REPRINT

R&C risk & compliance

HEALTHCARE FRAUD MITIGATION AND INVESTIGATIONS: IMPACT OF AI

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2024 ISSUE

www.riskandcompliancemagazine.com

BDO

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

HEALTHCARE FRAUD MITIGATION AND INVESTIGATIONS: IMPACT OF AI

PANEL EXPERTS

Jared Crafton
Forensic Technology Practice Leader
BDO USA, LLP
T: +1 (617) 378 3689
E: jcrafton@bdo.com

As the head of BDO's forensic technology practice, **Jared Crafton** brings over 20 years of experience advancing the scientific maturity of his client's investigations, compliance programmes and litigation matters. He leads a team of onshore and offshore resources in the areas of e-discovery, managed document review, forensic data analytics, privacy and data protection, and data breach advisory services. His personal book of business focuses on forensic data science, providing clients with effective strategies for tackling complex data environments with easy to understand analyses and mitigations.

Pavel Petrov
Global Head, SpeakUp Office
Novartis
T: +41 (61) 529 2954
E: pavel.petrov@novartis.com

Pavel Petrov is the global head of the SpeakUp Office at Novartis. The SpeakUp Office oversees the management of complaints concerning possible instances of misconduct within the company that may involve allegations relating to violations of the code of ethics, relevant company policies, as well as local laws and regulations. He joined Novartis in 2005 and has assumed positions of greater accountability within the finance, internal audit, and ethics, risk and compliance departments.

Robert Sikellis
Global Head of Litigation and
Investigations
Novartis
T: +1 (862) 223 0780
E: robert.sikellis@novartis.com

Robert Sikellis is the global head of litigation and investigations at Novartis. In this capacity, he has overall global responsibility for group-relevant litigation, as well as internal and governmental investigations. Prior to joining Novartis in 2019, he worked for Siemens AG where he held several leadership roles in the legal and compliance functions including as chief counsel compliance, where he was responsible for all compliance-related investigations worldwide and all governmental investigations.

R&C: Could you provide an overview of the scale of fraud in the healthcare sector? How would you describe the nature and scope of the problem?

Sikellis: Fraud in the healthcare industry is a major problem worldwide, resulting in the loss of billions of dollars annually. Estimates suggest that around $455bn of the $7.35 trillion spent on healthcare each year is lost to fraud and corruption – translating into as much as 10 percent of total healthcare expenditure in certain countries. While the secretive nature of fraud makes it difficult to determine its exact scale, it has wide-ranging consequences that include substandard or unnecessary procedures, counterfeit medications, delayed or denied treatments, compromised patient safety, increased costs and a profound loss of trust in the healthcare system. Additionally, fraud diverts resources away from legitimate healthcare needs, potentially compromising the quality of care. With the rise of digital healthcare systems, new methods of fraud are emerging, such as cyber fraud and data breaches. Therefore, remaining vigilant and staying ahead of potential risk areas is crucial for the industry.

Crafton: When we talk about fraud in healthcare, we could be talking about internal fraud by employees, external fraud from consumers and companies defrauding the government. As an industry valued at over $800bn, there is a lot of incentive for individuals as well as organisations to misbehave. With many organisations operating on a global scale and increasing their reliance on data and technology, healthcare fraud is at an all-time high. Healthcare fraud can also stem from other types of fraud. For example, an unrelated data breach that leads to identity theft can result in a fraudulent healthcare claim. These complexities can make fraud detection and prevention even more difficult.

R&C: What types of healthcare frauds are typically being perpetrated? How are methods evolving?

Crafton: Medical coding fraud, kickbacks, drug diversion and false claims are some of the most common healthcare fraud schemes. Many of these schemes share patterns, though some have evolved with new twists. For example, telehealth claims are increasingly common and can be harder for healthcare organisations to verify. The industry is seeing an increase in coordinated attacks both on the cyber front, which leads to identity theft, but also with using the stolen data to perpetrate false claims. Increased sophistication in technology allows bad actors to perpetrate large frauds quicker and more rigorously. Some examples of this include email spoofing and using deepfakes to make false claims.

