include:
  > Copy-and-paste capabilities allowing errors to be introduced when information is not reviewed for accuracy and can facilitate fraudulent activities such as inflated or duplicate billing.
  > Automated documentation capabilities facilitating fraudulent claims by instantly generating documentation for services that were not actually performed.
  > Creating another path for unauthorized access to patient information and identity theft.

• **M-health:** This is the practice of medicine supported by mobile devices, such as telemedicine. Risks include:
  > Violating privacy, security and confidentiality of protected data.
  > Credentialing, continuity of care, appropriateness of care, or care failures that impact quality and outcomes.

**Technology Influences on Next-Generation FWA**
Technology advances are a double-edged sword for FWA. While these technologies enable new strategies and capabilities for identifying and alleviating FWA, they also create new risks and compliance issues, including:

• **Social.** The rapid growth of social media and networking over the last five years has created risks related to data privacy and brand damage.

• **Mobility.** The proliferation of devices that can store and access data, yet generally offer less robust security than non-mobile systems, introduces risk, including theft and loss of data.

• **Analytics.** Individuals and organized crime can use these powerful tools to identify opportunities and exploit weaknesses.

• **Cloud.** Compliance and risk are at issue with cloud solutions, in which a third-party hosting organization has control and responsibility for data security.

• **Data.** The increasing availability of data in a multitude of forms facilitates privacy breaches and increases identity theft risks.
The Regulatory Compliance Chase
Major healthcare regulations are continually being refined and reinterpreted, making it difficult to define auditing approaches and compliance strategies.

<table>
<thead>
<tr>
<th>Patient Protection and Affordable Care Act (PPACA)</th>
<th>Health Insurance Portability and Accountability Act (HIPAA)</th>
<th>Health Information Technology for Economic and Clinical Health (HITECH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes:</td>
<td>Title 1</td>
<td>Promoting and expanding the adoption of health information technology to improve healthcare quality, safety and efficiency — e.g., electronic health records (EHR), health information exchanges (HIE) and meaningful use.</td>
</tr>
<tr>
<td>• Health insurance exchanges (HIX).</td>
<td>• Healthcare access, portability and renewability.</td>
<td></td>
</tr>
<tr>
<td>• Medicaid and Children’s Health Insurance Program (CHIP) expansion.</td>
<td>• Maintaining privacy and security of protected electronic health data.</td>
<td></td>
</tr>
<tr>
<td>• Medicare payment reform, including accountable care organizations (ACO).</td>
<td>• Preventing healthcare fraud and abuse.</td>
<td></td>
</tr>
<tr>
<td>• Anti-fraud provisions, including Medicare and Medicaid recovery auditor contractors (RACs).</td>
<td>• Administrative simplification (AS).</td>
<td></td>
</tr>
<tr>
<td>• Dual-eligible care coordination improvements.</td>
<td>• Medical liability.</td>
<td></td>
</tr>
<tr>
<td>• Quality improvement measures.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4

Regulations, Compliance and FWA Impact
Finally, a continuous stream of new regulations – and in many cases, their stop-and-go implementation – creates continually changing compliance challenges (see Figure 4).

Mitigating Evolving Healthcare FWA with Effective, Technology-Empowered Auditing
Amid rising and unfamiliar risks, the audit functions within healthcare organizations are under increasing pressure to deliver deeper insights; identify and respond to risk more quickly and proactively; and deliver analysis and actionable recommendations around key issues to drive business change. To accomplish these goals, audit must be equipped with a new strategic outlook on FWA mitigation, supported by new technology. The enhanced compliance can lead to transformed business processes and superior financial results (see Figure 5).

Audit Strategy, Planning and Approach
Minimizing the compliance risks and FWA threats requires a new strategic partnership between investigative services and business owners across the enterprise and beyond. To get started, the organization must shift its perception of audit-
tors from a “policing” function to one of strategic intelligence assets. Such a shift can ensure at the outset that business partnerships and associated agreements do not introduce or expose the organization to unnecessary risks, thereby eliminating some or all audit effort. Similar benefits can be realized in other areas, including development of policies and procedures, and business processes and rules, as well as procurement and vendor management.

While collecting information from a hospital, a mobile platform can help an auditor compare costs with national and regional averages, provide history of the provider’s error trends, validate diagnosis to procedure combination or validate medical codes and grouping.

Seating audit with business strategy leaders can facilitate transformation and ensure that the best decisions are made. By adding their knowledge to the decision-making process, audit professionals can help identify and prevent problems, such as vulnerable business processes and inadequate or inappropriate policies. If the audit role is narrow and held to a policing function, as it too often is, these opportunities are often lost, as audit cannot adequately influence decision-making or prioritize audit activities to align with business strategy.

Audit success also requires organizations to adopt a prospective rather than retrospective approach. Retrospective audits review transactions only after they are paid or processed. A prospective audit uses real-time surveillance to examine susceptible transactions when they are submitted to identify anomalies and ensure they are appropriate before they are paid or processed. This is a critical distinction because organizations need to prevent FWA rather than chase it. By detecting fraud more quickly, organizations can limit their losses, as well as the expense and time of recovery activities. The continuous surveillance of prospective auditing also has been shown to deter fraud.

Finally, an effective audit plan prioritizes and addresses internal and external threats to business processes and systems. The plan must address traditional risks and also provide a way to identify and address the new risks outlined above. An effective plan also realizes efficiencies by coordinating efforts to meet multiple operational, strategic and compliance requirements across the organization, which are necessary with initiatives such as the ICD-10 transition and EHR adoption.

Leveraging Evolving Technology to Enhance Audit Functionality

As discussed, technology creates risks but also enables the evolution of audit capabilities and functionality through innovations such as computer-assisted audit tools (CAAT), predictive analytics, data visualization, and continuous auditing and monitoring to help counter threats. Effective audit also means that systems and tools have appropriate and usable built-in logs and alerts. For example, ensuring that an EHR logs how information was entered and by whom facilitates investigation and prevention of FWA.

Organizations must develop and maintain technological expertise within the audit function. Putting together key audit advances with four underlying technologies – social, mobility, cloud and analytics (aka the SMAC Stack™) – can help address existing and emerging healthcare threats more efficiently and effectively.

- **Social tools:** Disability, medical liability and worker’s compensation insurance fraud investigators in particular are using social tools and platforms to profile cases and understand fraud patterns. For example, social media updates and photos can be used as evidence to contradict claims. An example is an Ohio construction worker who pleaded guilty in August 2013 to worker’s compensation fraud. The worker was doing construction work in Arizona while collecting benefits for an injury in Ohio. The tipping point in the investigation was evidence from Facebook photos and messages that identified the fraud scheme.

Text analytics and social network analytics are two key social investigation tools. Text analytics can analyze unstructured data like Twitter logs, Facebook or other social medical files. Social network analytics can be used to uncover how the location of events, time (geo-tagging) and different users or service providers are connected.

- **Mobility:** Mobile platforms greatly streamline and automate on-site audits and evidence collection. Advanced analysis and algorithms built into mobile devices can provide both strategic and operational intelligence. For example, while collecting information from a hospital, a mobile platform can help an auditor...
compare costs with national and regional averages, provide history of the provider’s error trends, validate diagnosis to procedure combination or validate medical codes and grouping. This increases the effectiveness of the investigation and reduces the possibility of user errors that typically arise in manual processes.

- **Advanced analytics and big data:** Leveraging advanced analytics and big data eliminates the incompleteness and inaccuracies associated with sampling techniques. Importantly, analysis can be done in real time or near real time to ensure action can be taken as soon as data is available. Structured and unstructured data, including police records, Social Security death records, court proceedings, credit data, government agency assistance, social media and customer service logs, can be used along with standard administrative and medical records to identify FWA trends.