Sikellis: Healthcare fraud is a constantly evolving problem that encompasses various activities targeting vulnerabilities in the system. Both individuals and organised criminal networks engage in schemes to exploit these weaknesses for personal financial gain. With the increasing digitalisation of healthcare systems, schemes are now targeting sensitive patient data through cyber fraud. Data breaches can lead to medical identity theft, fraudulent insurance claims and the creation of counterfeit identities. These fraudulent practices not only jeopardise patient safety but also undermine public trust in scientific research and medical advancements. To combat these evolving methods, regulatory bodies, healthcare organisations and technology experts are utilising advanced analytics, machine learning (ML) and artificial intelligence (AI) to detect patterns of fraud and identify suspicious activities. Ongoing research and collaboration are crucial in staying ahead of new vulnerabilities and protecting the integrity of healthcare systems.

R&C: How would you describe monitoring and detection efforts around healthcare sector fraud? Are you seeing a rise in investigations into suspected wrongdoing?

> “Predictive modelling and anomaly detection, powered by ML algorithms, are becoming widely used to proactively identify fraudulent activities.”
>
> *Pavel Petrov, Novartis*

Petrov: To effectively combat healthcare fraud, a strong monitoring and detection programme is crucial. Predictive modelling and anomaly detection, powered by ML algorithms, are becoming widely used to proactively identify fraudulent activities. Collaboration and information sharing among healthcare organisations, government agencies and other stakeholders is vital to identify fraudulent activities and build comprehensive cases against wrongdoers. Encouraging employees to report fraudulent activities through company whistleblower programmes is also important. Companies are increasing investments in fraud prevention, training programmes and technology to identify suspicious activities. The digitalisation of healthcare systems and stricter regulations have increased the visibility of potential fraud, leading to a rise in investigations. Data analytics and whistleblower reports also play major roles in identifying fraudulent activities. However, healthcare sector fraud remains a persistent challenge, and ongoing collaboration, technological advancements and vigilance are necessary to enhance monitoring and detection efforts.

Crafton: As a highly regulated sector, healthcare has traditionally had strong monitoring and detection embedded in its culture. Compliance departments have built out robust programmes focusing on risks and processes. The rise of advanced technology and AI is providing a new arms race between compliance officers and bad actors. It is imperative that healthcare organisations invest in skillsets and technology to combat these new challenges, as well as educate compliance and legal teams on navigating a rapidly evolving landscape. One of the biggest challenges for compliance officers is to understand the newest schemes that evolve in the sector and then quickly implement countermeasures.

R&C: In what ways can artificial intelligence (AI) help to detect healthcare-related scams? What AI solutions are being deployed?

> “Data breaches can lead to medical identity theft, fraudulent insurance claims and the creation of counterfeit identities.”
>
> *Robert Sikellis, Novartis*

Crafton: There are many use cases for AI in the detection of healthcare fraud. Transaction monitoring is a mature use case that leverages ML models to detect anomalies in large data sets. These kinds of tools can be used in an unsupervised environment where the data tells a story on its own or in a supervised environment with more direction around the types of insights that are generated. Supervised methodology, for example if a compliance team identifies a fraudulent transaction, can train an ML model to look for more instances of the same scheme, multiplying the force of existing knowledge. We are also seeing increased usage of AI to review more unstructured data such as emails and documents. For example, technology assisted review utilises AI models to quickly cut through large corpuses of information to get to key issues.

Petrov: AI offers multifaceted support in identifying healthcare-related scams. AI-powered models can detect patterns indicative of fraudulent activities, utilising AI techniques, such as pattern recognition or predictive analytics, to detect anomalies, irregular patient information or counterfeit products. ML models can learn from past instances of falsified medicines to predict and prevent future occurrences and can continuously evolve to recognise new scam tactics, enhancing detection accuracy over time. Some AI solutions already in deployment utilise AI-driven analytics to flag suspicious activities which may safeguard healthcare systems from financial losses and protect patients from potential harm. Regarding the deployment of AI solutions, it is an area that is evolving rapidly, with some aspects still in the testing and exploration phase. Because the healthcare industry may handle sensitive and confidential information, such as patient information, companies should take into consideration ethical practices and privacy protection for any deployed AI solution.

R&C: What challenges and complexities may arise when using AI for fraud prevention?