Advanced and predictive analytics used in conjunction with big data can become the foundation for prospective auditing, as well as provide intelligence for transforming a variety of business processes. Specific tools and their capabilities include:

- **Predictive analytics** (see sidebar):
  - Supervised models use historically known behaviors to identify suspicious behaviors. Examples of such models include linear regression models and neural networks.
  - Unsupervised models are used to identify outliers or abnormal behaviors. Examples of techniques include peer group comparisons and clustering.

- **Text analysis:** Text analysis can be applied to vast amounts of unstructured data such as claim notes, customer service logs, police records and court records. These are valuable sources of information both at the time of detection and during an investigation.

- **Geospatial analysis:** Geospatial analysis provides the locational view of clusters to identify potential relationships, such as proximity of claimants or a pharmacy to member or provider locations, and helps identify group schemes.

- **Link analysis:** Link analysis reviews social relationships and ties between entities in a network. Often, a single claim might not be identified as incorrect, but with a group of claims created at a similar time, location or group, a relationship can become visible. Link analysis can show member-to-member or provider-to-member or provider connections in related cases like multiple same-pharmacy claims from a few pharmacies for a small group of members in which member-to-pharmacy distance is very high.

- **Cloud:** Cloud-hosted FWA analytical services provide the capabilities to process large data sets at cost-effective price points. All health organizations can benefit from software-as-a-service (SaaS) platforms for FWA detec-

---

**Quick Take**

**A Case for Predictive Analytics**

A brief case from CMS illustrates the value of predictive analytics. On June 30, 2011, CMS began using a fraud prevention system (FPS) based on predictive analytics to analyze all Medicare fee-for-service (FFS) claims to detect fraudulent activity. The FPS uses algorithms and models to examine FFS claims in real-time to flag suspicious billing. The system builds profiles of providers, networks, billing patterns and beneficiary utilization to create risk scores to estimate fraud likelihood and both flag and prioritize potentially fraudulent claims and billing patterns.

CMS is also continuously developing and refining models. FPS savings in 2013 were $210.7 million, or a $5 to $1 (500%) return on investment. Additional benefits include permanently stopping future billings by fraudulent providers and the associated “sentinel effect” that deters fraud from occurring in the first place.

A benefit of predictive analytics can be illustrated using the example of detecting ICD-10 FWA after the October 1, 2015, cutover. The job of converting and recalibrating detection rules from ICD-9 to ICD-10 is complex and requires the ability to predict new coding behaviors, since the history won’t be immediately available. Predictive analytics can be used instead to detect and identify upcoding and improper treatments by comparing a provider with peers to identify outliers. This is facilitated as the increased coding specificity of ICD-10 replaces some clinical notes (that cannot be machine-read), allowing audit activities to be automated.
tion, investigation and management. Cloud services provide turnkey support for the following:

» Integration of disparate data sources for more accurate and insightful audit results.
» Advanced security, including encryption of data that is static, in-transit and being processed; strong authentication; and fine-grained authorization.
» HIPAA-compliant private clouds.

Strategic Partnering
Collaborating with business partners and government is critical to FWA success. This includes coordinating activities, sharing findings and working to integrate data stores and access across the value chain. The benefits of partnering include:

• Identification of FWA across the entire population of patients, possible medical conditions and treatments, and multiple insurers, including public programs. Such a comprehensive perspective is typically difficult for any single organization to build.
• Aggregation of patient data across constituents. Such data consolidation can help support new insights and pattern detection, using advanced analytics.
• Engaging members and patients who are often ignored as part of an audit. For example, patients can often easily detect fraud; they may receive billing for services, pharmaceuticals or equipment never received or used. However, explanations of benefits (EOB) statements are often complex, making it unlikely that a patient will thoroughly review them, especially when copays are low. Payers should work to simplify bills to make it easy for patients to review and help detect fraud and errors. They should also ensure patients have access to EHRs and can easily validate the data they contain.

Learning and Continuously Optimizing
Organizations must use audit results to strengthen processes and internal controls to detect, correct and prevent FWA and ensure compliance. Additionally, the audit organization must define measures to assess audit effectiveness and identify opportunities for improvement. FWA must be carefully differentiated from legitimate errors so the appropriate corrective actions can be taken, whether recovery, legal, training or outreach.

Audit Program Management
Finally, executing an effective audit program across the organization requires management that is similar in many ways to an effective program management office (PMO). This effort can be part of the PMO responsibility; conversely, an organization can set up a dedicated audit program management function. While a detailed discussion is beyond the scope of this paper, key elements of successful audit program management address governance and organization, review and reporting, planning and tracking, assurance, and management of risks, resources, budget, benefits, stakeholders, vendors and technology.

Looking Forward
Rapid changes across the healthcare industry, a dynamic regulatory environment and emerging technologies demand a new approach to fraud, waste, abuse and compliance strategies. Organizations must identify, prioritize and plan audit and compliance strategies and efforts as a key part of overall FWA strategy to ensure success. Our recommendations include:

• Use predictive analytics to review every transaction susceptible to fraud, waste and abuse on a real-time basis across all systems and processes. Leverage internal data together with partner data and augment with external data.
• Use real-time monitoring and surveillance to stop fraud before payments are made and other negative effects occur.
• Understand how to do root-cause analysis to quickly determine the source of the problem and correct it, whether it lies within a process, people, partner or system.
• Implement capabilities to measure the effectiveness of audit techniques by identifying meaningful measures and implementing monitoring, alerts and reporting.
• Leverage cloud and SaaS technologies to enable flexible solutions to deal with evolving threats at lower price points and with low maintenance.
• Improve efficiency by using mobility-based platforms and tools.
• Engage partners, including providers, to reduce errors and inadvertent non-compliance.
• Leverage a vendor that understands anomalies that result from analytics and how to separate false positives and prioritize the rest for maximum benefit.
Many organizations have existing audit capabilities. However, even the most advanced must adapt and upgrade them to meet rapidly evolving challenges. Organizations must follow a thorough and rigorous evaluation process to understand the effects of existing practices, the current financial drain due to FWA and how the changing healthcare business landscape affects FWA trends in different lines of business.

In this climate, auditors are very well-positioned to save healthcare organizations time and money and even help them create and enhance key business processes through next-generation FWA and compliance activities. Business leaders must champion audit’s capabilities to achieve these strategic goals, helping to transform their organization’s perception of the value of audit.

Footnotes

About the Authors
Anirbanjyoti Chakraborty is an Associate Director with Cognizant’s Healthcare Solutions Practice, with nearly 15 years of experience in health plan strategy, operation, solution design and program management. In this role, Anirban focuses on creating IP-based business solutions to help health plans solve critical business problems and improve business outcomes. He can be reached at Anirbanjyoti.Chakraborty@cognizant.com.

Bill Hamilton is a Principal with Cognizant Business Consulting’s Healthcare Practice, with 20 years of experience in management and IT consulting across various industries. Bill has extensive experience in health plan strategy, operations and program management in the areas of transformation, modernization, information management and regulatory compliance. Technical areas of expertise include enterprise system design and development, analytics, mobile and distributed computing, cloud computing and software development lifecycle management and governance. Bill has written seven books and published articles about software development and database technologies. He can be reached at William.Hamilton@cognizant.com.

Ramesh Raghavan is a founder of Cognizant’s Healthcare Business Unit and currently serves as Vice-President of the unit, responsible for solutions and services. He has 25 years of experience in information technology, serving various lines of businesses. Ramesh envisioned, led and built many of Cognizant’s healthcare business offerings, including IP-based solution assets and knowledge centers that address healthcare clients’ evolving business needs, spanning payment integrity practices and services. Ramesh is a member of and participant in several industry bodies and thought leadership forums that drive the direction of healthcare, globally. He holds a master’s in engineering from Indian Institute of Technology. Ramesh can be reached at rraghava@cognizant.com.

Acknowledgments
The authors would like to thank Palani Munisamy, Director of Healthcare Industry Business Development, for his contributions to this white paper.
About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world’s leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 75 development and delivery centers worldwide and approximately 199,700 employees as of September 30, 2014, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.