Sikellis: Implementing AI for fraud prevention in the healthcare industry comes with several challenges and complexities. One major obstacle is ensuring data quality is accurate and up to date and this is, no doubt, crucial for reliable predictions. Another issue is the potential for biases in AI algorithms which can result in discriminatory targeting or missing fraud in specific demographics. Scalability is also a concern, as AI systems must be continually updated to keep up with evolving

> “While the healthcare industry is very excited about the possibilities that new technologies bring to bear, there are many pitfalls.”
>
> *Jared Crafton, BDO USA, LLP*

fraud techniques. Explainability poses a challenge as well, as understanding the decision-making process of AI can be difficult. Privacy regulations add another layer of complexity, potentially limiting the data available for AI training. Overall, ongoing research, development and ethical considerations are essential for leveraging the full potential of AI in healthcare fraud prevention while maintaining responsible and effective usage.

Crafton: The considerations for using AI for fraud prevention are generally the same as those for implementing AI for any other use case. Data privacy and security, bias, transparency, and regulatory compliance top the list. It is critical for any AI user to know how their data was created, governed and manipulated so they can understand the full mechanics of the AI model. Most compliance teams are a few steps removed from the data they are monitoring, so it is important for them to work with business lines and IT to gain the understanding they need. Part of this is also understanding the changing regulatory environment, particularly around data privacy, to avoid any potential risk of noncompliance. Finally, many legal and compliance teams do not have the budget they need to implement AI and need to create strong business cases to fight for their share of innovation.

R&C: What advice would you offer to healthcare companies on selecting and implementing AI systems for mitigating and investigating potential fraud?

Crafton: While the healthcare industry is very excited about the possibilities that new technologies bring to bear, there are many pitfalls. It is important to define the use cases that are going to be most beneficial to an organisation and understand their specific risks. It is generally recommended to start with small proofs of concept or pilot projects to test ideas. Many companies are further away than they realise from achieving meaningful results, but setting a vision is the first step to building a roadmap. Most of the gaps in expectations have to do with data quality and lacking the knowledge for how to enrich it. In some cases, it may be easier and more valuable for an organisation to improve its analytics maturity rather than implement an AI tool. The addition of a workflow tool can also pay significant dividends.

Sikellis: When assessing the implementation of AI systems to combat healthcare fraud, there are several factors to consider. First, it is important to understand the specific needs and challenges that the AI system should address. This involves identifying the types of fraud prevalent in the company's operations and ensuring reliable source data. It is crucial to prioritise AI models that provide explainable outputs for regulatory compliance and scalability to detect emerging fraud patterns. Involving stakeholders such as fraud experts, data scientists, IT professionals, and legal and privacy advisers is vital to align with regulatory requirements and best practices. Ongoing monitoring, evaluation and refinement of the AI models should be implemented, and investment in training and change management is important to maximise the AI system's impact. Lastly, human oversight is essential to review the cases flagged by the AI system to ensure fairness, accountability and error-free decision making.

R&C: Looking ahead, what innovations may we expect to see in AI technologies designed to combat new healthcare fraud threats?

Petrov: In the future, there is a possibility that fraudulent activities will not be carried out by humans but by AI agents themselves. As AI systems become more advanced and independent, they might engage in fraudulent activities to achieve their objectives. To counter this, advanced monitoring AI systems could be developed to regulate other AI systems and ensure they operate ethically and legally. This oversight, known as 'AI-on-AI', would prevent AI agents from committing fraud. Specialised fraud detection agents built upon large language model (LLM) platforms are expected to be deployed. These agents would be tailored to identify and respond to fraud in healthcare, providing a dynamic fraud detection system. The role of LLMs is also anticipated to grow significantly, as they can process and analyse complex datasets such as medical records and insurance claims, making them valuable tools for detecting fraud across different fields.

Crafton: Some of the most exciting innovation has to do with human and machine interaction. Layering in an LLM chatbot over a compliance dashboard brings incredibly powerful analytics to people who otherwise might lack the skills, training or accessibility to consume these results. This can significantly decrease the effort around fostering technology adoption within an organisation. Learning to effectively communicate with technology is also going to open minds for more creative analysis and free up time to accomplish more strategic goals. Equally as exciting are the possibilities around collaboration that AI brings. The ability to scan large data sets, both structured and unstructured, and quickly get meaningful results will allow more companies to share intelligence around what fraud schemes are being perpetrated and how to combat them. Portable AI detection models that organisations can quickly adopt will help close compliance gaps faster than we have ever seen before.